Lecture notes for MATH 770 : Foundations of Mathematics

—

University of Wisconsin – Madison, Fall 2005

Itaï BEN YAACOV

Itaï BEN YAACOV, Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex

URL: http://math.univ-lyon1.fr/~begnac/

Contents

CHAPTER 1

Propositional Logic

Basic ingredients:

- *Propositional variables*, which will be denoted by capital letters $P, Q, R, \ldots$, or sometimes $P_0, P_1, P_2, \ldots$. These stand for basic statements, such as "the sun is hot", "the moon is made of cheese", or "everybody likes math". The set of propositional variables will be called *vocabulary*. It may be infinite.
- Logical connectives: $\neg$ (unary connective), $\rightarrow$, $\wedge$, $\vee$ (binary connectives), and possibly others.

Each logical connective is defined by its *truth table*:

A	$\neg A$
T	F
F	T

A	B	$A \rightarrow B$	$A \wedge B$	$A \vee B$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	F

Thus:

- The connective $\neg$ means "not": $\neg A$ means "not A".
- The connective $\wedge$ means "and".
- The connective $\vee$ means "*inclusive* or": $A \vee B$ means "A, or B, *or both*".
- The connective $\rightarrow$ means "if ... then ...": $A \rightarrow B$ means "if A then B (but if not A then anything goes)".

We can always define new connectives by specifying their truth tables.

1.1. Syntax

We will define propositional formulae as finite sequences of symbols. The allowable symbols are usually grouped in two:

(i) *Logical symbols:* parentheses and connectives (,),$\neg$,$\rightarrow$,$\wedge$,$\vee$.
(ii) *Nonlogical symbols:* The propositional variables, each viewed as a single symbol (even if we denote it by P_{13}).

The *propositional formulae* (sometimes simply called *propositions*) are constructed inductively:

- Each propositional variable is a formula. These are the *atomic formulae*.

- If φ and ψ are formulae, so are $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ and $(\varphi \to \psi)$. These are the *compound formulae*.

Formally: we let $\mathcal{S}_0$ be the set of all propositional variables. For each n, given $\mathcal{S}_n$ define

$$\mathcal{S}_{n+1} = \mathcal{S}_n \cup \{(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi) \colon \varphi, \psi \in \mathcal{S}_n\}.$$

Then $\mathcal{S} = \bigcup_{n\in\mathbb{N}} \mathcal{S}_n$ is the set of all formulae.

We call $\mathcal{S}_n$ the set of formulae *constructed in n steps*.

For example, $(P \to Q)$ and $(R \vee (P \wedge (\neg Q)))$ are formulae, but $(\wedge P)$ and $\neg Q)$ are not. With time we will allow ourselves to omit some parentheses if the meaning remains clear: for example, instead of $(\neg((\neg P) \to (\neg Q)))$ we will write $\neg(\neg P \to \neg Q)$ (we follow the convention that $\neg$ binds more strongly than the binary connectives).

When wanting to prove that all formulae have a certain property, we usually use "proof by induction on the construction of the formula":

THEOREM 1.1.1 (Proof by induction on the structure). *Let X is a property that a formula may or may not have. Assume that:*

(i) *All atomic formulae have property X.*
(ii) *If φ and ψ are formulae which have property X then so do $(\neg\varphi)$, $(\varphi \to \psi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$.*

Then all formulae have property X.

PROOF. Let $C \subseteq \mathbb{N}$ be the set of all natural numbers n such that there exists $\varphi \in \mathcal{S}_n$ which does not have property X. Assume first that $C \neq \varnothing$. Then there is a minimal $n \in C$. Since all atomic formulae have property X: $n > 0$. But then all formulae in $\mathcal{S}_{n-1}$ have property X, whereby all formulae in $\mathcal{S}_n$ must have it, so $n \notin C$. This contradiction shows that $C = \varnothing$. Therefore all formulae have property X. ■$_{1.1.1}$

We can similarly prove:

THEOREM 1.1.2 (Proof by induction on the structure). *Let X is a property that a formula may or may not have. Assume that for every formula φ, if all shorter formulae have property X then so does φ. Then every formula has property X.*

PROOF. Same idea: if not all formulae have property X then there is a shortest one which doesn't, and we get a contradiction. ■$_{1.1.2}$

The connectives give rise to functions $\mathcal{E}_\neg \colon \mathcal{S} \to \mathcal{S}$ and $\mathcal{E}_\to, \mathcal{E}_\wedge, \mathcal{E}_\vee \colon \mathcal{S}^2 \to \mathcal{S}$:

$$\mathcal{E}_\neg(\varphi) = (\neg\varphi),$$
$$\mathcal{E}_\square(\varphi, \psi) = (\varphi \square \psi) \qquad\qquad \square \in \{\to, \vee, \wedge\}.$$

We call these functions *construction operations*.

THEOREM 1.1.3 (Unique reading). (i) *The ranges of the construction operations $\mathcal{E}_\square \colon \square \in \{\neg, \to, \vee, \wedge\}$ are disjoint from each other and from $\mathcal{S}_0$.*

(ii) *All the construction operations are injective (= one-to-one).*

PROOF. Exercise 1.2. ■1.1.3

We may say that the set $\mathcal{S}$ is *freely generated* from $\mathcal{S}_0$ by the operations $\mathcal{E}_\square$: $\square \in \{\neg, \to, \wedge, \vee\}$.

1.2. Semantics

1.2.1. Truth assignments and truth values. We interpret a propositional language by assigning a truth value T or F (True or False, respectively) to the propositional variables (whence their name).

DEFINITION 1.2.1. A *truth assignment* is a mapping $v_0 \colon \mathcal{S}_0 \to \{T, F\}$.

THEOREM 1.2.2. *Let v_0 be a truth assignment. Then there is a unique mapping $v \colon \mathcal{S} \to \{T, F\}$ such that:*

(i) $v\restriction_{\mathcal{S}_0} = v_0$ *(i.e., $v(P) = v_0(P)$ for all $P \in \mathcal{S}_0$).*
(ii) *For all $\varphi, \psi \in \mathcal{S}$, the values of $v(\neg\varphi)$ and $v(\varphi \square \psi)$ for $\square \in \{\to, \wedge, \vee\}$ are determined from $v(\varphi)$ and $v(\psi)$ by the truth tables. (So if $v(\varphi) = T$ and $v(\psi) = F$ then $v(\neg\varphi) = F$, $v(\varphi \vee \psi) = T$, $v(\varphi \wedge \psi) = F$, $v(\varphi \to \psi) = F$.)*

PROOF. We define by induction on n mappings $v_n \colon \mathcal{S}_n \to \{T, F\}$ extending v_0. We are already given v_0. Given $v_n \colon \mathcal{S}_n \to \{T, F\}$, we extend it to $v_{n+1} \colon \mathcal{S}_{n+1} \to \{T, F\}$ according to the truth tables. By the unique reading theorem, there is no ambiguity. Then $v = \bigcup_{n \in \mathbb{N}} v_n$ is as required.

If v' is another such mapping, then we show that $v(\varphi) = v'(\varphi)$ for all φ by induction on the structure of φ, whence uniqueness. ■1.2.2

Since v_0 uniquely determines v we will not bother too much to distinguish between them and call either one a *truth assignment*. We call $v(\varphi)$ the *truth value* of φ under the assignment v.

DEFINITION 1.2.3 (Satisfaction).
(i) Let φ be a formula and v a truth assignment. If $v(\varphi) = T$ we say that v *satisfies* or *models* φ, in symbols $v \vDash \varphi$.
(ii) Let Γ be a set of formulae and v a truth assignment. We say that v *satisfies* or *models* Γ if $v \vDash \varphi$ for all $\varphi \in \Gamma$.
(iii) A *model* of a formula φ (or set of formulae Γ) is a truth assignment v which satisfies φ (or Γ).

DEFINITION 1.2.4 (Logical consequence and equivalence). Let φ be a formula, Γ a set of formulae. If every model of Γ is also a model of φ then φ is a *logical consequence* of Γ, or that Γ *logically implies* φ, in symbols $\Gamma \vDash \varphi$.

In case $\Gamma = \{\psi\}$ we say that ψ implies φ, etc.

If φ and ψ are two formulae such that $\varphi \vDash \psi$ and $\psi \vDash \varphi$ we say that φ and ψ are *logically equivalent*, denoted $\varphi \equiv \psi$.

EXAMPLE 1.2.5. P implies $P \vee Q$ and $Q \wedge P$ implies P. $P \wedge Q$, $Q \wedge P$ and $(P \wedge Q) \wedge P$ are all equivalent.

For our purposes logically equivalent formulae are indeed the same and we will allow ourselves to identify them. For example for every three formulae φ, χ, ψ we have:

$$(\varphi \wedge \psi) \wedge \chi \equiv \varphi \wedge (\psi \wedge \chi),$$
$$\varphi \wedge \psi \equiv \psi \wedge \varphi.$$

Therefore, up to logical equivalence, conjunction is commutative and associative. This allows us to write $\bigwedge_{i<n} \varphi_i$ instead of $\varphi_0 \wedge (\varphi_1 \wedge (\varphi_2 \wedge \ldots))$. The same holds for disjunction.

DEFINITION 1.2.6 (Tautologies). We say that a formula φ is *valid*, or that it is a *tautology*, if it is satisfied by every truth assignment.

EXAMPLE 1.2.7. $P \vee \neg P$ is a tautology. Also, φ implies ψ if and only if $\varphi \to \psi$ is a tautology. All tautologies are equivalent.

Let φ be a formula and $n \in \mathbb{N}$ such that all the propositional variables appearing in φ are among $P_0, \ldots, P_{n-1}$. Then for every truth assignment v, the truth value $v(\varphi)$ depends only on $v(P_0), \ldots, v(P_{n-1})$. Thus φ determines a function $g_{\varphi,n} \colon \{T, F\}^n \to \{T, F\}$ defined by the property:

$$g_{\varphi,n}(v(P_0), \ldots, v(P_{n-})) = v(\varphi).$$

(A function $g \colon \{T, F\}^n \to \{T, F\}$ is called a *Boolean function*.)

Also, if ψ is another formula which only involves $P_0, \ldots, P_{n-1}$, then $\varphi \equiv \psi$ if and only if $g_{\varphi,n} = g_{\psi,n}$. Thus, up to logical equivalence, the mapping sending φ to $g_{\varphi,n}$ is one-to-one. Is it onto?

The positive answer is a corollary of a result which is interesting in itself:

DEFINITION 1.2.8.
(i) A *literal* is an atomic proposition or its negation, i.e., something of the form $\neg P$ or Q. It is sometimes convenient to denote a literal by P^e, where $e \in \{T, F\}$: P^T is P, and P^F is $\neg P$.
(ii) A *(conjunctive) clause* is a conjunction of several literals, i.e., something of the form $P \wedge Q \wedge \neg R$, or more generally, of the form $\bigwedge_{i<n} P_i^{e_i}$ where $\bar{e} = (e_0, \ldots, e_{n-1}) \in \{T, F\}^n$.
(iii) A formula in *disjunctive normal form (DNF)* is a disjunction of clauses, i.e., something of the form $\bigvee_{i<m} \gamma_i$ where each γ_i is a clause.

PROPOSITION 1.2.9. *For every Boolean function $g \colon \{T, F\}^n \to \{T, F\}$ there is a formula φ in disjunctive normal form such that φ only involves $P_0, \ldots, P_{n-1}$, and $g = g_{\varphi,n}$.*

PROOF. Each possible input of g is a tuple $\bar{e} \in \{T, F\}^n$. For each such possible input define $\gamma_{\bar{e}} = \bigwedge_{i<n} P_i^{e_i}$. Then $\gamma_{\bar{e}}$ is a clause, and a truth assignment v satisfies $\gamma_{\bar{e}}$ if and only if $v(P_i) = e_i$ for all $i < n$.

Let $W \subseteq \{T,F\}^n$ be non-empty, and let $\varphi_W = \bigvee_{\bar{e}\in W} \gamma_{\bar{e}}$. Then $v \vDash \varphi_W$ if and only if $(v(P_0),\dots,v(P_{n-1})) \in W$.

Therefore, if there is at least one possible input for g such that $g(\bar{e}) = T$ we can define $\varphi = \varphi_{\{\bar{e}\in\{T,F\}^n:\, g(\bar{e})=T\}}$. If, on the other hand, $g(\bar{e}) = F$ for all $\bar{e} \in \{T,F\}^n$, let us just take $\varphi = P_0 \wedge \neg P_0$. In either case φ is in DNF and $g = g_{\varphi,n}$. ■1.2.9

COROLLARY 1.2.10. *Every formula is equivalent to a formula in DNF.*

1.2.2. Compactness.

DEFINITION 1.2.11 (Satisfiability).
We say that a set of formulae Γ is *satisfiable* if it has a model. A formula φ is satisfiable if $\{\varphi\}$ is.
We say that Γ is *finitely satisfiable* if every finite subset $\Gamma_0 \subseteq \Gamma$ is satisfiable.

FACT 1.2.12. *Assume that the set of propositional variables is countable, i.e., it is finite, or we can enumerate it (without repetitions) as* $\mathcal{S}_0 = \{P_0, P_1, P_2, \dots, P_n, \dots : n \in \mathbb{N}\}$.

Then the set of all formulae is countable.

PROOF. Define an order on the symbols: first come $(,), \neg, \wedge, \vee, \to$ in this order, then $P_0, P_1, \dots$. For every n, list, in lexicographic order, all formulae of length $\leq n$ in which only $P_0,\dots,P_{n-1}$ may appear. Each such list is finite, and every formula appears on some list. Concatenate these lists, omitting all but the first occurrence of each formula, to obtain an enumeration $\mathcal{S} = \{\varphi_n : n \in \mathbb{N}\}$ as required. ■1.2.12

LEMMA 1.2.13. *Let* Γ *be a finitely satisfiable set of formulae and* φ *a formula. Then at least one of* $\Gamma \cup \{\varphi\}$ *or* $\Gamma \cup \{\neg\varphi\}$ *is finitely satisfiable.*

PROOF. Assume for a contradiction that neither is. Then there are finite subsets $\Gamma_0, \Gamma_1 \subseteq \Gamma$ such that neither $\Gamma_0 \cup \{\varphi\}$ nor $\Gamma_1 \cup \{\neg\varphi\}$ are satisfiable. But $\Gamma_0 \cup \Gamma_1$ is a finite subset of Γ, and therefore satisfiable. Let v be a model of $\Gamma_0 \cup \Gamma_1$. Then either $v \vDash \varphi$ or $v \vDash \neg\varphi$, so it is a model of $\Gamma_0 \cup \{\varphi\}$ or of $\Gamma_1 \cup \{\neg\varphi\}$, a contradiction. ■1.2.13

LEMMA 1.2.14. *Let* Γ *be a finitely satisfiable set of formulae. Then there exists a finitely satisfiable set of formulae* $\Delta \supseteq \Gamma$ *such that in addition, for all* $\varphi \in \mathcal{S}$ *either* $\varphi \in \Delta$ *or* $\neg\varphi \in \Delta$.

PROOF. We will assume that $\mathcal{S}_0$ is countable: if not, we need tools from set theory we do not yet have (Zorn's Lemma). We can therefore enumerate $\mathcal{S} = \{\varphi_n : n \in \mathbb{N}\}$. We define a sequence $(\Delta_n : n \in \mathbb{N})$ by induction:

- $\Delta_0 = \Gamma$.
- If $\Delta_n \cup \{\varphi_n\}$ is finitely satisfiable then $\Delta_{n+1} = \Delta_n \cup \{\varphi_n\}$. Otherwise $\Delta_{n+1} = \Delta_n \cup \{\neg\varphi_n\}$.

We claim first that Δ_n is finitely satisfiable for all n. This is proved by induction on n: For $n = 0$ this is given. The passage from Δ_n to Δ_{n+1} is by the previous Lemma.

Note that by construction $\Gamma = \Delta_0 \subseteq \Delta_1 \subseteq \ldots \subseteq \Delta_n \subseteq \ldots$, and define $\Delta = \bigcup_n \Delta_n$. We claim that Δ is finitely satisfiable. Indeed, if $\Gamma_0 \subseteq \Delta$ is finite, then there is some $n \in \mathbb{N}$ such that $\Gamma_0 \subseteq \Delta_n$, and then Γ_0 is satisfiable since Δ_n is finitely satisfiable.

Therefore Δ is as required. ■1.2.14

THEOREM 1.2.15 (Compactness Theorem for Propositional Logic). (i) *A set of formulae Γ is satisfiable if and only if it is finitely satisfiable.*

(ii) *Let Γ be a set of formulae and φ a formula. Then $\Gamma \vDash \varphi$ if and only if there is a finite subset $\Gamma_0 \subseteq \Gamma$ such that $\Gamma_0 \vDash \varphi$.*

PROOF. We will only prove the first item. The equivalence of the two items is left as an exercise.

Assume Γ is finitely satisfiable. By Lemma 1.2.14 there is $\Delta \supseteq \Gamma$ which is finitely satisfiable and in addition for all φ either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$. Define a truth assignment v by:

$$v(P) = \begin{cases} T & \text{if } P \in \Delta \\ F & \text{if } \neg P \in \Delta. \end{cases}$$

We claim that for all φ: $v(\varphi) = T \iff \varphi \in \Delta$. We prove this by induction on the construction of φ. For φ atomic, this is by definition of v. Assume now that φ is compound, say $\varphi = \psi \wedge \chi$. If $v(\varphi) = T$, we must have $v(\psi) = v(\chi) = T$, so by the induction hypothesis $\psi, \chi \in \Delta$. Since $\{\psi, \chi, \neg\varphi\}$ is not satisfiable and Δ is finitely satisfiable we cannot have $\neg\varphi \in \Delta$, whereby $\varphi \in \Delta$. Conversely, assume that $\varphi \in \Delta$. Then $\{\neg\psi, \varphi\}$ is not satisfiable, so $\psi \in \Delta$, and similarly $\chi \in \Delta$. By the induction hypothesis $v(\psi) = v(\chi) = T$, whereby $v(\varphi) = T$. The other cases of compound formulae are treated similarly.

In particular, $v \vDash \Delta$, and *a fortiori* $v \vDash \Gamma$. ■1.2.15

1.3. Syntactic deduction

The notion of logical consequence introduced earlier is a form of *semantic deduction*. Consider for example an extremely simple instance of logical consequence, such as:

$$\varphi \vDash \psi \to \varphi.$$

In order to verify that $\psi \to \varphi$ is indeed a logical consequence of φ we need to understand semantic notions such as truth assignments and truth tables, and then go through the process of checking all possible truth assignments to the propositional variables appearing in φ and ψ and verifying such for every such assignment, if φ is true, then so is $\psi \to \varphi$.

This is bothersome: after all, just "by looking" on φ and $\psi \to \varphi$ we can see that the latter is a consequence of the former, without needing any semantic notions. This is a special case of *syntactic deduction*: with no more than simple syntactic manipulations we will be able to deduce (or "prove") formulae from other formulae. Indeed, in real-life Mathematics, a proof is merely a sequence of assertions (alas, in an informal natural

language such as English, Hebrew or French) such that each statement seems to follow from the previous ones (and sometimes, unfortunately, not even that).

Here we will define formal proofs, or deductions, which will follow very strict rules that ensure that no mistake is possible. Throughout this course we will consider more than one logic, and therefore more than one deduction systems. Still, all the deduction systems we will consider have similar structure. For our purposes (more general definitions can be given):

DEFINITION 1.3.1. A *deduction system* $\mathscr{D}$ consists of:

(i) A family of formulae which we call the *logical axioms*.
(ii) A single *inference rule* saying that from φ and $\varphi \to \psi$ we may infer ψ. This inference rule is called *Modus Ponens*.

Thus for our purposes a deduction system is given by its set of logical axioms.

DEFINITION 1.3.2 (Formal deduction). Let $\mathscr{D}$ be a deduction system (i.e., a set of logical axioms), and Γ a set of formulae. A *$\mathscr{D}$-deduction sequence* from Γ is a finite sequence of formulae $(\varphi_i \colon i < n)$ such that for each $i < n$ at least one of the following holds:

(i) φ_i is a logical axiom of $\mathscr{D}$.
(ii) $\varphi_i \in \Gamma$ (we then say that φ_i is a *premise*).
(iii) There are $j, k < i$ such that $\varphi_k = \varphi_j \to \varphi_i$. In other words, φ_i can be inferred via Modus Ponens from the formulae φ_j and φ_k appearing earlier in the sequence.

We say that a formula φ can be *deduced* (or *inferred*, or *proved*) from Γ in $\mathscr{D}$, in symbols $\Gamma \vdash_{\mathscr{D}} \varphi$, if there exists a $\mathscr{D}$-deduction sequence from Γ ending with φ.

We said that a formal deduction allows no mistake. Of course, this depends on the deduction system: false logical axioms could clearly lead to fallacious deductions. We will therefore restrict our consideration to sound deduction systems:

DEFINITION 1.3.3. A deduction system $\mathscr{D}$ is *sound* if for every set of formulae Γ and formula φ, if $\Gamma \vdash_{\mathscr{D}} \varphi$ then $\Gamma \vDash \varphi$.

LEMMA 1.3.4. *A deduction system is sound if and only if all its logical axioms are valid.*

PROOF. Clearly, if φ is a logical axiom of $\mathscr{D}$ and $\mathscr{D}$ is sound then $\vdash_{\mathscr{D}} \varphi$ whereby $\vDash \varphi$, i.e., φ is valid. Conversely, assume all the logical axioms of $\mathscr{D}$ are valid, and that $\Gamma \vdash_{\mathscr{D}} \varphi$. Let $(\varphi_i \colon i < n)$ be the deduction sequence witnessing this. We will show by induction on $i < n$ that $\Gamma \vDash \varphi_i$. For each i there are three cases to be considered:

(i) If φ_i is a logical axioms then it is valid, and in particular $\Gamma \vDash \varphi_i$.
(ii) If $\varphi_i \in \Gamma$ then $\Gamma \vDash \varphi_i$.
(iii) The last case is that there are $j, k < i$ such that $\varphi_k = \varphi_j \to \varphi_i$. By the induction hypothesis $\Gamma \vDash \varphi_j$ and $\Gamma \vDash \varphi_j \to \varphi_i$. Thus every models of Γ models φ_j and $\varphi_j \to \varphi_i$, and therefore φ_i. In other words, $\Gamma \vDash \varphi_i$.

We conclude that $\Gamma \vDash \varphi_{n-1}$, i.e., $\Gamma \vDash \varphi$. ■1.3.4

The converse property is more interesting, and less easy to characterise:

DEFINITION 1.3.5. A deduction system $\mathscr{D}$ is *complete* if it is sound, and for every set of formulae Γ and formula φ, if $\Gamma \vDash \varphi$ then $\Gamma \vdash_{\mathscr{D}} \varphi$.

Our task here will be to produce a complete proof system for Propositional Logic. To simplify notation we will restrict now the connectives to $\neg$ and $\rightarrow$. We thus redefine, until further notice, $\mathcal{S} = \mathcal{S}_{\{\neg,\rightarrow\}}$, and by a *formula* we mean $\varphi \in \mathcal{S}_{\{\neg,\rightarrow\}}$. Since the system of connectives $\{\neg, \rightarrow\}$ is full (see Exercise 1.4), there is no semantic loss, and we gain in syntactic simplicity.

Our deduction system will consist of the following logical axiom schemes:

(A1) $$\varphi \rightarrow (\psi \rightarrow \varphi),$$

(A2) $$((\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))),$$

(A3) $$((\neg\varphi \rightarrow \psi) \rightarrow ((\neg\varphi \rightarrow \neg\psi) \rightarrow \varphi)).$$

These being *schemes* means that we have such logical axioms for every possible choice of formulae φ, ψ and χ.

We will prove:

COMPLETENESS THEOREM FOR PROPOSITIONAL LOGIC. The deduction system consisting of the logical axiom schemes above is sound and complete.

Soundness will be left as an easy exercise, while completeness will occupy the rest of this section. Since we work with a fixed deduction system we will omit it: we will therefore speak of deduction sequences, write $\Gamma \vdash \varphi$, etc.

Let us start with a few warm-up exercises:

LEMMA 1.3.6.
(i) *The concatenation of deduction sequences is a deduction sequence.*
(ii) *Assume $\varphi_0, \ldots, \varphi_{n-1}$ is a deduction sequence and $i < n$. Then $\varphi_0, \ldots, \varphi_{n-1}, \varphi_i$ is also a deduction sequence.*
(iii) *Assume $\Gamma \vdash \varphi_i$ for $i < n$ and $\{\varphi_0, \ldots, \varphi_{n-1}\} \vdash \psi$. Then $\Gamma \vdash \psi$.*
(iv) *If $\Gamma \subseteq \Gamma'$ and $\Gamma \vdash \varphi$ then $\Gamma' \vdash \varphi$.*
(v) *Assume $\Gamma \vdash \varphi$. Then there is a finite subset $\Gamma_0 \subseteq \Gamma$ (namely, the set of premises used in a deduction of φ from Γ) such that $\Gamma_0 \vdash \varphi$.*

LEMMA 1.3.7. *For every formulae φ, ψ:*
(i) $\vdash (\varphi \rightarrow \varphi)$
(ii) $\varphi \vdash (\psi \rightarrow \varphi)$
(iii) $\neg\neg\varphi \vdash \varphi$

PROOF. (i) The following is a deduction sequence from the empty set:
1. $(\varphi \rightarrow (\varphi \rightarrow \varphi))$ A1 with $\psi = \varphi$.

2. $(\varphi \to ((\varphi \to \varphi) \to \varphi))$ A1 with $\psi = (\varphi \to \varphi)$.
3. $((\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)))$ A2 with $\chi = \varphi$, $\psi = (\varphi \to \varphi)$.
4. $((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$ MP from 2 and 3.
5. $(\varphi \to \varphi)$ MP from 1 and 4.

(ii) The following is a deduction sequence from φ:
1. φ premise.
2. $(\varphi \to (\psi \to \varphi))$ A1.
3. $(\psi \to \varphi)$ MP 1,2.

(iii) There is a deduction sequence from $\neg\neg\varphi$ containing:
1. $(\neg\varphi \to \neg\varphi)$ previous result.
2. $(\neg\varphi \to \neg\neg\varphi)$ provable from $\neg\neg\varphi$.
3. $((\neg\varphi \to \neg\varphi) \to ((\neg\varphi \to \neg\neg\varphi) \to \varphi))$ A3.
4. $((\neg\varphi \to \neg\neg\varphi) \to \varphi)$ MP 1,3.
5. φ MP 2,4. ■1.3.7

PROPOSITION 1.3.8 (The Deduction Theorem). *For every set of formulae* Γ *and formulae* φ, ψ*:* $\Gamma, \varphi \vdash \psi \iff \Gamma \vdash \varphi \to \psi$.

PROOF. Right to left is clear: first deduce $\varphi \to \psi$ then apply MP to obtain ψ.

Let us prove left to right. We assume that $\Gamma, \varphi \vdash \psi$, so there is a deduction sequence $\varphi_0, \ldots, \varphi_{n-1}$ from Γ, φ and $\psi = \varphi_{n-1}$. We will prove by induction on $i < n$ that $\Gamma \vdash \varphi \to \varphi_i$. At each step we consider several cases, according to the manner in which φ_i was added to the original sequence:

(i) If φ_i is either an axiom or a premise of Γ then $\Gamma \vdash \psi_i$, and as $\psi_i \vdash \varphi \to \psi_i$ we conclude that $\Gamma \vdash \varphi \to \psi_i$.

(ii) If $\varphi_i = \varphi$, we know that $\vdash \varphi \to \varphi$ whereby $\Gamma \vdash \varphi \to \varphi$.

(iii) The last case is that φ_i is obtained by Modus Ponens. Then there are $j, k < i$ such that $\varphi_k = \varphi_j \to \varphi_i$. Then by the induction hypothesis we have $\Gamma \vdash \varphi \to \varphi_j$ and $\Gamma \vdash \varphi \to (\varphi_j \to \varphi_i)$. We use the following instance of A2:

$$(\varphi \to (\varphi_j \to \varphi_i)) \to ((\varphi \to \varphi_j) \to (\varphi \to \varphi_i)).$$

Put together and applying MP twice we obtain $\Gamma \vdash \varphi \to \varphi_j$.

Since $\psi = \varphi_{n-1}$, we obtain a deduction of $\varphi \to \psi$ from Γ. ■1.3.8

DEFINITION 1.3.9. A set of formulae Γ is *consistent* if there exists a formula φ such that $\Gamma \nvdash \varphi$. Otherwise it is *contradictory*.

LEMMA 1.3.10. *For every formulae* φ, ψ*:*

(i) $\varphi, \neg\varphi \vdash \psi$ *(i.e.,* $\{\varphi, \neg\varphi\}$ *is contradictory).*
(ii) $\neg\varphi \vdash (\varphi \to \psi)$.

PROOF. (i) We can prove from $\varphi, \neg\varphi$:
1. $(\neg\psi \to \varphi)$ provable from φ.

2. $(\neg\psi \to \neg\varphi)$ provable from $\neg\varphi$.
3. $((\neg\psi \to \varphi) \to ((\neg\psi \to \neg\varphi) \to \psi))$ A3.
4. ψ MP (twice) 1,2,3.

(ii) By the Deduction Theorem.

■1.3.10

LEMMA 1.3.11. *If Γ is contradictory then there is a finite subset $\Gamma_0 \subseteq \Gamma$ which is.*

PROOF. Let φ be a formula. Then $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$. Therefore there are finite subsets $\Gamma_1, \Gamma_2 \subseteq \Gamma$ such that $\Gamma_1 \vdash \varphi$ and $\Gamma_2 \vdash \neg\varphi$. Then $\Gamma_0 = \Gamma_1 \cup \Gamma_2$ is contradictory. ■1.3.11

LEMMA 1.3.12. (i) *Assume that $\Gamma, \neg\varphi$ is contradictory. Then $\Gamma \vdash \varphi$.*

(ii) *Assume that Γ is consistent. Then at least on of $\Gamma \cup \{\varphi\}$ or $\Gamma \cup \{\neg\varphi\}$ is consistent.*

PROOF. (i) Assuming that $\Gamma, \neg\varphi$ is contradictory we have $\Gamma, \neg\varphi \vdash \varphi$, and we can deduce from Γ:

1. $(\neg\varphi \to \varphi)$ By the Deduction Theorem.
2. $(\neg\varphi \to \neg\varphi)$ By a previous result.
3. $((\neg\varphi \to \varphi) \to ((\neg\varphi \to \neg\varphi) \to \varphi))$ A3.
4. φ MP 1,2,3.

(ii) If $\Gamma, \neg\varphi$ is consistent, fine. If it is contradictory then $\Gamma \vdash \varphi$, and as Γ is assumed to be consistent, so is $\Gamma \cup \{\varphi\}$. ■1.3.12

In this section we wish to drop the assumption that the language is countable. For this we need a tool from set theory called Zorn's Lemma:

DEFINITION 1.3.13. Let $(X, \leq)$ be a partially ordered set.

(i) A subset $\mathcal{C} \subseteq X$ is a *chain* if for all $a, b \in \mathcal{C}$ either $a \leq b$ or $b \leq a$.

(ii) We say that $(X, \leq)$ is *inductive* if it is non-empty, and every chain in X is bounded from above, i.e., if for every chain $\mathcal{C} \subseteq X$ there is $a \in X$ such that for all $b \in \mathcal{C}$: $b \leq a$.

(iii) A *maximal* member of $(X, \leq)$ is a member $a \in X$ such that for all $b \in X$, if $b \geq a$ then $b = a$ (i.e., no $b \in X$ may be strictly greater than a, but they may be incomparable).

FACT 1.3.14 (Zorn's Lemma). *Let $(X, \leq)$ be an inductive partially ordered set. Then X contains a maximal element.*

LEMMA 1.3.15. *Let Γ be a consistent set of formulae. Then:*

(i) *The following set is inductive when ordered by inclusion:*

$$X = \{\Gamma' \colon \Gamma \subseteq \Gamma' \subseteq \mathcal{S} \text{ and } \Gamma' \text{ is consistent}\}.$$

It therefore contains a maximal member.

(ii) *Let Δ be a maximal consistent set of formulae containing Γ. Then for every φ either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$, and $\varphi \in \Delta$ if and only if $\Delta \vdash \varphi$.*

PROOF. We only prove the first item, the second being quite easy. Since $\Gamma \in X$ it is non-empty. Let $\mathcal{C} \subseteq X$ be a (non-empty) chain, and let $\Gamma' = \bigcup \mathcal{C}$. Clearly $\Gamma'' \subseteq \Gamma'$ for all $\Gamma'' \in \mathcal{C}$, so all we need to show is that $\Gamma' \in X$. First, $\Gamma \subseteq \Gamma'$. Second, assume that Γ' is contradictory. Then there is a finite subset $\Gamma'_0 \subseteq \Gamma'$ which is contradictory. But since Γ'_0 is finite and Γ' is the union of the chain $\mathcal{C}$, there is $\Gamma'' \in \mathcal{C}$ such that $\Gamma'_0 \subseteq \Gamma''$, so Γ'_0 cannot be contradictory. This contradiction shows that Γ' is consistent, and therefore belongs to X. ■1.3.15

THEOREM 1.3.16 (Completeness Theorem for Propositional Logic). *Let Γ be a set of formulae and φ a formula (in which the only connectives are $\neg$ and $\rightarrow$).*

(i) *The set Γ is satisfiable if and only if it is consistent (in the deduction system given above).*
(ii) $\Gamma \vDash \varphi \Longleftrightarrow \Gamma \vdash \varphi$.

PROOF. We only prove the first item. The equivalence of the two items is left as an exercise.

If Γ is satisfiable then it is consistent by soundness (for example $\Gamma \nvdash \neg(P \rightarrow P)$).

Conversely, assume that Γ is consistent, and we need to show it is satisfiable. By Lemma 1.3.15, there exists a maximal consistent set of formulae $\Delta \supseteq \Gamma$. For every formula φ we have $\varphi \in \Delta$ or $\neg\varphi \in \Delta$, and $\varphi \in \Delta \Longleftrightarrow \Delta \vdash \varphi$.

Define a truth assignment v by:

$$v(P) = \begin{cases} T & \text{if } P \in \Delta \\ F & \text{if } P \notin \Delta. \end{cases}$$

We claim that for all φ: $v \vDash \varphi \Longleftrightarrow \varphi \in \Delta$. We prove this by induction on the construction of φ. There are three cases to be considered:

(i) For φ atomic, this is by definition of v.
(ii) If $\varphi = \neg\psi$, we have by the induction hypothesis:

$$v \vDash \varphi \Longleftrightarrow v \nvDash \psi \Longleftrightarrow \psi \notin \Delta \Longleftrightarrow \varphi = \neg\psi \in \Delta.$$

(iii) Finally, assume that $\varphi = \psi \rightarrow \chi$. If $v \vDash \psi \rightarrow \chi$ then either $v \vDash \chi$ or $v \vDash \neg\psi$ (or both). By the induction hypothesis, either $\chi \in \Delta$ or $\neg\psi \in \Delta$. In either case, $\Delta \vdash \psi \rightarrow \chi$, whereby $\psi \rightarrow \chi \in \Delta$.

If $v \nvDash \psi \rightarrow \chi$ then necessarily $v \vDash \psi$ and $v \vDash \neg\chi$. By the induction hypothesis $\psi, \neg\chi \in \Delta$, and since $\{\psi, \neg\chi, \psi \rightarrow \chi\}$ is contradictory: $\psi \rightarrow \chi \notin \Delta$.

In particular, $v \vDash \Delta$, and *a fortiori* $v \vDash \Gamma$. ■1.3.16

REMARK 1.3.17. The Compactness Theorem is also a consequence of the Completeness Theorem: if Γ is finitely satisfiable then it is consistent by soundness (and the fact

that deductions are finite) and therefore satisfiable by completeness. This means that we have now proved the Compactness Theorem for uncountable languages as well.

Exercises

EXERCISE 1.1. Let α be any finite sequence of symbols. Define:

$$len(\alpha) = \langle \text{length of } \alpha \rangle,$$
$$k(\alpha) = \langle \text{number of left parentheses in } \alpha \rangle - \langle \text{number of right parentheses in } \alpha \rangle,$$

and assuming $n \leq len(\alpha)$:

$$\alpha\restriction_n = \langle \text{first } n \text{ symbols of } \alpha \rangle.$$

Prove that:

(i) For every $\varphi \in \mathcal{S}$: $k(\varphi) = 0$, and if $0 < n < len(\varphi)$ then $k(\varphi\restriction_n) > 0$.
(ii) If $\varphi = \mathcal{E}_\square(\psi, \chi)$, where $\square \in \{\rightarrow, \vee, \wedge\}$ and $\psi, \chi \in \mathcal{S}$, then $len(\psi)$ is the minimal n such that $0 < n < len(\varphi)$ and and $k(\varphi\restriction_{n+1}) = 1$.

EXERCISE 1.2. Using the previous exercise, prove Theorem 1.1.3.

EXERCISE 1.3 (Polish notation). The syntax we defined above is called *infix notation*, since the binary connectives come between the two formulae which they connect. We can also defined *prefix notation* sometimes better known as *Polish notation*.

The set $\mathcal{S}'$ of Polish formulae is defined as the set of finite sequences of symbols generated from $\mathcal{S}_0$ by the following construction operators:

$$\mathcal{E}'_\neg(\varphi) = \neg\varphi,$$
$$\mathcal{E}'_\square(\varphi, \psi) = \square\varphi\psi \qquad \square \in \{\wedge, \vee, \rightarrow\}.$$

This notation has several advantages over standard notation: it does not require parentheses, and it accommodates more easily higher-arity connectives. For example, we can introduce a new ternary connective $*$ through $\mathcal{E}'_*(\varphi, \psi, \chi) = *\varphi\psi\chi$. On the other hand, it is less natural to read.

Prove the unique readability theorem for Polish notation. (Hint: you may want to replace the parentheses counting function k with an appropriate auxiliary function k'. Since it cannot count parentheses, what should it count?)

EXERCISE 1.4. In the same way we defined the connectives $\neg, \rightarrow, \vee, \wedge$ we can define other connectives, specifying their arity (i.e., no. of arguments) and truth table. If $\mathcal{C}$ is any family of connectives, we can the define $\mathcal{S}_\mathcal{C}$ as the family of formulae generated from $\mathcal{S}$ using the connectives in $\mathcal{C}$ (so $\mathcal{S}$ defined earlier is just $\mathcal{S}_{\{\neg,\rightarrow,\vee,\wedge\}}$).

Satisfaction is defined again according to the truth tables.

We say that a system of connectives $\mathcal{C}$ is *full* if every $\varphi \in \mathcal{S}$ is logically equivalent to some $\varphi' \in \mathcal{S}_\mathcal{C}$.

For example Corollary 1.2.10 says in particular that the system $\{\neg, \vee, \wedge\}$ is full.

(i) Prove that the system $\{\neg, \to\}$ is full. (To simplify life, show that it is enough to prove that each of the formulae $P \wedge Q$ and $P \vee Q$ has a logically equivalent counterpart in $\mathcal{S}_{\{\neg,\to\}}$.)

(ii) We define a new connective, called the Sheffer stroke, or NAND ("not and"):

A	B	$A \mid B$
T	T	F
T	F	T
F	T	T
F	F	T

Show that $\{|\}$ is a full system of connectives.

EXERCISE 1.5 (Boolean algebras). A *Boolean algebra* is a set $\mathscr{A}$ equipped with constants $0, 1 \in \mathscr{A}$, a unary operation $\neg$, and binary operations $\wedge, \vee$, satisfying for all $a, b, c \in \mathscr{A}$:

$$\begin{array}{ccc}
\neg\neg a = a & & \\
\neg 0 = 1 & \neg 1 = 0 & \\
\neg(a \vee b) = \neg a \wedge \neg b & \neg(a \wedge b) = \neg a \vee \neg b & \text{(de Morgan's laws)} \\
a \vee (b \vee c) = (a \vee b) \vee c & a \wedge (b \wedge c) = (a \wedge b) \wedge c & \text{(associativity)} \\
a \vee b = b \vee a & a \wedge b = b \wedge a & \text{(commutativity)} \\
a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) & a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) & \text{(distributivity)} \\
a \vee (a \wedge b) = a & a \wedge (a \vee b) = a & \text{(absorption)} \\
a \vee \neg a = 1 & a \wedge \neg a = 0 & \text{(complements)}
\end{array}$$

(Notice the duality between the two columns: the two axioms of each row are equivalent modulo previous axioms.) Show that the following identities hold in every Boolean algebra:

$$\begin{array}{cc}
a \vee a = a & a \wedge a = a \\
a \vee 0 = a & a \wedge 1 = a \\
a \vee 1 = 1 & a \wedge 0 = 0
\end{array}$$

EXERCISE 1.6. Let X be a set and let $\mathcal{P}(X)$ be the family of subsets of X (called the *power set* of X). Let $0_{\mathcal{P}(X)} = \varnothing$, $1_{\mathcal{P}(X)} = X$, $\neg_{\mathcal{P}(X)}$ be complement, and $\vee_{\mathcal{P}(X)}, \wedge_{\mathcal{P}(X)}$ be union and intersection, respectively. Show that $\langle \mathcal{P}(X), 0_{\mathcal{P}(X)}, 1_{\mathcal{P}(X)}, \neg_{\mathcal{P}(X)}, \vee_{\mathcal{P}(X)}, \wedge_{\mathcal{P}(X)} \rangle$ is a Boolean algebra.

EXERCISE 1.7. Let T be a set of formulae. Say that φ and ψ are equivalent *modulo* T, in symbols $\varphi \equiv_T \psi$, if $T \vDash \varphi \to \psi$ and $T \vDash \psi \to \varphi$.

(i) Show that $\equiv_T$ is an equivalence relation.

(ii) Show that it is a congruence relation with respect to the connectives, i.e., that if $\varphi \equiv_T \varphi'$ and $\psi \equiv_T \psi'$ then $\neg\varphi \equiv_T \neg\varphi'$, $\varphi \wedge \psi \equiv_T \varphi' \wedge \psi'$, etc.

(iii) Define $[\varphi]_T$ as the equivalence of φ modulo $\equiv_T$, and $\mathscr{A}_T$ as the family of all such equivalence classes:

$$[\varphi]_T = \{\psi \in \mathcal{S} \colon \varphi \equiv_T \psi\},$$
$$\mathscr{A}_T = \mathcal{S}/\equiv_T = \{[\varphi]_T \colon \varphi \in \mathcal{S}\}.$$

We define the following operations on $\mathscr{A}_T$:

$$\neg[\varphi]_T = [\neg\varphi]_T,$$
$$[\varphi]_T \wedge [\psi]_T = [\varphi \wedge \psi]_T,$$
$$[\varphi]_T \vee [\psi]_T = [\varphi \vee \psi]_T.$$

Show that these operations are well-defined: namely, if $a \in \mathscr{A}_T$, then $\neg a$ does not depend on the particular choice of φ such that $a = [\varphi]_T$, etc.

(iv) Show that with these operations $\mathscr{A}_T$ is a Boolean algebra (what should 0 and 1 be?) It is called the *Lindenbaum (or Lindenbaum-Tarski) algebra* of T.

EXERCISE 1.8. Show that the two statements in Theorem 1.2.15 are equivalent.

EXERCISE 1.9. Let R be a commutative ring (all rings considered here have a unit). An ideal $I \lhd R$ is *proper* if it is not equal to R, or equivalently, if $1 \notin I$. An ideal $I \lhd R$ is *prime* if it is proper and for all $a, b \in R$, if $ab \in I$ then at least one of a, b belongs to I. We denote by $(a, b, \ldots)$ the ideal generated in R by $\{a, b, \ldots\}$.

(i) Show that if I is a proper ideal and $ab \in I$ then at least one of $I + (a)$ and $I + (b)$ is proper.

(ii) Use the Compactness Theorem of Propositional Logic to show that if $I \lhd R$ is proper then it is contained in a prime ideal.

EXERCISE 1.10. Let Φ and Ψ be two sets of formulae satisfying that for every truth assignment v, if $v \vDash \varphi$ for all $\varphi \in \Phi$ then $v \vDash \psi$ for some $\psi \in \Psi$ (informally we may write this as $\bigwedge \Phi \vDash \bigvee \Psi$). Show there are finite subsets $\{\varphi_0, \ldots, \varphi_{n-1}\} \subseteq \Phi$ and $\{\psi_0, \ldots, \psi_{m-1}\} \subseteq \Psi$ such that $\bigwedge_{i<n} \varphi_i \vDash \bigvee_{j<m} \psi_j$.

EXERCISE 1.11. Let Φ be a set of formulae closed under logical connectives, and assume that ψ is a formula satisfying that for every two truth assignments v and v', if $v(\varphi) = v'(\varphi)$ for all $\varphi \in \Phi$ then $v(\psi) = v'(\psi)$. Show that ψ is logically equivalent to some formula in Φ.

Hint: you may need to use the Compactness Theorem twice. Show first that if $v \vDash \psi$ then there is a formula $\varphi_v \in \Phi$ such that $v \vDash \varphi_v$ and $\varphi_v \vDash \psi$.

EXERCISE 1.12 (Boolean rings). A *Boolean ring* is a ring R all of whose elements are idempotent: $a^2 = a$ for all $a \in R$.

(i) Let R be a Boolean ring. Show that R is commutative or characteristic 2 (i.e., $a + a = 0$ for all $a \in R$). Define operations on R as follows:

$$\begin{aligned} \neg a &= 1 + a, \\ a \wedge b &= ab, \\ a \vee b &= a + b + ab. \end{aligned}$$

Prove that $(R, 0, 1, \neg, \vee, \wedge)$ is a Boolean algebra.

(ii) Let $(\mathscr{A}, 0, 1, \neg, \vee, \wedge)$ be a Boolean algebra. Define:

$$\begin{aligned} ab &= a \wedge b, \\ a + b &= (a \wedge \neg b) \vee (b \wedge \neg a), \\ -a &= a. \end{aligned}$$

Show that $(\mathscr{A}, 0, 1, -, +, \cdot)$ is a Boolean ring.

(iii) Show that these operations are one the inverse of the other.

Exercise 1.13. Let $\mathscr{A}$ be a Boolean algebra. Show that the relation $a \leq b \iff a \wedge b = a$ is a partial ordering. Show that 0 is the least element, 1 is the greatest, $\vee$ and $\wedge$ preserve the order (in both arguments) and $\neg$ inverses it.

Exercise 1.14 (Filters). Let $\mathscr{A}$ be a Boolean algebra. A *filter* is a subset $\mathscr{F} \subseteq \mathscr{A}$ satisfying:

(i) $\mathscr{F} \neq \varnothing$.
(ii) If $a, b \in \mathscr{F}$ then $a \wedge b \in \mathscr{F}$.
(iii) If $a \in \mathscr{F}$ and $b \geq a$ then $b \in \mathscr{F}$.

It is *proper* if $0 \notin \mathscr{F}$. It is an *ultrafilter* if it is proper, and in addition:

(iv) For all $a \in \mathscr{A}$ either $a \in \mathscr{F}$ or $\neg a \in \mathscr{F}$.

Show that:

(i) Let $\mathscr{F} \subseteq \mathscr{A}$ and $I_{\mathscr{F}} = \{\neg a \colon a \in \mathscr{F}\}$. Then $\mathscr{F}$ is a filter if and only if $I_{\mathscr{F}}$ is an ideal of the corresponding Boolean ring.
(ii) Show that $\mathscr{F}$ is an ultrafilter if and only if $I_{\mathscr{F}}$ is a prime ideal, if and only if it is a maximal (proper) ideal.
(iii) Show that if $\mathscr{F}$ is a proper filter on a Boolean algebra $\mathscr{A}$ then it extends to an ultrafilter $\mathscr{U}$ on $\mathscr{A}$.

Exercise 1.15 (Stone duality). Let $\mathscr{A}$ be a Boolean algebra. Let $S(\mathscr{A})$ be the set of all ultrafilters on $\mathscr{A}$. For $a \in \mathscr{A}$, let $[a] = \{x \in S(\mathscr{A}) \colon a \in x\}$.

The space $S(\mathscr{A})$ is called the *Stone space* of $\mathscr{A}$, and we equip it with the *Stone topology*:

(i) Show that the family of sets $\{[a] \colon a \in \mathscr{A}\}$ is a basis for a topology on $S(\mathscr{A})$.

(ii) Show that the topology from the previous item is compact and totally disconnected (i.e., the only connected subsets of $S(\mathscr{A})$ are single points; and no, the empty space is not connected).
(iii) Show that $\mathscr{A}$ is naturally isomorphic to the Boolean algebra of clopen subsets of $S(\mathscr{A})$.
(iv) Conversely, show that if S is a totally disconnected compact space and $\mathscr{A}$ is the Boolean algebra of clopen subsets of S, then $S \approx S(\mathscr{A})$.

The last two items say that we can go back and forth between Boolean algebras and totally disconnected compact topological spaces without losing any essential information. This is usually referred to as the *Stone duality*. It is frequently use in Mathematical Logic (e.g., in Model Theory).

EXERCISE 1.16. By the Completeness Theorem we have $\varphi \vdash \neg\neg\varphi$ for all φ. Show this directly (i.e., give a deduction sequence).

EXERCISE 1.17. Show that the two items of Theorem 1.3.16 are equivalent.

CHAPTER 2

First order Predicate Logic

Consider the following reasoning:

> Socrates is a dog.
> Every dog likes the circus.
> Therefore, Socrates likes the circus.

This is a valid logical argument, given in a natural language. However, we cannot translate this to propositional logic, since it lacks the ability to express that some property holds *for a individual*, or to say something like "for every individual". We could partially formalise the reasoning above as follows:

> Dog(Socrates).
> For all x (Dog(x) $\rightarrow$ LikesTheCircus(x)).
> Therefore LikesTheCircus(Socrates).

Here Dog() and LikesTheCircus() are what we call *predicates*, and saying "for all" is a *quantifier*. The symbol x is a variable which varies over a space of possible individuals.

Let us look at another example:

> The sum of every two positive numbers is positive.
> a and b are positive.
> Therefore $a + b$ is positive.

To formalise this example we also need a notion of *functions* (addition, in this case).

These are the essential ingredients of *predicate logic*. We will only study *first order* predicate logic, meaning we only quantify over individuals (and not, say, over sets of individuals).

2.1. Syntax

In order to define first order formulae we need to fix a vocabulary:

DEFINITION 2.1.1. A *signature* (sometimes called *language*) is a triplet $\mathcal{L} = \{\mathcal{R}, \mathcal{F}, \nu\}$, where $\mathcal{R} \cap \mathcal{F} = \varnothing$ and $\nu \colon \mathcal{R} \cup \mathcal{F} \rightarrow \mathbb{N}$.

We call the members of $\mathcal{R}$ *predicate symbols* or *relation symbols* and the members of $\mathcal{F}$ *function symbols*. For $R \in \mathcal{R}$ (or $f \in \mathcal{F}$), $\nu(R)$ (or $\nu(f)$) is the number of arguments the symbol takes, also called its *arity*. (So we have unary, binary, ternary, and in general n-ary symbols.)

Unless said otherwise, every signature contains a distinguished binary relation symbol for equality, denoted $=$.

A *constant symbol* is just another name for a 0-ary function symbol.

Informally, we will usually identify $\mathcal{L}$ with $\mathcal{R} \cup \mathcal{F}$: so a signature is simply a collection of symbols, and we assume it is known for each symbol whether it is a predicate symbol of a function symbol, and what its arity is.

We also fix a set of *variables*. This will usually be a countable set denoted V. Variables will be denoted by x, y, z, etc.

Syntactic objects will be finite sequences of symbols in an alphabet consisting of:

- *Logical symbols:* parentheses, connectives, the two quantifiers $\forall$, $\exists$ and the variables. Sometimes the equality relation symbol is also considered a logical symbol.
- *Non-logical symbols (depending on the signature $\mathcal{L}$):* all relation and function symbols (except for equality).

Fix a signature $\mathcal{L}$. We first define $\mathcal{L}$-terms by induction:

DEFINITION 2.1.2. We define *$\mathcal{L}$-terms* recursively:

(i) A variable x is a term.
(ii) If $t_0, \ldots, t_{n-1}$ are terms, and f is an n-ary function symbol then $ft_0 \ldots t_{n-1}$ is a term.

Note that this means that a constant symbol c is a term.

The set of all $\mathcal{L}$-terms will be denoted by $\mathcal{T}_{\mathcal{L}}$.

Now we define $\mathcal{L}$-formulae:

DEFINITION 2.1.3.
(i) If $t_0, \ldots, t_{n-1}$ are terms, and R is an n-ary predicate symbol, then $Rt_0 \ldots t_{n-1}$ is an *atomic formula*.
(ii) If φ and ψ are formulae, then so are $(\neg\varphi)$, $(\varphi \to \psi)$, $(\varphi \wedge \psi)$ and $(\varphi \vee \psi)$.
(iii) If φ is a formula and x a variable then $(\forall x\, \varphi)$ and $(\exists x\, \varphi)$ are formulae. The symbols $\forall$ and $\exists$ are called the universal and existential quantifiers, respectively.

The set of all $\mathcal{L}$-formulae is denoted by $\mathcal{L}_{\omega,\omega}$.

What we defined above is the *formal* notation, for which we prove unique reading etc. Note that it uses Polish (i.e., prefix) notation for function and predicate symbols. In real life it may be convenient to divert somewhat from formal notation, as long as no ambiguities arise:

- We may add parentheses, and write $f(t_0, t_1, \ldots)$ instead of $fx_0x_1 \ldots$.
- If f is a binary function symbol we may write $(t_1\ f\ t_2)$ rather than ft_1t_2, and similarly for relation symbols (so we write $(t_0 + t_1)$, $(t_0 = t_1)$, etc.)
- If R is a binary relation symbol, we may further write $(t_0\ \not R\ t_1)$ as shorthand for $\neg Rt_0t_1$.

EXAMPLE 2.1.4. The signature (or language) of rings is $\mathcal{L}_{ring} = \{0, 1, -, +, \cdot\}$, where 0 and 1 are constant symbols, $-$ is a unary function symbol, and $+$ and $\cdot$ are binary function symbols.

In this language $x + y$ and $(x \cdot x) \cdot (-y)$ are terms, and $x \cdot x = y$, $\exists y\, y \cdot y = -1$ are formulae.

An occurrence of a variable in a formula can be either a part of a quantifier ($\forall x$ or $\exists x$) or a part of a term. An occurrence of the second kind is either *bound* to a corresponding quantifier, or else it is *free*.

DEFINITION 2.1.5.
- If φ is an atomic formula, all occurrences of variables in φ are free.
- If $\varphi = \psi \to \chi$ then all bound variable occurrences in either ψ or χ are bound in φ to the same quantifier, and all free occurrences in ψ or χ are free in φ. Similarly with other connectives.
- If $\varphi = \forall x \psi$ (or $\exists x \psi$) then all bound variables in ψ are also bound in φ to the same quantifier. All free occurrences of x in ψ are bound in φ to the outermost quantifier. All free occurrences of other variables in ψ are free in φ.

A variable x is *free* in φ if it has a free occurrence in φ; it is *bound* in φ if a quantifier $\forall x$ or $\exists x$ appears in φ. The sets of free and bound variables of φ are denoted by $\mathrm{fvar}(\varphi)$ and $\mathrm{bvar}(\varphi)$, respectively.

A formula without free variables is called a *sentence*.

Note that while an occurrence of a variable in φ is either free, bound, or part or a quantifier, a variable may be both free and bound, or neither.

If t is a term we may use $\mathrm{fvar}(t)$ to denote the set of all the variables occurring in t (which are by convention all free).

A finite tuple of variables $x_0, \ldots, x_{n-1}$ may be denoted by $\bar{x}$, or more explicitly by $x_{<n}$.

NOTATION 2.1.6. Let $\bar{x} = x_0, \ldots, x_{n-1}$ be a tuple of *distinct* variables. When we write a formula φ as $\varphi(\bar{x})$, this means that all the free variables of φ are among $x_0, \ldots, x_{n-1}$.

Similar notation holds for terms.

Thus "let $\varphi(\bar{x}) \in \mathcal{L}_{\omega,\omega}$" is a short way of saying "let φ be a formula all of whose free variables belong to the tuple $\bar{x}$".

If we write a formula as $\varphi(x_0, \ldots, x_{n-1})$, it may happen that some of the x_i are not free in φ, in which case they are called *dummy variables*.

2.2. Semantics

In the same manner that a truth assignment was an interpretation of a propositional vocabulary, we would like to define interpretations of signatures in predicate logic. Such an interpretation will consist of two parts: First, we need to interpret the quantifiers,

i.e., say what is the universe of possible "individuals". Then we need to interpret each predicate (function) symbol as an actual predicate (function) on this universe.

Fix a signature $\mathcal{L}$.

DEFINITION 2.2.1. An *$\mathcal{L}$-structure* $\mathfrak{M}$ consists of:

(i) A non-empty set M called its *domain*.
(ii) For every n-ary predicate symbol $R \in \mathcal{L}$, an n-ary relation $R^{\mathfrak{M}} \subseteq M^n$. (We understand $R^{\mathfrak{M}}$ as the set of n-tuples in M which satisfy the predicate R.)
The predicate symbol $=$ is always interpreted as equality in M, so $=^{\mathfrak{M}}$ is always the diagonal $\{(a,a) : a \in M\}$.
(iii) For every n-ary predicate symbol $f \in \mathcal{L}$, an n-ary function $f^{\mathfrak{M}} : M^n \to M$.

We will usually use uppercase Gothic letters $\mathfrak{M}$, $\mathfrak{N}$, etc., to denote structures, and the corresponding Roman letters M, N, etc., to denote their domains.

Also, having enumerated a signature as $\mathcal{L} = \{R_0, R_1, \ldots, f_0, f_1, \ldots\}$, it is common to write $\mathcal{L}$-structures explicitly as $\mathfrak{M} = \langle M, R_0^{\mathfrak{M}}, R_1^{\mathfrak{M}}, \ldots, f_0^{\mathfrak{M}}, f_1^{\mathfrak{M}}, \ldots\rangle$.

EXAMPLE 2.2.2. Here are a few common mathematical structures, written as structures in the sense of predicate logic.

(i) The field of real numbers: $\langle \mathbb{R}, 0, 1, -, +, \cdot\rangle$ give as an $\mathcal{L}_{ring}$-structure.
(ii) The *ordererd* field of real numbers: $\langle \mathbb{R}, 0, 1, -, +, \cdot, \leq\rangle$. This is an $\mathcal{L}_{oring}$-structure, where $\mathcal{L}_{oring} = \mathcal{L}_{ring} \cup \{\leq\}$.
(iii) The natural numbers: $\langle \mathbb{N}, 0, s, +, \cdot\rangle$: here s the unary successor function. This structure will be of great interest to us later on in the course.
(iv) A module space over a fixed ring R: $\langle M, 0, -, +, m_a : a \in R\rangle$. Here m_a is the unary function of scalar multiplication by a. Notice that the ring is part of the language.

DEFINITION 2.2.3. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure, and let V denote the set of variables. An *assignment to the variables in* $\mathfrak{M}$, or simply an *$\mathfrak{M}$-assignment*, is a mapping $\sigma\colon V \to M$.

DEFINITION 2.2.4. If σ is an $\mathfrak{M}$-assignment, x is a variable and and $a \in M$, we define an $\mathfrak{M}$-assignment σ_x^a by:

$$\sigma_x^a(y) = \begin{cases} a & \text{if } y = x \\ s(y) & \text{if } y \neq x. \end{cases}$$

We first interpret terms:

DEFINITION 2.2.5. Let $\mathfrak{M}$ be a structure and σ and $\mathfrak{M}$-assignment. We define for every term t its value *in* $\mathfrak{M}$ *under the assignment* σ (or simply *in* M, σ), denoted $t^{\mathfrak{M},\sigma}$, by induction on t:

(i) If $t = x$ is a variable, then $x^{\mathfrak{M},\sigma} = \sigma(x)$.
(ii) Otherwise, $t = ft_0 \ldots t_{n-1}$, and we define $t^{\mathfrak{M},\sigma} = f^{\mathfrak{M}}(t_0^{\mathfrak{M},\sigma}, \ldots, t_{n-1}^{\mathfrak{M},\sigma})$.

We now give truth values to formulae:

DEFINITION 2.2.6. Let $\mathfrak{M}$ be a structure. For a formula φ and an $\mathfrak{M}$ assignment σ we define whether or not φ is true *in* $\mathfrak{M}$ *under* σ, denoted $M \vDash_\sigma \varphi$. We do this by induction on φ, simultaneously for all $\mathfrak{M}$-assignments σ:

(i) If $\varphi = Pt_0 \dots t_{n-1}$ is atomic:

$$\mathfrak{M} \vDash_\sigma \varphi \iff (t_0^{\mathfrak{M},\sigma}, \dots, t_{m-1}^{\mathfrak{M},\sigma}) \in P^{\mathfrak{M}}.$$

(ii) If φ is constructed from simpler formulas using connectives, we follow their truth tables as in propositional logic.

(iii) If $\varphi = \forall x\psi$ or $\varphi = \exists x\psi$:

$$\mathfrak{M} \vDash_\sigma \forall x\psi \iff \text{ for every } a \in M\text{: } \mathfrak{M} \vDash_{\sigma_x^a} \psi$$
$$\mathfrak{M} \vDash_\sigma \exists x\psi \iff \text{ there exists } a \in M \text{ such that: } \mathfrak{M} \vDash_{\sigma_x^a} \psi.$$

If Γ is a set of formulae, we say that $\mathfrak{M} \vDash_\sigma \Gamma$ if $\mathfrak{M} \vDash_\sigma \varphi$ for all $\varphi \in \Gamma$.

Once we have defined satisfaction of single formulae we may define:

DEFINITION 2.2.7 (Models). (i) Let Γ be a set of formulae, $\mathfrak{M}$ a structure and σ an $\mathfrak{M}$-assignment. Then $\mathfrak{M} \vDash_\sigma \Gamma$ if $\mathfrak{M} \vDash_\sigma \varphi$ for all $\varphi \in \Gamma$.

(ii) A *model* of a formula φ (or set of formulae Γ) is a pair $\mathfrak{M}, \sigma$ such that $\mathfrak{M} \vDash_\sigma \varphi$ (or $\mathfrak{M} \vDash_\sigma \Gamma$). We also say that the pair $\mathfrak{M}, \sigma$ *models* φ (or Γ).

We may now define logical consequence as in Propositional Logic:

DEFINITION 2.2.8 (Logical consequence and equivalence). Let φ be a formula, Γ a set of formulae. We say that φ is a *logical consequence* of Γ, or that Γ *logically implies* φ, in symbols $\Gamma \vDash \varphi$, if every model of Γ is a model of φ.

If φ and ψ are two formulae such that $\varphi \vDash \psi$ and $\psi \vDash \varphi$ we say that φ and ψ are *logically equivalent*, denoted $\varphi \equiv \psi$.

Thus, for example, the formula $z = x + y$ is a logical consequence of the two formulae $z = y + x$ and $\forall t \forall w\, (t + w = w + t)$.

DEFINITION 2.2.9. A formula φ is *valid* if it is true in every structure and under every assignment, i.e., if $\vDash \varphi$.

Of course, a formula or term only depend on the values assigned to their free variables:

LEMMA 2.2.10. *Let $\mathfrak{M}$ be a structure and σ, σ' two $\mathfrak{M}$-assignments.*

(i) *For every term t, if $\sigma\restriction_{\mathrm{fvar}(t)} = \sigma'\restriction_{\mathrm{fvar}(t)}$ then*

$$t^{\mathfrak{M},\sigma} = t^{\mathfrak{M},\sigma'}.$$

(ii) *For every formula φ, if $\sigma\restriction_{\mathrm{fvar}(\varphi)} = \sigma'\restriction_{\mathrm{fvar}(\varphi)}$ then*

$$\mathfrak{M} \vDash_\sigma \varphi \iff \mathfrak{M} \vDash_{\sigma'} \varphi.$$

We may therefore introduce a new notation:

NOTATION 2.2.11. Let $\mathfrak{M}$ be a structure, $\bar{a} \in M^n$. Let $t(x_{<n})$ and $\varphi(x_{<n})$ be a term and a formula, respectively. Let $\sigma\colon V \to M$ be an $\mathfrak{M}$-assignment satisfying $\sigma(x_i) = a_i$ for all $i < n$. Then we write $t^{\mathfrak{M}}(\bar{a})$ instead of $t^{\mathfrak{M},\sigma}$, and $\mathfrak{M} \vDash \varphi(\bar{a})$ instead of $\mathfrak{M} \vDash_\sigma \varphi$.

By the previous Lemma, this does not depend on the choice of σ.

In particular, if φ is a sentence, then either $\mathfrak{M} \vDash \varphi$ or not (no free variables that require an assignment). We may therefore speak of structures as being *models* of sentences, or of sets of sentences, without mentioning assignments.

EXAMPLE 2.2.12. Let $\mathcal{L} = \{0, 1, -, +, \cdot\}$, and consider $\mathbb{R}$ and $\mathbb{Z}$ as $\mathcal{L}$-structures with the natural interpretation of the symbols. Let $t(x, y) = x + y^2 + 1$ (y^2 is just shorthand for $y \cdot y$). Then $t^{\mathbb{R}}(3, 5) = tx^{\mathbb{Z}}(3, 5) = 29$. Similarly, let $\varphi(x) = \exists y\,(y^2 = x)$. Then $\mathbb{R} \vDash \varphi(5) \wedge \neg\varphi(-1)$ and $\mathbb{Z} \vDash \varphi(4) \wedge \neg\varphi(5)$.

Finally, in many situation we may wish to augment the language of a structure by interpreting new symbols, or to forget the interpretation of some symbols.

DEFINITION 2.2.13. Let $\mathcal{L} \subseteq \mathcal{L}'$ be two signatures. Let $\mathfrak{M}'$ be an $\mathcal{L}'$-structure, and let $\mathfrak{M}$ be the $\mathcal{L}$-structure obtained from $\mathfrak{M}'$ by "forgetting" the interpretations of the symbols in $\mathcal{L}' \setminus \mathcal{L}$ (i.e., the domains are the same, and $s^{\mathfrak{M}} = s^{\mathfrak{M}'}$ for every symbol $s \in \mathcal{L}$).

We then say that $\mathfrak{M}$ is the $\mathcal{L}$-*reduct* of $\mathfrak{M}'$, in symbols $\mathfrak{M} = \mathfrak{M}'\restriction_{\mathcal{L}}$, or that $\mathfrak{M}'$ is an *expansion* of $\mathfrak{M}$ to $\mathcal{L}'$.

Note that while the $\mathcal{L}$-reduct of $\mathfrak{M}'$ is unique, $\mathfrak{M}$ may have many expansions to $\mathcal{L}'$.

2.3. Substitutions

Let us again look at the example of the formula $\varphi(x) = \exists y\,(y^2 = x)$, saying "$x$ is a square". We can obtain a formula saying "$z + w$ is a square" from φ through free substitution (we substitute the term $z + w$ for the free variable x).

This is done in two stages. We first define substitutions in terms.

DEFINITION 2.3.1. Let t be a term and x a variable. We define the *substitution* of t for x inside another term t', denoted $t'[t/x]$, by induction on t':

(i) $y[t/x] = \begin{cases} t & y = x \\ y & y \neq x. \end{cases}$

(ii) $(ft_0 \dots t_{n-1})[t/x] = ft_0[t/x] \dots t_{n-1}[t/x]$.

The term substitution is a pure syntactic operation. Its semantic value is given by the following Lemma:

LEMMA 2.3.2. *Let $\mathfrak{M}$ be a structure and σ an $\mathfrak{M}$-assignment. Let t, t' be terms, x a variable, and $a = t^{\mathfrak{M},\sigma} \in M$. Then:*

$$(t'[t/x])^{\mathfrak{M},\sigma} = t'^{\mathfrak{M},\sigma^a_x}.$$

PROOF. By induction on t'. ■2.3.2

We can now define free substitution, i.e., substitution to free occurrences of a variable. If we are not careful, the result of a free substitution might not be what we expect; to avoid this we also need to make sure a free substitution is correct.

DEFINITION 2.3.3. Let t be a term and x a variable. We define the *free substitution* of t for x inside a formula φ, denoted $\varphi[t/x]$, by induction on φ. At the same time we also say whether the substitution is *correct*:

(i) Atomic formulae: $(Pt_0 \dots t_{n-1})[t/x] = Pt_0[t/x] \dots t_{n-1}[t/x]$. The substitution is always correct.
(ii) Connectives: $(\neg\psi)[t/x] = \neg\psi[t/x]$, $(\psi \to \chi)[t/x] = \psi[t/x] \to \chi[t/x]$, etc. The substitution is correct if the substitutions to the components are.
(iii) Quantifier, case I:

$$(Qx\,\psi)[t/x] = Qx\,\psi \qquad\qquad Q \in \{\forall, \exists\}.$$

The substitution is correct.
(iv) Quantifier, case II:

$$(Qy\,\psi)[t/x] = Qy\,(\psi[t/x]) \qquad\qquad Q \in \{\forall, \exists\},\ y \neq x.$$

The substitution is correct if:
(a) The substitution $\varphi[t/x]$ is correct; and
(b) The variable y does not appear in t.

The semantic meaning of free substitution is given by:

LEMMA 2.3.4. *Let $\mathfrak{M}$ be a structure and σ an $\mathfrak{M}$-assignment. Let t be a term, x a variable, φ a formula, and $a = t^{\mathfrak{M},\sigma} \in M$. Assume furthermore that the free substitution $\varphi[t/x]$ is correct. Then:*

$$\mathfrak{M} \vDash_\sigma \varphi[t/x] \iff \mathfrak{M} \vDash_{\sigma^a_x} \varphi.$$

PROOF. By induction on φ. For φ atomic this follows from Lemma 2.3.4. If φ is constructed from simpler formulae using connectives, this follows immediately from the induction hypothesis.

If $\varphi = \forall x\,\psi$ then $\varphi[t/x] = \varphi$. Also, $x \notin \operatorname{fvar}(\varphi)$ is not free in φ, so $\sigma\restriction_{\operatorname{fvar}\varphi} = (\sigma^a_x)\restriction_{\operatorname{fvar}(\varphi)}$. Therefore:

$$\mathfrak{M} \vDash_\sigma \varphi[t/x] \iff \mathfrak{M} \vDash_\sigma \varphi \iff \mathfrak{M} \vDash_{\sigma^a_x} \varphi.$$

Finally, assume that $\varphi = \forall y\,\psi$, $y \neq x$. By the correctness assumption, y does not appear in t. Therefore, for every $b \in M$: $t^{\mathfrak{M},\sigma} = t^{\mathfrak{M},\sigma^b_y}$. Also, as $y \neq x$: $(\sigma^a_x)^b_y = (\sigma^b_y)^a_x$,

and by the induction hypothesis:

$$\begin{aligned}\mathfrak{M} \vDash_\sigma \forall y\,(\psi[t/x]) &\iff \text{for all } b \in M\colon\ \mathfrak{M} \vDash_{\sigma_y^b} \psi[t/x]\\ &\iff \text{for all } b \in M\colon\ \mathfrak{M} \vDash_{(\sigma_y^b)_x^a} \psi\\ &\iff \text{for all } b \in M\colon\ \mathfrak{M} \vDash_{(\sigma_x^a)_y^b} \psi\\ &\iff \mathfrak{M} \vDash_{\sigma_x^a} \forall y\,\psi.\end{aligned}$$

The quantifier $\exists$ is treated similarly. ■2.3.4

EXAMPLE 2.3.5. Let $\varphi(x) = \exists y\,(y^2 = x)$.

(i) The free substitution $\varphi[z + w/x] = \exists y\,(y^2 = z + w)$ is correct, and says indeed that $z + w$ is a square.
(ii) On the other hand, the substitution $\varphi[z + y/x] = \exists y\,(y^2 = z + y)$ is incorrect, and indeed it does not say that $z + y$ is a square.

The problem in the second example is that φ contains quantification on y which also appears in the term $z + y$. But φ is logically equivalent (why?) to the formula $\varphi'(x) = \exists w\,(w^2 = x)$, and the substitution $\varphi'[z + y]$ is correct. This is a special case of bound substitution.

DEFINITION 2.3.6. Let φ be a formula, and x, y variables. The *bound substitution* of y for x in φ, denoted $\varphi\{y/x\}$, is defined as follows:

(i) Atomic formulae: $\varphi\{y/x\} = \varphi$, and the bound substitution is correct.
(ii) Connectives: $(\neg\varphi)\{y/x\} = \neg\varphi\{y/x\}$, $(\varphi \to \psi)\{y/x\} = \varphi\{y/x\} \to \psi\{y/x\}$, etc. The substitution is correct if the substitutions to the components are.
(iii) Quantifier, case I:

$$(Qx\,\varphi)\{y/x\} = Qy\,(\varphi[y/x]) \qquad\qquad Q \in \{\forall, \exists\}.$$

The bound substitution is correct if:
  (a) The variable y is not free in φ; and
  (b) The free substitution $\varphi[y/x]$ is correct.
(iv) Quantifier, case II:

$$(Qz\,\varphi)\{y/x\} = Qz\,(\varphi\{y/x\}) \qquad\qquad Q \in \{\forall, \exists\},\ z \neq x$$

The substitution is correct if $\varphi\{y/x\}$ is.

In other words, we look for something of the form $Qx\,(\ldots x \ldots)$ and replace it with $Qy\,(\ldots y \ldots)$.

LEMMA 2.3.7. *Assume that the bound substitution $\varphi\{y/x\}$ is correct. Then $\varphi \equiv \varphi\{y/x\}$.*

PROOF. By induction on φ. In case φ is atomic then $\varphi = \varphi\{y/x\}$ and there is nothing to prove. If φ is obtained from simpler formulae using connectives, then the results follows immediately from the induction hypothesis.

We are left with $\varphi = Qz\,\psi$, $Q \in \{\forall, \exists\}$.

(i) Assume $z = x$, i.e., $\varphi = Qx\,\psi$. Assume $Q = \forall$. Then $\varphi\{y/x\} = \forall y\,(\psi[y/x])$, y is not free in ψ, and the substitution $\psi[y/x]$ is correct. Therefore:

$$\mathfrak{M} \vDash \forall y\,(\psi[y/x]) \iff \text{for all } a \in M\colon\ \mathfrak{M} \vDash_{\sigma_y^a} \psi[y/x]$$

As $y^{\mathfrak{M},\sigma_y^a} = a$ and $\psi[y/x]$ is correct:

$$\iff \text{for all } a \in M\colon\ \mathfrak{M} \vDash_{(\sigma_y^a)_x^a} \psi$$

As y is not free in ψ:

$$\begin{aligned}&\iff \text{for all } a \in M\colon\ \mathfrak{M} \vDash_{\sigma_x^a} \psi\\ &\iff \mathfrak{M} \vDash_\sigma \forall x\,\psi.\end{aligned}$$

The case $Q = \exists$ is proved identically.

(ii) Assume $z \neq x$. Then $\varphi\{y/x\} = Qz\,(\psi\{y/x\})$, and by the induction hypothesis $\psi\{y/x\} \equiv \psi$, whereby $Qz\,\psi \equiv Qz\,(\psi\{y/x\})$.

■2.3.7

Finally, we observe that if we substitute a new variable then the substitution is correct and reversible:

LEMMA 2.3.8. *Let x, y be two distinct variables. Let t and φ be a term and a formula, respectively, in which y does not appear. Then:*

$$\begin{aligned}(t[y/x])[x/y] &= t,\\ (\varphi[y/x])[x/y] &= \varphi,\\ (\varphi\{y/x\})\{x/y\} &= \varphi,\end{aligned}$$

and all the substitutions above are correct.

PROOF. Exercise. ■2.3.8

Bound substitution allows us to rectify an incorrect free substitution:

LEMMA 2.3.9. *Let φ be a formula, and $x_0, \ldots, x_{n-1}$ a finite sequence of variables. Then by a finite sequence of correct bound substitutions we can transform into a formula φ' such that $\varphi \equiv \varphi'$ and there is no quantification on any of the x_i in φ'.*

PROOF. Let $\varphi_0 = \varphi$. Assume we have constructed φ_j. If φ_j contains $\forall x_i$ or $\exists x_i$ for some $i < n$, choose a variable y which does not appear in φ_j or on the list $x_0, \ldots, x_{n-1}$, and let $\varphi_{j+1} = \varphi_j\{y/x_i\}$. Otherwise, stop and let $\varphi' = \varphi_j$.

At each step the formula φ_{j+1} contains fewer occurrences of $\forall x_i$ and $\exists x_i$ $(i < n)$ than φ_j, so the process must stop. Since at each stage we substituted a new variable, all the substitutions were correct, and $\varphi_j \equiv \varphi_{j+1}$ for all j, whereby $\varphi \equiv \varphi'$. ■2.3.9

NOTATION 2.3.10. Let $\varphi(x, \bar{y})$ be a formula, t a term. If the substitution $\varphi[t/x]$ is correct, we define $\varphi(t, \bar{y}) = \varphi[t/x]$.

If the substitution is incorrect we use the previous lemma to choose φ' obtained from φ by a series of bound substitutions, such that all the variables appearing in t are not bound in φ'. Then we define $\varphi(t, \bar{y}) = \varphi'[t/x]$, and the substitution is correct.

Note that the choice of φ' is somewhat arbitrary. We have though:

LEMMA 2.3.11. *Let $\mathfrak{M}$ be a structure and σ an $\mathfrak{M}$-assignment. Let $t(z_{<n})$ be a term and $\varphi(x, y_{<m})$ a formula such that t and φ have no common variables, and let $\psi(\bar{y}, \bar{z}) = \varphi(t, \bar{y})$. Let $\bar{b} \in M^m$, $\bar{c} \in M^n$ and $a = t^{\mathfrak{M}}(\bar{c}) \in M$. Then:*

$$\mathfrak{M} \vDash \psi(\bar{b}, \bar{c}) \iff \mathfrak{M} \vDash \varphi(a, \bar{b}).$$

PROOF. This is just a special case of Lemma 2.3.4. $\blacksquare_{2.3.11}$

Under the assumptions of Lemma 2.3.11 is will be legitimate to denote $\psi(\bar{y}, \bar{z})$ by $\varphi(t(\bar{z}), \bar{y})$, and accordingly denote the property $\mathfrak{M} \vDash \psi(\bar{b}, \bar{c})$ by $\mathfrak{M} \vDash \varphi(t(\bar{c}), \bar{b})$.

If particular, if we go back to our example of $\varphi(x) = \exists y\,(y^2 = x)$, we have $\varphi(z+w) = \exists y\,(y^2 = z + w)$, but also $\varphi(z + y) = \exists u\,(u^2 = z + y) = \varphi\{u/y\}[z + y/x]$. Both have the intended meaning.

2.4. Syntactic deduction

We seek to understand notions such as logical implication. Direct verification of logical implication (i.e., that $\Gamma \vDash \varphi$) would consist of going over all possible truth assignments (in Propositional Logic) or structures (in Predicate Logic), checking which are models of Γ, and whether they are also models of φ. This can be done in a finite amount of time in Propositional Logic when Γ is finite, since then we only need to consider truth assignments to finitely many propositional variables (but not if it is infinite, although we can wiggle our way out of this using the Compactness Theorem).

However, *direct verification of logical implication in Predicate Logic is entirely unfeasible*, for several reasons. First, we would have to consider all possible $\mathcal{L}$-structures, and all possible assignments to such structures. Second, even within a single structure, checking satisfaction of a formula of the form $\forall x\,\varphi$ may require an infinite amount of time (as we need to test satisfaction of φ for every possible value for x). Testing satisfaction for a formula of the form $\forall x \exists y\,\varphi$ would be even worse, and we can write formulae which are far more complex.

On the other hand, a complete (and sound) deduction system for Predicate Logic would allow us to reduce logical implication to formal deduction, and verifying whether a sequence of formulae is a deduction sequence or not is a relatively easy (and finite) task.

In order to keep syntax as simple as possible, we will convene that:

CONVENTION 2.4.1. In this section all formulae only contain the connectives $\neg, \rightarrow$ and the quantifier $\forall$.

As we know how to find for every formula φ an equivalent formula φ' which is in this form, we do not lose any generality by this convention.

We will now introduce a deduction system as we did for Propositional Logic. In particular, it will consist of a single inference rule, Modus Ponens. Its logical axioms will be given by schemes, divided in several group. If φ is an instance of a scheme then φ, as well as any formula of the form $\forall x \forall y \ldots \varphi$ is a logical axiom. (In other words, if φ is a logical axiom and x is a variable, then $\forall x\, \varphi$ is a logical axiom as well.)

The first group consists of the logical axioms of Propositional Logic. It only deals with connectives:

(A1) $\varphi \to (\psi \to \varphi)$,

(A2) $((\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)))$,

(A3) $((\neg\varphi \to \psi) \to ((\neg\varphi \to \neg\psi) \to \varphi))$.

The second group of axioms deals with quantification:

(A4) $(\forall x\, (\varphi \to \psi)) \to ((\forall x\, \varphi) \to (\forall x\, \psi))$

(A5) $\varphi \to (\forall x\, \varphi)$ if x is not free in φ

(A6) $(\forall x\, \varphi) \to \varphi[t/x]$ if the substitution is correct.

The third group deals with equality. It is only present in languages with equality, (i.e., almost always):

(A7) $x = x$

(A8) $(x = y) \to (y = x)$

(A9) $(x = y) \to ((y = z) \to (x = z))$

(A10) $(x = y) \to (f\bar{z}x\bar{w} = f\bar{z}y\bar{w})$ $|\bar{z}| + |\bar{w}| + 1 = \nu(f)$

(A11) $(x = y) \to (P\bar{z}x\bar{w} \to P\bar{z}y\bar{w})$ $|\bar{z}| + |\bar{w}| + 1 = \nu(P)$.

Deduction sequences and the deduction relation $\vdash$ are defined as in every deduction system.

FACT 2.4.2. *This proof system is sound.*

PROOF. Exercise. ■2.4.2

Having the first group of logical axiom schemes and Modus Ponens as an only inference rule implies that many results from Section 1.3 hold in this deduction system, *with the same proof*. For example:

(i) The Deduction Theorem: $\Gamma, \varphi \vdash \psi \iff \Gamma \vdash \varphi \to \psi$.

(ii) If $\Gamma, \neg\varphi$ is contradictory then $\Gamma \vdash \varphi$.

(iii) If Γ is consistent, then at least one of Γ, φ or $\Gamma, \neg\varphi$ is.

(iv) Let Γ be a consistent set of formulae. Then there exists a maximal set consistent set of formulae $\Delta \supseteq \Gamma$. Moreover, for every formula φ either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$, and $\varphi \in \Delta \iff \Delta \vdash \varphi$.

In propositional logic, the was almost the end of the proof: once we have a maximal consistent set of propositional formulae, constructing a model for it was a trivial matter. Here this is just the beginning of our troubles.

In Predicate Logic, a model for a set of formulae is a structure, and the first thing we need in order to construct a structure is to choose its domain. A natural candidate for this is the term algebra of $\mathcal{L}$, which already comes equipped with interpretations of the function symbols:

DEFINITION 2.4.3. Recall that $\mathcal{T}$ denotes the set of all $\mathcal{L}$-terms. For every n-ary function symbol $f \in \mathcal{L}$ and $t_0, \ldots, t_{n-1} \in \mathcal{T}$ we define:

$$f^{\mathcal{T}}(t_0, \ldots, t_{n-1}) = f t_0 \ldots t_{n-1} \in \mathcal{T}.$$

The set $\mathcal{T}$ equipped with these interpretations of the function symbols is called the *term algebra* of $\mathcal{L}$.

There are still several issues (this should be viewed as an informal discussion):

(i) First assume that $\forall x\, \varphi(x) \in \Delta$. Then for every $t \in \mathcal{T}$ we would like to make sure that $\mathcal{T} \vDash \varphi(t)$. For this to be true we might think to apply A6: but what if the substitution $\varphi[t/x]$ is incorrect? Our discussion of bound substitutions in the previous section should take care of that.

(ii) Worse yet, assume $\neg\forall x\, \varphi(x) \in \Delta$. The we must find a term $t \in \mathcal{T}$ such that $\mathcal{T} \vDash \neg\varphi(t)$, i.e., that $\varphi[t/x] \in \Delta$. There is absolutely no reason to assume that such t exists. To make sure that it does exist we will use a trick called Henkin's method.

(iii) Finally, if we have the equality symbol in our language, we must make sure that it is interpreted as actual equality. Again, this needs not be true, but can be achieved by dividing by an appropriate equivalence relation.

We first deal with quantifiers.

Let us start by thinking how we usually prove universal statements (i.e., statements of the form "for all x, if $A(x)$ then $B(x)$"). Usually a proof would go as follows: we name one such x, assume that $A(x)$, and prove that $B(x)$; since we made no assumption about the identity of x, beyond that $A(x)$ holds, we conclude that $A(x) \to B(x)$ for all x. This method has a counterpart in formal deductions:

LEMMA 2.4.4 (The Generalisation Theorem). *Assume that $\Gamma \vdash \varphi$, and that x is not free in Γ. Then $\Gamma \vdash \forall x\, \varphi$.*

PROOF. Let $\psi_0, \ldots, \psi_{n-1}$ be a deduction sequence from Γ. We will prove by induction on $i < n$ that $\Gamma \vdash \forall x\, \psi_0$. We treat each $i < n$ according to cases:

(i) ψ_i is a logical axiom. Then $\forall x\, \psi_i$ is a logical axiom as well.

(ii) $\psi_i \in \Gamma$. Then x is not free in ψ_i, whereby we have an instance of A5: $\psi_i \to \forall x\, \psi_i$. It follows that $\Gamma \vdash \forall x\, \psi_i$.

(iii) ψ_i is obtained by Modus Ponens from ψ_j and $\psi_k = (\psi_j \to \psi_i)$, where $j, k < i$. By the induction hypothesis we have:

$$\Gamma \vdash \forall x\, \psi_j, \qquad \Gamma \vdash \forall x\, (\psi_j \to \psi_k)$$

By A4:

$$\Gamma \vdash (\forall x\, (\psi_j \to \psi_i)) \to ((\forall x\, \psi_j) \to (\forall x\, \psi_i))$$

Which put together yields:

$$\Gamma \vdash \forall x\, \psi_i$$ ■2.4.4

We have proved in Section 2.3 that if a bound substitution $\varphi\{y/x\}$ is correct then $\varphi \equiv \varphi\{y/x\}$. We can now prove a similar result, namely that we can actually deduce this equivalence in our proof system. To simplify the proof we will strengthen the assumption, assuming that y does not even appear in φ.

LEMMA 2.4.5. *Assume that φ is a formula in which y does not appear. Then $\vdash \varphi \to \varphi\{y/x\}$ and $\vdash \varphi\{y/x\} \to \varphi$. (Recall that by Lemma 2.3.8, the bound substitution is correct.)*

PROOF. We prove by induction on the complexity of φ.

(i) If φ is atomic then $\varphi\{y/x\} = \varphi$ and we know that $\vdash \varphi \to \varphi$.

(ii) If $\varphi = \neg\psi$, then $\varphi\{y/x\} = \neg\psi\{y/x\}$ and $\psi\{y/x\}$ is correct. We know from the Completeness Theorem for Propositional Logic that:

$$P \to P' \vdash \neg P' \to \neg P.$$

Substituting in a deduction sequence for this $P = \psi\{y/x\}$ and $P' = \psi$ for P', we get a deduction (which only uses A1-3) of

$$\psi\{y/x\} \to \psi \vdash \varphi \to \varphi\{y/x\}.$$

The opposite substitution yields:

$$\psi \to \psi\{y/x\} \vdash \varphi\{y/x\} \to \varphi.$$

The induction hypothesis tells us that $\vdash \psi \to \psi\{y/x\}$ and $\vdash \psi\{y/x\} \to \psi$, and we are done.

(iii) A similar argument works for $\varphi = \psi \to \chi$, this time using the fact that

$$P' \to P, Q \to Q' \vdash (P \to Q) \to (P' \to Q').$$

(iv) If $\varphi = \forall x\, \psi$, then $\varphi\{y/x\} = \forall y\, \psi[y/x]$, y is not free in ψ, and the substitution $\psi[y/x]$ is correct. Therefore we have an instance of A6: $\forall x\, \psi \to \psi[y/x]$, whereby $\forall x\, \psi \vdash \psi[y/x]$. Since y is not free in $\forall x\, \psi$, we have by the Generalisation

Theorem: $\forall x\,\psi \vdash \forall y\,\psi[y/x]$, i.e., $\varphi \vdash \varphi\{y/x\}$. We conclude that $\vdash \varphi \to \varphi\{y/x\}$ by the Deduction Theorem.

Since y does not appear in ψ, we have by Lemma 2.3.8 that $\psi = \psi'[x/y]$ and this substitution is correct as well. Also, clearly x is not free in $\psi[y/x]$ (by an easy inductive argument which we leave as an exercise). Since $\varphi = (\varphi\{y/x\})\{x/y\}$ (by Lemma 2.3.8), the mirror image of the above argument shows that $\vdash \varphi\{y/x\} \to \varphi$.

(v) If $\varphi = \forall z\,\psi$, where $z \neq x$, then $\varphi\{y/x\} = \forall z\,\psi\{y/x\}$, and the bound substitution $\psi\{y/x\}$ is correct. By the induction hypothesis we have $\vdash \psi \to \psi\{y/x\}$, and by the Generalisation Theorem: $\vdash \forall z\,(\psi \to \psi\{y/x\})$. Use an instance of A4: $\forall z\,(\psi \to \psi\{y/x\}) \to ((\forall z\,\psi) \to (\forall z\,\psi\{y/x\}))$, and apply Modus Ponens to conclude.

We obtain $\vdash \varphi\{y/x\} \to \varphi$ similarly.

■$_{2.4.5}$

We now have what we need to treat the case where $\forall x\,\varphi \in \Delta$:

LEMMA 2.4.6. *Assume that Δ is a maximal consistent set of formulae, $\forall x\,\varphi \in \Delta$, and $t \in \mathcal{T}$. Then there is a formula φ' such that $\varphi' \equiv \varphi$ and $\varphi'[t/x] \in \Delta$.*

PROOF. By Lemma 2.3.9 we can obtain a formula φ' through a sequence of correct bound substitutions, such that no variable of t is bound in φ'. Then $\vdash \varphi \to \varphi'$, and by the Generalisation Theorem $\vdash \forall x\,(\varphi \to \varphi')$. By A4 $\vdash (\forall x\,\varphi) \to (\forall x\,\varphi')$, so $\Delta \vdash \forall x\,\varphi'$. Finally, $\varphi'[t/x]$ is correct so by A6: $\Delta \vdash \varphi'[t/x]$. As Δ is maximal consistent: $\varphi'[t/x] \in \Delta$. ■$_{2.4.6}$

The next case is when $\neg\forall x\,\varphi \in \Delta$, and is more difficult: we need $t \in \mathcal{T}$ (as $\mathcal{T}$ is going to be the domain of our model) that would witness that $\neg\forall x\,\varphi$, i.e., such that $\neg\varphi[t/x] \in \Delta$, but there is no reason for such t to exist. We solve this through a process of artificially adding witnesses, due to Henkin.

We first need an auxiliary result, which is a modified version of the Generalisation Theorem for constant symbols. If c is a constant symbol and x a variable, we can define the substitution $\varphi[x/c]$ in the obvious way. Given the very limited fashion we will use this kind of substitution we will not worry about correctness.

LEMMA 2.4.7. *Assume that $\Gamma \vdash \varphi$, and c is a constant symbol which does not appear in Γ. Let x be a variable which does not appear in φ. Then $\Gamma \vdash \forall x\,\varphi[x/c]$.*

PROOF. Let $\varphi_0, \ldots, \varphi_{n-1}$ be a deduction sequence for φ from Γ, and let y be a variable not appearing in any formula on that sequence. We first claim that $\Gamma \vdash \varphi_i[y/c]$ for all $i < n$. If $\varphi_i \in \Gamma$ is a premise then $\varphi_i[y/c] = \varphi_i$ (since c does not appear in Γ), so $\Gamma \vdash \varphi_i[y/c]$. If φ_i is obtained from φ_j and $\varphi_k = (\varphi_j \to \varphi_i)$ by Modus Ponens, we need only observe that $\varphi_k[y/c] = (\varphi_j[y/c] \to \varphi_i[y/c])$, and use the induction hypothesis.

We are left with the case that φ_i is a logical axiom, and we wish to show that so it $\varphi_i[y/c]$. This is easily verified scheme by scheme. The only two cases where it is not completely trivial are:

- Scheme A5: $\varphi_i = \psi \to (\forall z\, \psi)$, and z is not free in ψ. Then $y \neq z$, so z is not free in $\psi[y/c]$. Therefore $\psi[y/c] \to (\forall z\, \psi[y/c])$ is an instance of A5.
- Scheme A6: $\varphi_i = (\forall z\, \psi) \to \psi[t/z]$, and $\psi[t/z]$ is correct. Then $y \neq z$, whereby:
$$(\psi[t/z])[y/c] = (\psi[y/c])[t[y/c]/z].$$
Also, since y does not appear in ψ, if only has free occurrences in $\psi[y/c]$ (but there are no quantifiers $\forall y$ in $\varphi[y/c]$), so the substitution $(\psi[y/c])[t[y/c]/z]$ is also correct. Therefore $\varphi_i[y/c]$ is also an instance of A6.

Same holds for instances of A5-6 preceded by universal quantifiers.

Let Γ_0 be the set of premises used in this deduction. Then $\Gamma_0 \vdash \varphi[y/c]$ and y is not free in Γ_0, so by the Generalisation Theorem $\Gamma_0 \vdash \forall y\, \varphi[y/c]$ and therefore $\Gamma \vdash \forall y\, \varphi[y/c]$. Finally, if $x \neq y$ then $(\forall y\, \varphi[y/c])\{x/y\} = \forall x\, \varphi[x/c]$ and x does not appear in $\forall y\, \varphi[y/c]$, so $\Gamma \vdash \forall x\, \varphi[x/c]$ by Lemma 2.4.5. ■2.4.7

Proposition 2.4.8. *Fix a signature $\mathcal{L}$. There exists a signature $\mathcal{L}^H \supseteq \mathcal{L}$, such that $\mathcal{L}^H \smallsetminus \mathcal{L}$ consists solely of constant symbols, and a set of $\mathcal{L}^H$ formulae Γ^H, such that:*

(i) *For every $\mathcal{L}^H$-formula φ and variable x there exists a constant symbol $c \in \mathcal{L}^H$ such that:*
$$(\neg\forall x\, \varphi) \to \neg\varphi[c/x] \in \Gamma^H.$$
(Note that the free substitution of a constant symbol is always correct).

(ii) *For every set of $\mathcal{L}$-formulae Γ, if Γ is consistent the so is $\Gamma \cup \Gamma^H$.*

Moreover, $|\mathcal{L}^H| = |\mathcal{L}| + \aleph_0$ (assuming, as we may, that there are only countable many variables.)

Proof. We define an increasing sequence of signatures $\mathcal{L}^H_n$ inductively. We start with $\mathcal{L}^{0,H} = \mathcal{L}$. Given $\mathcal{L}^{n,H}$, for every $\mathcal{L}^{n,H}$-formula φ and variable x we introduce a new constant symbol $c_{\varphi,x}$, and define:
$$\mathcal{L}^{n+1,H} = \mathcal{L}^{n,H} \cup \{c_{\varphi,x} \colon \varphi \in \mathcal{L}^{n,H}_{\omega,\omega}, x \in V\}.$$
We then define:
$$\begin{aligned}\mathcal{L}^H &= \bigcup_{n\in\mathbb{N}} \mathcal{L}^{n,H}\\ \psi_{\varphi,x} &= (\neg\forall x\, \varphi) \to \neg\varphi[c_{\varphi,x}/x]\\ \Gamma^H &= \{\psi_{\varphi,x} \colon \varphi \in \mathcal{L}^H_{\omega,\omega}, x \in V\}.\end{aligned}$$
Clearly Γ^H has the first property. We wish to prove the second.

Assume therefore that $\Gamma \subseteq \mathcal{L}_{\omega,\omega}$ is consistent, but Γ^H is not. Then there is a finite subset $\Gamma^H_0 \subseteq \Gamma^H$ such that $\Gamma \cup \Gamma^H_0$ is contradictory, and we may assume that Γ^H_0 is minimal such. Since Γ was assumed consistent, $\Gamma^H_0 \neq \varnothing$. Also, Γ^H_0 is of the form $\{\psi_{\varphi_i,x_i} \colon i < n\}$, where $\varphi_i \in \mathcal{L}^H_{\omega,\omega}$, and all the pairs (φ_i, x_i) are distinct. For each $i < n$ there is a minimal m_i such that $\varphi_i \in \mathcal{L}^{m_i,H}_{\omega,\omega}$, and without loss of generality m_0 is maximal among $\{m_i \colon i < n\}$.

Let $\varphi = \varphi_0$, $x = x_0$, $m = m_0 = \max\{m_i : i < n\}$. Then $\varphi_i \in \mathcal{L}^{m,H}_{\omega,\omega}$ for all $i < n$, but $c_{\varphi,x} \in \mathcal{L}^{m+1,H} \setminus \mathcal{L}^{m,H}$ (since m is minimal such that $\varphi \in \mathcal{L}^{m,H}_{\omega,\omega}$). Let $\Gamma^H_1 = \{\psi_{\varphi_i,x_i} : 0 < i < n\} = \Gamma_0 \setminus \{\psi_{\varphi,x}\}$, and $\Gamma_1 = \Gamma \cup \Gamma^H_1$. Then $c_{\varphi,x}$ does not appear in Γ_1: indeed, it does not appear in any φ_i, and $c_{\varphi,x} \neq c_{\varphi_i,x_i}$ for all $i > 0$.

Our assumption was that $\Gamma \cup \Gamma^H_0 = \Gamma_1 \cup \{(\neg\forall x\,\varphi) \to \neg\varphi[c_{\varphi,x}/x]\}$ is contradictory. Then *a fortiori* $\Gamma_1 \cup \{\neg\neg\forall x\,\varphi\}$ and $\Gamma_1 \cup \{\neg\varphi[c_{\varphi,x}/x]\}$ are contradictory, whereby $\Gamma_1 \vdash \neg\forall x\,\varphi$ and $\Gamma_1 \vdash \varphi[c_{\varphi,x}/x]$. Let y be a variable not appearing in φ. By Lemma 2.4.5:

$$\Gamma_1 \vdash \neg\forall x\,\varphi \Longrightarrow \Gamma_1 \vdash (\neg\forall x\,\varphi)\{y/x\} = \neg\forall y\,\varphi[y/x]$$

As $c_{\varphi,x}$ does not appear in Γ_1 we have by Lemma 2.4.7:

$$\Gamma_1 \vdash \varphi[c_{\varphi,x}/x] \Longrightarrow \Gamma_1 \vdash \forall y\,(\varphi[c_{\varphi,x}/x])[y/c_{\varphi,x}] = \forall y\,\varphi[y/x].$$

In other words, $\Gamma_1 = \Gamma \cup \Gamma^H_1$ is contradictory, contradicting the minimality of Γ^H_0. ■$_{2.4.8}$

We may now prove an intermediary result:

THEOREM 2.4.9 (Completeness Theorem for Predicate Logic without equality). *Let Γ be a set of formulae in a first order language $\mathcal{L}_{\omega,\omega}$ without equality (with only the connectives $\neg$ and $\to$ and the quantifier $\forall$). Then Γ is satisfiable if and only if it is consistent (in the deduction system given above).*

PROOF. If Γ is satisfiable then it is consistent by soundness. For the converse, assume that Γ is consistent. Let $\mathcal{L}^H \supseteq \mathcal{L}$ and Γ^H be as in Proposition 2.4.8. Then $\Gamma \cup \Gamma^H$ is consistent, and is therefore contained in a maximal consistent set $\Delta \subseteq \mathcal{L}^H_{\omega,\omega}$.

Let $\mathcal{T}$ be the term algebra of $\mathcal{L}^H$. We define an $\mathcal{L}$-structure $\mathfrak{M}$ whose domain is $M = \mathcal{T}$. We interpret the function symbols on M in the standard fashion:

$$f^{\mathfrak{M}} = f^{\mathcal{T}} : (t_0, \ldots, t_{n-1}) \mapsto f t_0 \ldots t_{n-1}.$$

For an n-ary predicate symbol P define:

$$P^{\mathfrak{M}} = \{(t_0, \ldots, t_{n-1}) \in M^n : Pt_0 \ldots t_{n-1} \in \Delta\}.$$

Once $\mathfrak{M}$ is defined we define an $\mathfrak{M}$-assignment σ by $\sigma(x) = x$ (here the variable x is both a variable and a member of M).

We claim without proof that for all $t \in \mathcal{T}$: $t^{\mathfrak{M},\sigma} = t$. We then prove that for all $\varphi \in \mathcal{L}^H_{\omega,\omega}$: $\mathfrak{M} \vDash_\sigma \varphi \Longleftrightarrow \varphi \in \Delta$, by induction on the number of quantifiers in φ, and for formulae with the same number of quantifiers, by induction on the complexity:

(i) If φ is atomic then we can prove what we want directly:

$$\begin{aligned} Pt_0 \ldots t_{n-1} \in \Delta &\Longleftrightarrow (t_0^{\mathfrak{M},\sigma}, \ldots, t_{n-1}^{\mathfrak{M},\sigma}) = (t_0, \ldots, t_{n-1}) \in P^{\mathfrak{M}} \\ &\Longleftrightarrow \mathfrak{M} \vDash_\sigma Pt_0 \ldots t_{n-1}. \end{aligned}$$

(ii) If $\varphi = \neg\psi$ then the induction hypothesis applies to ψ, which is simpler, and we conclude as in the proof of Theorem 1.3.16. Similarly if $\varphi = \psi \to \chi$.

(iii) Finally, assume $\varphi = \forall x\, \psi$. Each direction is handled separately. If $\forall x\, \psi \in \Delta$, then we need to show for all $t \in M$: $\mathfrak{M} \vDash_{\sigma_x^t} \psi$. But t is a term, and Lemma 2.4.6 tells us that under the circumstances there is a formula $\psi' \equiv \psi$ such that $\psi'[t/x] \in \Delta$, and the substitution is correct. As $\psi'[t/x]$ has fewer quantifiers than φ the induction hypothesis holds and $\mathfrak{M} \vDash_\sigma \psi'[t/x]$. Since the substitution is correct, and $t = t^{\mathfrak{M},\sigma}$: $\mathfrak{M} \vDash_\sigma \psi'[t/x] \iff \mathfrak{M} \vDash_{\sigma_x^t} \psi'$. Since $\psi' \equiv \psi$, this is further equivalent to $\mathfrak{M} \vDash_{\sigma_x^t} \psi$, which is what we wanted.

Conversely, assume $\forall x\, \psi \notin \Delta$, so $\neg\forall x\, \psi \in \Delta$. Since $\Gamma^H \subseteq \Delta$ we have $(\neg\forall x\, \psi) \to \neg\psi[c_{\psi,x}/x] \in \Delta$, whereby $\neg\psi[c_{\psi,x}/x] \in \Delta$. By the induction hypothesis:

$$\mathfrak{M} \vDash_\sigma \neg\psi[c_{\psi,x}/x]$$

And since $c_{\psi,x}^{\mathfrak{M},\sigma} = c_{\psi,x}$:

$$\mathfrak{M} \vDash_{\sigma_x^{c_{\varphi,x}}} \neg\psi$$

Whereby:

$$\mathfrak{M} \vDash_\sigma \neg\forall x\, \psi.$$

Therefore $\mathfrak{M} \vDash_\sigma \Delta$, and in particular $\mathfrak{M} \vDash_\sigma \Gamma$. ■2.4.9

The last thing to deal with is equality. The problem in the proof of Theorem 2.4.9 for a language with equality is that it may happen that $t \neq t'$ are two terms such that $(t = t') \in \Delta$, so $=^{\mathfrak{M}}$ does not coincide with actual equality in M. We can solve this through simple division by an equivalence relation.

Definition 2.4.10. Let $\mathcal{L}$ be a signature without equality, and $\mathfrak{M}$ and $\mathcal{L}$-structure. Let $\sim$ be a binary relation on M. We say that $\sim$ is a *congruence relation* for $\mathfrak{M}$ if it is an equivalence relation, and for every n-ary function symbol f or n-ary predicate symbol P, $a \sim b$ and $\bar{c}$, $\bar{d}$ in M such that $|\bar{c}| + |\bar{d}| + 1 = n$:

$$f^{\mathfrak{M}}(\bar{c}, a, \bar{d}) = f^{\mathfrak{M}}(\bar{c}, b, \bar{d}),$$
$$(\bar{c}, a, \bar{d}) \in P^{\mathfrak{M}} \iff (\bar{c}, b, \bar{d}) \in P^{\mathfrak{M}}.$$

Lemma 2.4.11. *Let $\mathcal{L}$ be a signature without equality, and $\mathfrak{M}$ and $\mathcal{L}$-structure. Let $\sim$ be a congruence relation for $\mathfrak{M}$. Let $\bar{M} = M/\!\sim$, and for $a \in M$ let $[a] \in \bar{M}$ denote the equivalence class $a/\!\sim$. Then there is a unique $\mathcal{L}$-structure $\bar{\mathfrak{M}}$ with domain $\bar{M}$ satisfying for every n-ary function symbol f or n-ary predicate symbol P and $\bar{a} \in M^n$:*

$$f^{\bar{\mathfrak{M}}}([a_0], \ldots, [a_{n-1}]) = [f^{\mathfrak{M}}(a_0, \ldots, a_{n-1})],$$
$$([a_0], \ldots, [a_{n-1}]) \in P^{\bar{\mathfrak{M}}} \iff (a_0, \ldots, a_{n-1}) \in P^{\mathfrak{M}}.$$

Moreover, let σ be an $\mathfrak{M}$-assignment, and $\bar{\sigma}$ the $\bar{\mathfrak{M}}$-assignment defined by $\bar{\sigma}(x) = [\sigma(a)]$. Then for every $\mathcal{L}$-formula φ and $\mathfrak{M}$-assignment σ:

$$\mathfrak{M} \vDash_\sigma \varphi \Longleftrightarrow \bar{\mathfrak{M}} \vDash_{\bar{\sigma}} \varphi.$$

We call $\bar{\mathfrak{M}}$ the quotient *of $\mathfrak{M}$ by $\sim$, denoted $\mathfrak{M}/\sim$, and may similarly denote $\bar{\sigma}$ by $\sigma/\sim$.*

PROOF. Exercise 2.13. ■2.4.11

LEMMA 2.4.12. *Assume that $\mathcal{L}$ is now a signature with equality, and Δ and $\mathfrak{M}$ are as in the proof of Theorem 2.4.9. Let $\tilde{\mathcal{L}}$ be a signature without equality, such that $\tilde{\mathcal{L}} = \mathcal{L}$ but $=\in \tilde{\mathcal{L}}$ is just an ordinary predicate symbol. Then $\mathfrak{M}$ is an $\tilde{\mathcal{L}}$-structure and $=^{\mathfrak{M}}$ is a congruence relation for $\mathfrak{M}$.*

PROOF. Since $\mathcal{L}$ is a language with equality, we have logical axiom schemes A7-11, and since Δ is maximal they all belong to Δ. In particular, the following sentences belong to Δ:

$$\begin{aligned}
&\forall x\, x = x \\
&\forall xy\, (x = y) \to (y = x) \\
&\forall xyz\, (x = y) \to ((y = z) \to (x = z)) \\
&\forall xy\bar{z}\bar{w}\, (x = y) \to (f\bar{z}x\bar{w} = f\bar{z}y\bar{w}) && |\bar{z}| + |\bar{w}| + 1 = \nu(f) \\
&\forall xy\bar{z}\bar{w}\, (x = y) \to (P\bar{z}x\bar{w} \to P\bar{z}y\bar{w}) && |\bar{z}| + |\bar{w}| + 1 = \nu(P).
\end{aligned}$$

They are therefore true in $\mathfrak{M}$, which means precisely that $=^{\mathfrak{M}}$ is a congruence relation. ■2.4.12

THEOREM 2.4.13 (Completeness Theorem for Predicate Logic). *Let Γ be a set of formulae and φ a formula in a first order language $\mathcal{L}_{\omega,\omega}$ (with only the connectives $\neg$ and $\to$ and the quantifier $\forall$). Then:*

(i) *The set Γ is satisfiable if and only if it is consistent (in the deduction system given above).*
(ii) $\Gamma \vDash \varphi \Longleftrightarrow \Gamma \vdash \varphi$.

PROOF. As usual we only prove the first item, and we only need to prove that if Γ is consistent then it is satisfiable.

If $\mathcal{L}$ is without equality, this has already been proved in Theorem 2.4.9. If $\mathcal{L}$ has equality, let $\Delta \supseteq \Gamma$, $\mathfrak{M}$ and σ be as in the proof of Theorem 2.4.9. Let $\tilde{\mathcal{L}}$ be the signature without equality obtained from $\mathcal{L}$ by making the equality symbol an ordinary predicate symbol. By Lemma 2.4.12, $\mathfrak{M}$ is a $\tilde{\mathcal{L}}$-structure and $=^{\mathfrak{M}}$ is a congruence relation. Let $\bar{\mathfrak{M}} = \mathfrak{M}/=^{\mathfrak{M}}$. Then for $[a], [b] \in \bar{M}$ we have:

$$[a] =^{\bar{f}M} [b] \Longleftrightarrow a =^{\mathfrak{M}} b \Longleftrightarrow [a] = [b].$$

This means that $=^{\bar{\mathfrak{M}}}$ coincides with equality, so $\bar{\mathfrak{M}}$ is actually an $\mathcal{L}$-structure, and by Lemma 2.4.11: $\bar{\mathfrak{M}} \vDash_{\bar{\sigma}} \Gamma$. ■2.4.13

COROLLARY 2.4.14 (Compactness Theorem for Predicate Logic). *Let Γ be a set of first order formulae and φ a formula. Then:*

(i) *Γ is satisfiable if and only if it is finitely satisfiable.*
(ii) *$\Gamma \vDash \varphi$ if and only if there is a finite subset $\Gamma_0 \subseteq \Gamma$ such that $\Gamma_0 \vDash \varphi$.*

PROOF. Follows from the finite nature of formal deduction. ■2.4.14

Exercises

EXERCISE 2.1. Recall that V denote the set of variables, $\mathcal{T}$ the set of terms, and $\mathcal{L}_{\omega,\omega}$ the set of first order formulae.

For each n-ary function symbol f define:

$$\begin{array}{rccc} \mathcal{E}_f\colon & \mathcal{T}^n & \to & \mathcal{T} \\ & \bar{t} & \mapsto & f\bar{t}. \end{array}$$

Similarly, for each n-ary predicate symbol P define:

$$\begin{array}{rccc} \mathcal{E}_P\colon & \mathcal{T}^n & \to & \mathcal{L}_{\omega,\omega} \\ & \bar{t} & \mapsto & P\bar{t}. \end{array}$$

Lastly, for each variable $x \in V$ define:

$$\begin{array}{rccc} \mathcal{E}_{\forall,x}\colon & \mathcal{L}_{\omega,\omega} & \to & \mathcal{L}_{\omega,\omega} \\ & \varphi & \mapsto & (\forall x\varphi) \end{array}, \qquad \begin{array}{rccc} \mathcal{E}_{\exists,x}\colon & \mathcal{L}_{\omega,\omega} & \to & \mathcal{L}_{\omega,\omega} \\ & \varphi & \mapsto & (\exists x\varphi) \end{array}.$$

Prove unique readability: $\mathcal{T}$ and $\mathcal{L}_{\omega,\omega}$ are disjoint; $\mathcal{T}$ is freely generated from V by the $\mathcal{E}_f$s; the operators $\mathcal{E}_P$ are injective with disjoint images, and $\mathcal{L}_{\omega,\omega}$ is freely generated from the images by the operators $\mathcal{E}_\square\colon \square \in \{\neg, \to, \vee, \wedge\}$ and $\mathcal{E}_{\forall,x}, \mathcal{E}_{\exists,x}\colon x \in V$.

EXERCISE 2.2. Let us consider another kind of substitution, which we may call *propositional substitution*. Let φ be a propositional formula in the (distinct) propositional variables $P_0, \ldots, P_{n-1}$, and let $\psi_0, \ldots, \psi_{n-1}$ be first order $\mathcal{L}$-formulae. We define $\varphi[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}]$ by replacing each occurrence of P_i in φ with ψ_i (a proper definition would be by induction on φ).

(i) Show that $\varphi[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}]$ is an $\mathcal{L}$-formula.
(ii) Let Γ be a set of propositional formulae, also all in $P_0, \ldots, P_{n-1}$, and let

$$\Gamma[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}] = \{\gamma[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}]\colon \gamma \in \Gamma\}.$$

Show that

$$\Gamma \vDash \varphi \Longrightarrow \Gamma[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}] \vDash \varphi[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}].$$

(iii) Use the previous item to show that if φ is valid then so is $\varphi[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}]$, and that:

$$\varphi \equiv \varphi' \Longrightarrow \varphi[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}] \equiv \varphi'[\psi_0/P_0, \ldots, \psi_{n-1}/P_{n-1}].$$

EXERCISE 2.3. As in Propositional Logic, define a *literal* of predicate logic to be an atomic formula or its negation, and define disjunctive normal form (DNF) accordingly. Prove that every quantifier-free formula is logically equivalent to one in DNF.

EXERCISE 2.4. Let T be a set of sentences. Define $\varphi \equiv_T \psi$ if $T \vDash \varphi \to \psi$ and $T \vDash \psi \to \varphi$.

(i) Let $\mathcal{L}_{\omega,\omega}(n)$ consist of the set of all formulae of the form $\varphi(x_0, \ldots, x_{n-1})$, and $\mathcal{L}_T(n) = \mathcal{L}_{\omega,\omega}(n)/\equiv_T$. Let the equivalence class $\varphi/\equiv_T$ be denoted by $[\varphi]_T$. Show that $\mathcal{L}_T(n)$ is naturally equipped with the structure of a Boolean algebra.

(ii) Show that the ordering on $\mathcal{L}_T(n)$ (as defined in Exercise 1.13) is given by $[\varphi]_T \leq [\psi]_T \iff T \vDash \varphi \to \psi$.

(iii) Let $i\colon \mathcal{L}_T(n) \hookrightarrow \mathcal{L}_T(n+1)$ denote the inclusion mapping (this is the addition of a dummy variable x_n). Show that for all $[\varphi]_T \in \mathcal{L}_T(n+1)$ there are unique equivalence classes $[\varphi']_T, [\varphi'']_T \in \mathcal{L}_T(n)$ such that for all $[\psi]_T \in \mathcal{L}_T(n)$:

$$i([\psi]_T) \leq [\varphi]_T \iff [\psi]_T \leq [\varphi']_T$$
$$[\varphi]_T \leq i([\psi]_T) \iff [\varphi'']_T \leq [\psi]_T.$$

How would you obtain $[\varphi']_T$ and $[\varphi'']_T$ explicitly from φ?

EXERCISE 2.5. State and prove the analogues of Exercise 1.10 and Exercise 1.11 for first order logic, replacing propositions with first order sentences and truth assignments with structures.

EXERCISE 2.6 (Reduced products). Let I be a set, which we view as a set of indices. Let $(\mathfrak{M}_i\colon i \in I)$ be a sequence of $\mathcal{L}$-structures indexed by I. Let $\mathscr{F}$ be a proper filter on I (i.e., on the Boolean algebra of subsets of I): we view subsets of I which belong to $\mathscr{F}$ as "big".

Let $N_0 = \prod_{i\in I} M_i$. We will denote members of N_0 by $(a_i\colon i \in I)$ (where $a_i \in M_i$) or just by (a_i). We interpret function symbols $f \in \mathcal{L}$ on N_0 coordinate-wise:

$$f^{\mathfrak{N}_0}((a_i), (b_i), \ldots) = (f^{\mathfrak{M}_i}(a_i, b_i, \ldots)).$$

With predicate symbols this are more delicate, and the filter $\mathscr{F}$ will be taken into account:

$$P^{\mathfrak{N}_0} = \big\{((a_i), (b_i), \ldots)\colon \{i \in I\colon (a_i, b_i, \ldots) \in P^{\mathfrak{M}_i}\} \in \mathscr{F}\big\}.$$

(Explanation: a tuple belongs to $P^{\mathfrak{N}_0}$ if its components belong to the corresponding $P^{\mathfrak{M}_i}$ on a "big" set of indices.)

In particular, the binary relation $=^{\mathfrak{N}_0}$ is defined as above. It is not necessarily equality, so $\mathfrak{N}_0$ is *not* a structure, according to our definitions. Nevertheless:

(i) Show that $=^{\mathfrak{N}_0}$ is an equivalence relation.

(ii) Show that $=^{\mathfrak{N}_0}$ is a congruence relation for every function $f^{\mathfrak{N}_0}$ (i.e., $(a_i) =^{\mathfrak{N}_0} (a'_i)$, $(b_i) =^{\mathfrak{N}_0} (b'_i)$, etc., imply that $f^{\mathfrak{N}_0}((a_i), (b_i), \ldots) =^{\mathfrak{N}_0} f^{\mathfrak{N}_0}((a'_i), (b'_i), \ldots)$.)

(iii) Show that $=^{\mathfrak{N}_0}$ is a congruence relation for every relation $P^{\mathfrak{N}_0}$ (i.e., $(a_i) =^{\mathfrak{N}_0} (a'_i)$, $(b_i) =^{\mathfrak{N}_0} (b'_i)$, etc., imply that $((a_i), (b_i), \ldots) \in P^{\mathfrak{N}_0} \iff ((a'_i), (b'_i), \ldots) \in P^{\mathfrak{N}_0}$.)

(iv) Show you can quotient $\mathfrak{N}_0$ by the equivalence relation $=^{\mathfrak{N}_0}$ to obtain an actual $\mathcal{L}$-structure $\mathfrak{N}$ whose domain N is equal to $N_0/=^{\mathfrak{N}_0}$. We will use the notation $[a_i] = [a_i \colon i \in I] \in N$ for the equivalence class of $(a_i) = (a_i \colon i \in I) \in N_0$.

We call this $\mathfrak{N}$ the *reduced product* of $(M_i \colon i \in I)$ modulo $\mathscr{F}$, denoted $\prod_{i\in I} M_i/\mathscr{F}$.

EXERCISE 2.7. Prove Lemma 2.3.2.

EXERCISE 2.8. Prove Lemma 2.3.8.

EXERCISE 2.9 (Prenex normal form). We say that a formula is in *prenex normal form*, or simply that it is a *prenex formula*, if it is of the form

$$Q_0 x_0 \, Q_1 x_1 \ldots Q_{n-1} x_{n-1} \, \varphi,$$

where each Q_i is either $\forall$ or $\exists$, the x_i are distinct variables, and φ is quantifier-free. Show that every first order formula is logically equivalent to a prenex formula.

EXERCISE 2.10 (Ultraproducts and Łoś's Theorem). Recall the construction of reduced products from Exercise 2.6. If $\mathscr{U}$ is an ultrafilter, then the reduced product $\prod_i \mathfrak{M}_i/\mathscr{U}$ is called an *ultraproduct*.

Prove Łoś's Theorem:

> Let $\{\mathfrak{M}_i \colon i \in I\}$ be structures, $\mathscr{U}$ an ultrafilter on I, and $\mathfrak{N} = \prod_i \mathfrak{M}_i$ the ultraproduct. Then for every formula $\varphi(x, y, \ldots) \in \mathcal{L}$, and $[a_i], [b_i], \ldots \in N$:
>
> $$\mathfrak{N} \vDash \varphi([a_i], [b_i], \ldots) \iff \{i \in I \colon \mathfrak{M}_i \vDash \varphi(a_i, b_i, \ldots)\} \in \mathscr{U}.$$
>
> In other words, if σ_i is an $\mathfrak{M}_i$-assignment for each $i \in I$ and τ is defined by $\tau(x) = [\sigma_i(x) \colon i \in I]$, then:
>
> $$\mathfrak{N} \vDash_\tau \varphi \iff \{i \in I \colon \mathfrak{M}_i \vDash_{\sigma_i} \varphi\} \in \mathscr{U}.$$

Hint: argue first why it suffices to show this for formulae which only use the connectives $\wedge$ and $\neg$, and the quantifier $\exists$, and prove by induction on such formulae.

(At some point you will need to use the Axiom of Choice which says that if you have a sequence $\{X_i \colon i \in I\}$ of non-empty sets then there exists a function $f \colon I \to \bigcup_{i\in I} X_i$ such that $f(i) \in X_i$ for all $i \in I$. If this remark seems obscure, it will become clearer when we speak about axioms for Set Theory.)

EXERCISE 2.11 (Compactness Theorem via Łoś's Theorem). Let Γ be a finitely satisfiable set of formulae. We will prove it is satisfiable in several steps:

(i) Let $I = \mathcal{P}^{fin}(\Gamma)$ be the family of all finite subsets of Γ. For $\Delta \in I$, let $J_\Delta = \{\Delta' \in I \colon \Delta \subseteq \Delta'\}$. Show that the family $\{J_\Delta \colon \Delta \in I\}$ is closed under finite intersections and does not contain $\varnothing$.

(ii) Let:

$$\mathscr{F} = \{J \subseteq I \colon (\exists \Delta \in I)(J \supseteq J_\Delta)\}.$$

Show that $\mathscr{F}$ is a proper filter on I.

(iii) Let $\mathscr{U}$ be an ultrafilter containing $\mathscr{F}$. Why is there one?
(iv) By assumption, for every $\Delta \in I$ there are $\mathfrak{M}_\Delta, \sigma_\Delta$ such that $\mathfrak{M}_\Delta \vDash_{\sigma_\Delta} \Delta$. Show that for every formula $\varphi \in \Gamma$:

$$\{\Delta \in I : \mathfrak{M}_\Delta \vDash_{\sigma_\Delta} \varphi\} \in \mathscr{U}.$$

(v) Let $\mathfrak{N} = \prod_{\Delta \in I} \mathfrak{M}_\Delta / \mathscr{U}$, and $\tau(x) = [\sigma_\Delta(x) : \Delta \in I] \in N$. Show that $\mathfrak{N} \vDash_\tau \Gamma$.

Exercise 2.12. Show that the proof system for predicate logic we introduced is sound.

Exercise 2.13. Prove Lemma 2.4.11.

CHAPTER 3

Model Theory

Model Theory is a branch of Mathematical Logic that studies the relation between properties of first order theories (i.e., sets of first order sentences) and more general properties of the classes of their models.

Fix a signature $\mathcal{L}$ (with equality). Unless said otherwise, all formulae, structures, etc., are in $\mathcal{L}$.

DEFINITION 3.0.15. (i) A *theory* T is a set of first order sentences, closed under logical implication (i.e., if $T \vDash \varphi$ then $\varphi \in T$).

(ii) A *complete* theory is one which is maximal consistent (equivalently: T is consistent and for every sentence φ either $\varphi \in T$ or $\neg\varphi \in T$).

(iii) If $\mathcal{K}$ is any class of structures, we define its *theory* as:

$$\mathrm{Th}(\mathcal{K}) = \{\varphi\colon \varphi \text{ is a sentence and } \mathfrak{M} \vDash \varphi \text{ for all } \mathfrak{M} \in \mathcal{K}\}.$$

If $\mathcal{K} = \{\mathfrak{M}\}$ consists of a single structure, we write $\mathrm{Th}(\mathfrak{M})$ instead of $\mathrm{Th}(\{\mathfrak{M}\})$. Note that $\mathrm{Th}(\mathfrak{M})$ is a complete theory, naturally called the *complete theory of* $\mathfrak{M}$.

DEFINITION 3.0.16. (i) Let T be a theory. We define the class of models of T as:

$$\mathrm{Mod}(T) = \{\mathfrak{M}\colon \mathfrak{M} \text{ is a structure and } \mathfrak{M} \vDash T\}.$$

(ii) A class of structures $\mathcal{K}$ is *elementary* if it is of the form $\mathcal{K} = \mathrm{Mod}(T)$ for some theory T.

With these definitions we can rephrase what we said earlier, saying that Model Theory studies relations between properties of elementary classes and properties of their theories. Let us give two examples whose proofs lie beyond the scope of this class.

A *cardinal* is a measure for the "size" of a set: 4, 17, 666, etc., are finite cardinals; $\aleph_0 = |\mathbb{N}| = |\mathbb{Q}|$ is the infinite countable cardinal (sometimes also denoted ω or ω_0); $\aleph = |\mathbb{R}| = |\mathbb{C}|$ is the *continuum*; and there are *many* others.

DEFINITION 3.0.17. Let κ be a cardinal. We say that a theory T is *κ-categorical* if it has a unique model of size κ up to isomorphism. In other words, if it has models of size κ, and all its models of size κ are isomorphic.

THEOREM 3.0.18 (Ryll-Nardzewski). *The following are equivalent for a complete theory T in a countable language $\mathcal{L}$:*

(i) *The theory T is $\aleph_0$-categorical.*
(ii) *For every n there are only finitely many formulae in n variables which are not equivalent modulo T (i.e., the Boolean algebra $\mathcal{L}_T(n)$ of Exercise 2.4 is finite for all n).*

THEOREM 3.0.19 (Morley, conjectured by Łoś). *The following are equivalent for a complete theory T in a countable language $\mathcal{L}$:*

(i) *The theory T is κ-categorical for some uncountable cardinal κ.*
(ii) *The theory T is κ-categorical for every uncountable cardinal κ.*

It should be pointed out that the proof of Morley's Theorem is in fact much more interesting than its statement: it involves proving that models of T admit a notion of independence, much like linear independence in vector spaces and algebraic independence in fields, and that every such model can be viewed as "generated" by a basis of independent elements (as in vector spaces). This served as a starting point for much of modern Model Theory one of whose main themes is notions of independence and their properties.

3.1. Elementary extensions and embeddings

DEFINITION 3.1.1. Let $\mathfrak{M}$ and $\mathfrak{N}$ be two structures, $\theta\colon M \to N$ a mapping. We say that θ is an *embedding*, in symbols $\theta\colon \mathfrak{M} \hookrightarrow \mathfrak{N}$, if for every n-ary predicate symbol P or function symbol n, and every $\bar{a} \in M$:

$$\theta(f^{\mathfrak{M}}(\bar{a})) = f^{\mathfrak{N}}(\theta(\bar{a}))$$
$$\bar{a} \in P^{\mathfrak{M}} \iff \theta(\bar{a}) \in P^{\mathfrak{N}}.$$

(Here $\theta(a_0, a_1, \ldots) = \theta(a_0), \theta(a_1), \ldots)$. If $M \subseteq N$ and the inclusion is an embedding, we say that $\mathfrak{M}$ is a *sub-structure* of $\mathfrak{N}$, or that $\mathfrak{N}$ is an *extension* of $\mathfrak{M}$, in symbols $\mathfrak{M} \subseteq \mathfrak{N}$.

LEMMA 3.1.2. *Let $\mathfrak{M}$ be an $\mathcal{L}$-structure and $\mathfrak{A} \subseteq \mathfrak{M}$ a subset. Then there exists a sub-structure $\mathfrak{A} \subseteq \mathfrak{M}$ whose underlying set is A if and only if A is closed under the interpretations in $\mathfrak{M}$ of the function symbols.*

PROOF. Exercise. ■3.1.2

LEMMA 3.1.3. *Let $\mathfrak{M}$ and $\mathfrak{N}$ be structures and $\theta\colon M \to N$ a mapping. Then the following are equivalent:*

(i) *θ is an embedding.*
(ii) *For every atomic formula $\varphi(\bar{x})$ and tuple $\bar{a} \in M$ (of the appropriate length):*
$$\mathfrak{M} \vDash \varphi(\bar{a}) \iff \mathfrak{N} \vDash \varphi(\theta(\bar{a})).$$
(iii) *For every quantifier-free formula $\varphi(\bar{x})$ and tuple $\bar{a} \in M$ (of the appropriate length):*
$$\mathfrak{M} \vDash \varphi(\bar{a}) \iff \mathfrak{N} \vDash \varphi(\theta(\bar{a})).$$

PROOF. Exercise 3.4. ■3.1.3

EXAMPLE 3.1.4. We have $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, all viewed as structures in $\mathcal{L}_{ring} = \{0, 1, +, -, \cdot\}$.

Plain embeddings (or extensions) are not enough for us, and we "prefer" to consider ones which preserve the entire first order language:

DEFINITION 3.1.5. Let $\mathfrak{M}$ and $\mathfrak{N}$ be structures and $\theta\colon M \to N$ a mapping. We say that θ is an *elementary embedding* if for every first order formula $\varphi(\bar{x})$ and tuple $\bar{a} \in M$ (of the appropriate length):

$$\mathfrak{M} \vDash \varphi(\bar{a}) \iff \mathfrak{N} \vDash \varphi(\theta(\bar{a})).$$

If $M \subseteq N$ and the inclusion is an elementary embedding, we say that $\mathfrak{M}$ is an *elementary sub-structure* of $\mathfrak{N}$, or that $\mathfrak{N}$ is an *elementary extension* of $\mathfrak{M}$, in symbols $\mathfrak{M} \preceq \mathfrak{N}$.

While it is relatively straightforward to verify that one structure is an extension of another, verifying that it is an elementary extension is much more difficult. Of course, in order to verify an extension is *not* elementary a single counterexample suffices.

EXAMPLE 3.1.6. None of the inclusions $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is elementary.

PROOF. Let $\varphi(x)$ be the formula $\exists y\,(y + y = x)$. Then $\mathbb{Z} \vDash \neg\varphi(1)$ when all of the other structures satisfy $\varphi(1)$. This shows that $\mathbb{Z}$ is not an elementary substructure of either $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The rest is left as an exercise. ■3.1.6

The existence of (elementary) embeddings from one structure to another is closely related to the notion of a diagram. Recall the notion of expansion from Definition 2.2.13.

DEFINITION 3.1.7. Let $\mathcal{L}$ be a signature and A a set. We define $\mathcal{L}(A) = \mathcal{L} \cup \{c_a\colon a \in A\}$, where each c_a is a new distinct constant symbol.

This will almost exclusively be used in a situation where $\mathfrak{M}$ is an $\mathcal{L}$-structure and $A \subseteq M$. In that case $\mathfrak{M}$ has a natural expansion to an $\mathcal{L}(A)$-structure by interpreting each c_a by a, and we will identify $\mathfrak{M}$ with this expansion.

To simplify notation, if $\bar{a} = a_0, \ldots, a_{n-1} \in A^n$, we will write $c_{\bar{a}}$ for $c_{a_0}, \ldots, c_{a_{n-1}}$. Notice that an (atomic) $\mathcal{L}(A)$-sentence is always of the form $\varphi(c_{\bar{a}})$ where $\varphi(\bar{x})$ is an (atomic) $\mathcal{L}$-formula and $\bar{a} \in A$.

DEFINITION 3.1.8. Let $\mathfrak{M}$ be a $\mathcal{L}$-structure. The *atomic diagram* and *elementary diagram* of $\mathfrak{M}$, respectively, are the following two sets of $\mathcal{L}(M)$-sentences:

$$\begin{aligned} D_{at}(\mathfrak{M}) = &\{\varphi\colon \varphi \in \mathcal{L}(M)_{\omega,\omega} \text{ is an atomic sentence and } \mathfrak{M} \vDash \varphi\} \\ &\cup \{\neg\varphi\colon \varphi \in \mathcal{L}(M)_{\omega,\omega} \text{ is an atomic sentence and } \mathfrak{M} \vDash \neg\varphi\} \\ = &\{\varphi(c_{\bar{a}})\colon \varphi(\bar{x}) \in \mathcal{L}_{\omega,\omega} \text{ is an atomic formula and } \mathfrak{M} \vDash \varphi(\bar{a})\} \\ &\cup \{\neg\varphi(c_{\bar{a}})\colon \varphi(\bar{x}) \in \mathcal{L}_{\omega,\omega} \text{ is an atomic formula and } \mathfrak{M} \vDash \neg\varphi(\bar{a})\} \\ D_{el}(\mathfrak{M}) = &\operatorname{Th}_{\mathcal{L}(M)}(\mathfrak{M}) \\ = &\{\varphi\colon \varphi \in \mathcal{L}(M)_{\omega,\omega} \text{ is a sentence and } \mathfrak{M} \vDash \varphi\} \\ = &\{\varphi(c_{\bar{a}})\colon \varphi(\bar{x}) \in \mathcal{L}_{\omega,\omega} \text{ is a formula and } \mathfrak{M} \vDash \varphi(\bar{a})\}. \end{aligned}$$

PROPOSITION 3.1.9. *Let $\mathfrak{M}$ and $\mathfrak{N}$ be $\mathcal{L}$-structure.*

(i) *There is a natural bijection between embeddings of $\mathfrak{M}$ in $\mathfrak{N}$ and expansions $\mathfrak{N}'$ of $\mathfrak{N}$ to $\mathcal{L}(M)$ such that $\mathfrak{N}' \vDash D_{at}(\mathfrak{M})$.*
(ii) *There is a natural bijection between elementary embeddings of $\mathfrak{M}$ in $\mathfrak{N}$ and expansions $\mathfrak{N}'$ of $\mathfrak{N}$ to $\mathcal{L}(M)$ such that $\mathfrak{N}' \vDash D_{el}(\mathfrak{M})$.*

PROOF. Let $\theta\colon \mathfrak{M} \to \mathfrak{N}$ be an embedding. Define an expansion $\mathfrak{N}'$ by $c_a^{\mathfrak{N}'} = \theta(a)$ for all $a \in M$. Then $\mathfrak{N}'$ is an $\mathcal{L}(M)$-structure and $\mathfrak{N}' \vDash D_{at}(\mathfrak{M})$. Conversely, if $\mathfrak{N}'$ is such an expansion, then defining $\theta(a) = c_a^{\mathfrak{N}'}$ for all $a \in M$ yields an embedding $\theta\colon \mathfrak{M} \to \mathfrak{N}$. The details and second item are left as an exercise. ■$_{3.1.9}$

DEFINITION 3.1.10 (Tarski-Vaught Test). Assume that $\mathfrak{M} \subseteq \mathfrak{N}$. We say that $\mathfrak{M}$ satisfies the *Tarski-Vaught test* in $\mathfrak{N}$ if for every formula $\varphi(\bar{x}, y) \in \mathcal{L}_{\omega,\omega}$, and for every tuple $\bar{a} \in M$ (of the same length as $\bar{x}$), if $N \vDash \exists y\, \varphi(\bar{a}, y)$ then there is $b \in M$ such that $N \vDash \varphi(\bar{a}, b)$. (Note that we only speak about satisfaction in N).

PROPOSITION 3.1.11 (Tarski-Vaught test). *Assume that $\mathfrak{M} \subseteq \mathfrak{N}$. Then $\mathfrak{M} \preceq \mathfrak{N}$ if and only if $\mathfrak{M}$ satisfies the Tarski-Vaught Test in $\mathfrak{N}$.*

PROOF. Left to right: Assume that $\mathfrak{M} \preceq \mathfrak{N}$ and $\mathfrak{N} \vDash \exists y\, \varphi(\bar{a}, y)$, where $\bar{a} \in M$. Then $\mathfrak{M} \vDash \exists y\, \varphi(\bar{a}, y)$ since $\mathfrak{M} \preceq \mathfrak{N}$, so there is $b \in M$ such that $\mathfrak{M} \vDash \varphi(\bar{a}, b)$, and again $\mathfrak{M} \preceq \mathfrak{N} \Longrightarrow \mathfrak{N} \vDash \varphi(\bar{a}, b)$.

Right to left: we prove that $\mathfrak{M} \vDash \varphi(\bar{a}) \Longleftrightarrow \mathfrak{N} \vDash \varphi(\bar{a})$ for every $\varphi \in \mathcal{L}_{\omega,\omega}$ and $\bar{a} \in M$, by induction on φ:

(i) φ atomic: since $\mathfrak{M} \subseteq \mathfrak{N}$.
(ii) φ constructed using connectives: as usual.
(iii) $\varphi(\bar{x}) = \exists y\, \psi(\bar{x}, y)$. Then

$$\mathfrak{M} \vDash \exists y\, \psi(\bar{a}, y) \Longleftrightarrow \exists b \in M \text{ such that } \mathfrak{M} \vDash \psi(\bar{a}, b)$$

By the induction hypothesis, if $\bar{a}, b \in M$ then $\mathfrak{M} \vDash \psi(\bar{a}, b) \Longleftrightarrow \mathfrak{N} \vDash \psi(\bar{a}, b)$, so:

$$\ldots \Longleftrightarrow \exists b \in M \text{ such that } \mathfrak{N} \vDash \psi(\bar{a}, b)$$

Since $\mathfrak{M}$ satisfies the Traski-Vaught test:

$$\ldots \Longleftrightarrow \mathfrak{N} \vDash \exists y\, \psi(\bar{a}, y) \qquad \blacksquare_{3.1.11}$$

We next prove the Löwenheim-Skolem theorems. Let us make a quick reminder about cardinalities:

We say that two sets A and B *have the same cardinality*, in symbols $|A| = |B|$, if there is a bijection (i.e., a one-to-one and onto mapping) from A to B. Intuitively, this means that A and B have the same size. The relation $|A| = |B|$ is an equivalence relation. The *cardinality* of A, denoted by $|A|$, is the equivalence class of A (this gives the notation $|A| = |B|$ a new meaning, but this new meaning coincides with the first one). Such an equivalence class is called a *cardinal*, and is usually denoted by lowercase Greek letters κ, λ, etc. The smallest infinite cardinal is $\aleph_0 = |\mathbb{N}| = |\mathbb{Q}|$.

We define sums and products as follows: If A and B are any two sets, then $|A| \cdot |B| = |A \times B|$ (where $A \times B = \{(a, b) : a \in A, b \in B\}$). If A and B are disjoint, then $|A| + |B| = |A \cup B|$. The finite cardinals (i.e., sizes of finite sets) can be identified with the natural numbers, and in this case addition and multiplication of cardinals and of natural numbers coincide.

Infinite sums are defined the same way: if $\{A_i : i \in I\}$ are all disjoint sets, then $\sum_{i\in I} |A_i| = |\bigcup_{i\in I} A_i|$. Infinite products can be defined similarly, but we shall avoid them. Classical commutative, associative and distributive laws hold. For example, the distributive law implies that

$$\sum_{i\in I} \kappa = \sum_{i\in I} 1 \cdot \kappa = \left(\sum_{i\in I} 1\right) \cdot \kappa = |I| \cdot \kappa.$$

The cardinals are ordered: $|A| \leq |B|$ if there is an injective (one-to-one) function from A to B, or equivalently if there is a surjective (onto) function from B to A. It is true (but requires a proof) that $|A| \leq |B| \wedge |B| \leq |A| \Longrightarrow |A| = |B|$. It is even less evident that for every two sets A and B, either $|A| \leq |B|$ or $|B| \leq |A|$; it is a consequence of the Axiom of Choice, which we accept as true (in fact, it is equivalent to the Axiom of Choice).

If at least one of κ and λ is infinite then $\kappa + \lambda = \max\{\kappa, \lambda\}$, and if both are non-zero then $\kappa \cdot \lambda = \max\{k, \lambda\}$. For infinite sums, the only rule we are going to use is that if $\kappa_i \leq \lambda_i$ for all $i \in I$ then $\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i$. Thus if $\kappa_i \leq \lambda$ for all $i \in I$ then $\sum_{i\in I} \kappa_i \leq |I| \cdot \lambda$.

Now Back to business. The upward Löwenheim-Skolem Theorem is a simple example of a very common manner in which the Compactness Theorem is applied.

THEOREM 3.1.12 (Upward Löwenheim-Skolem). *Let $\mathfrak{M}$ be an infinite $\mathcal{L}$-structure and κ a cardinal. Then there exists an elementary extension $\mathfrak{M} \preceq \mathfrak{N}$ such that $|N| \geq \kappa$. In other words, an infinite structure has arbitrarily big elementary extensions.*

PROOF. Let S be a set disjoint from M such that $\kappa = |S|$. Let Σ be the following set of $\mathcal{L}(M \cup S)$-sentences:

$$\Sigma = D_{el}(\mathfrak{M}) \cup \{c_s \neq c_{s'} : s \neq s' \in S\}.$$

We claim that Σ is finitely satisfiable. Indeed, let $\Sigma_0 \subseteq \Sigma$ be finite. Then there are finitely many $s \in S$ such that c_s appears in Σ_0, and let us enumerate them in a list $\{s_i : i < k\}$. Since M is infinite, we can find k distinct elements $a_0, \ldots, a_{k-1} \in M$. Let $\mathfrak{M}'$ be the expansion of $\mathfrak{M}$ to $\mathcal{L}(M \cup S)$ defined by first expanding $\mathfrak{M}$ to $\mathcal{L}(M)$ in the natural way, and then for $s \in S$:

$$c_s^{\mathfrak{M}'} = \begin{cases} a_i & s = s_i, i < k \\ a_0 & s \notin \{s_i : i < k\}. \end{cases}$$

Then $\mathfrak{M}' \models \Sigma_0$.

It follows by the Compactness Theorem that Σ is satisfiable and therefore has a model $\mathfrak{N}'$ with domain N. Let $\mathfrak{N} = \mathfrak{N}'|_{\mathcal{L}}$. The mapping $s \mapsto c_s^{\mathfrak{N}'}$ is injective, whereby $|N| \geq |S| = \kappa$. Also, since $\mathfrak{N} \models D_{el}(\mathfrak{M})$, there is an elementary embedding $\theta : \mathfrak{M} \to \mathfrak{N}$. By renaming the elements of $\mathfrak{M}$ we may assume that θ is an inclusion, whence $\mathfrak{M} \preceq \mathfrak{N}$ as required. ■3.1.12

In particular, a first order theory T with an infinite model $\mathfrak{M}$ cannot be categorical (i.e., has non-isomorphic models): indeed, let $\kappa > |M|$ (e.g., $\kappa = |\mathcal{P}(M)|$), and $\mathfrak{N} \succeq \mathfrak{M}$ such that $|N| \geq \kappa$. Then $N \models T$ (why?) and there can be no isomorphism between $\mathfrak{M}$ and $\mathfrak{N}$.

THEOREM 3.1.13 (Downward Löwenheim-Skolem). *Let $\mathfrak{M}$ be an $\mathcal{L}$-structure, and let $A \subseteq M$ be a set. Then there exists an elementary sub-model $\mathfrak{N} \preceq \mathfrak{M}$ containing A such that $|N| \leq \max\{|A|, |\mathcal{L}|, \aleph_0\} = |A| + |\mathcal{L}| + \aleph_0$.*

PROOF. For every formula of the form $\varphi(\bar{x}, y) \in \mathcal{L}_{\omega,\omega}$ and every tuple $\bar{a} \in M$ of the length of $\bar{x}$ such that if $\mathfrak{M} \models \exists y\, \varphi(\bar{a}, y)$, choose an element $b_{\varphi,\bar{a}} \in M$ such that $\mathfrak{M} \models \varphi(\bar{a}, b_{\varphi,\bar{a}})$.

We define by induction an increasing sequence of subsets of M: $A = A_0 \subseteq A_1 \subseteq \ldots$. We start with $A_0 = A$, and define

$$A_{n+1} = A_n \cup \{b_{\varphi,\bar{a}} : \bar{a} \in A_n \text{ and } \varphi \text{ such that } \mathfrak{M} \models \exists y\, \varphi(\bar{a}, y)\}.$$

Let $A_\omega = \bigcup_{n<\omega} A_n$. First we claim that the set A_ω is closed under the functions of $\mathfrak{M}$. Indeed, if f is an n-ary function symbol and $\bar{a} \in A_\omega^n$, then $\bar{a} \in A_m^n$ for some m. Let $\varphi(\bar{x}, y)$ be the formula $y = f(\bar{x})$. Then $f^M(\bar{a}) = b_{\varphi,\bar{a}} \in A_{m+1} \subseteq A_\omega$.

Therefore $\mathfrak{M}$ has a unique sub-structure $\mathfrak{N}$ whose underlying set is $N = A_\omega$. The Tarksi-Vaught criterion is satisfied by for $\mathfrak{N}$ in $\mathfrak{M}$ (same argument as above), whereby $\mathfrak{N} \preceq \mathfrak{M}$.

Last, we need to calculate cardinalities. Let $\kappa = |A| + |\mathcal{L}| + \aleph_0$. We prove by induction that $|A_n| \leq \kappa$. For A_0, this is since $A_0 = A$. For A_{n+1}: first, the number of finite tuples

in A_n is:

$$\sum_{m<\omega} |A_n|^m = \sum_{m<\omega} |A_n| = |A_n| \cdot \aleph_0 \leq \kappa \cdot \aleph_0 = \kappa.$$

Similarly, every formula is a finite sequence of symbols, and there are at most $|\mathcal{L}| + \aleph_0$ symbols to choose from, so there are at most $(|\mathcal{L}| + \aleph_0) \cdot \aleph_0 \leq \kappa$ formulae. Therefore at each step there are at most $\kappa^2 = \kappa$ pairs $\varphi, \bar{a}$ such that $\bar{a} \in A_n$ and $\varphi \in \mathcal{L}$, so we add at most κ witnesses to A_n, and $|A_{n+1}| \leq |A_n| + \kappa = \kappa$. Finally:

$$|N| = \left| \bigcup_{n<\omega} A_n \right| \leq \sum_{n<\omega} |A_n| \leq \kappa \cdot \aleph_0 = \kappa.$$

■3.1.13

We conclude with a result on which many constructions in Model Theory are based:

DEFINITION 3.1.14. Let $(I, <)$ be linearly ordered, and $(\mathfrak{M}_i \colon i \in I)$ an increasing sequence of structures, i.e., $i \leq j \implies \mathfrak{M}_i \subseteq \mathfrak{M}_j$. We define a structure $\mathfrak{N} = \bigcup_{i \in I} \mathfrak{M}_i$ in the obvious manner:

$$N = \bigcup_{i \in I} M_i$$

And for a function symbol f or predicate symbol P we define:

$$f^{\mathfrak{N}} = \bigcup_{i \in I} f^{\mathfrak{M}_i}, \qquad P^{\mathfrak{N}} = \bigcup_{i \in I} P^{\mathfrak{M}_i}$$

(By $\bigcup_{i \in I} f^{\mathfrak{M}_i}$ we mean the union of the graphs. One can and should verify that this is indeed the graph of a function.)

Notice that with this definition $\mathfrak{N} \supseteq \mathfrak{M}_i$ for all $i \in I$, and moreover, it is the unique such structure whose domain is $\bigcup_i M_i$. Also, for every n-ary function symbol f (predicate symbol P) and n-tuple $\bar{a} \in N^n$, there is $i \in I$ such that $\bar{a} \in \mathfrak{M}_i$, and then $f^{\mathfrak{N}}(\bar{a}) = f^{\mathfrak{M}_i}(\bar{a})$ ($\bar{a} \in P^{\mathfrak{N}} \iff \bar{a} \in P^{\mathfrak{M}_i}$).

PROPOSITION 3.1.15 (Elementary Chain Theorem). *Let $(I, <)$ be linearly ordered, and $(\mathfrak{M}_i \colon i \in I)$ an* elementary chain*, i.e., $i \leq j \implies \mathfrak{M}_i \preceq \mathfrak{M}_j$. Let $\mathfrak{N} = \bigcup_{i \in I} \mathfrak{M}_i$. Then $\mathfrak{N} \succeq \mathfrak{M}_i$ for all $i \in I$.*

PROOF. We will prove by induction on $\varphi(\bar{x})$ that for all $i \in I$ and $\bar{a} \in M_i$: $\mathfrak{M}_i \vDash \varphi(\bar{a}) \iff \mathfrak{N} \vDash \varphi(\bar{a})$.

(i) φ atomic: since $\mathfrak{N} \supseteq \mathfrak{M}_i$.

(ii) φ obtained using connectives: standard.

(iii) $\varphi(\bar{x}) = \exists y\, \psi(y, \bar{x})$. If $\mathfrak{M}_i \vDash \varphi(y, \bar{a})$ then there is $b \in M_i \subseteq N$ such that $\mathfrak{M}_i \vDash \psi(b, \bar{a})$, and by the induction hypothesis $\mathfrak{N} \vDash \psi(b, \bar{a})$ whereby $\mathfrak{N} \vDash \varphi(\bar{a})$. Conversely, assume $\mathfrak{N} \vDash \varphi(\bar{a})$. Then there is $b \in N$ such that $\mathfrak{N} \vDash \psi(b, \bar{a})$, and there is some $j \geq i$ such that $b \in M_j$. Since $\bar{a} \in M_i \subseteq M_j$ as well, our induction

hypothesis tells us that $\mathfrak{M}_j \models \psi(b, \bar{a})$, whereby $\mathfrak{M}_j \models \varphi(\bar{a})$. As $\mathfrak{M}_i \preceq \mathfrak{M}_j$: $\mathfrak{M}_i \models \varphi(\bar{a})$, as required. ■3.1.15

3.2. Quantifier elimination

Let $\mathbb{C}$ be the field of complex numbers, F the field of complex numbers which are algebraic over $\mathbb{Q}$ (i.e., are the roots of polynomials with rational coefficients). It is a classical fact that $\mathbb{C}$ is an algebraically closed field (the "Fundamental Theorem of Algebra", although it is in fact an analytic result), and that F is an algebraically closed sub-field of $\mathbb{C}$. Clearly $F \subseteq \mathbb{C}$ as structures (in $\mathcal{L}_{ring}$).

We would like to show that $F \preceq \mathbb{C}$. In order to do that we need, *a priori*, to verify for every formula $\varphi(\bar{x})$, and every tuple $\bar{a} \in F$, that $F \models \varphi(\bar{a}) \iff \mathbb{C} \models \varphi(\bar{a})$. Now this would be easy to verify for atomic formulae, and would therefore follow for quantifier-free formulae (i.e., formulae constructed without the use of quantifiers). But for a formula containing many quantifiers, this becomes a more complicated task.

The standard method of simplifying this task is what is a technique called *quantifier elimination*. We assume throughout that we work in a fixed signature $\mathcal{L}$.

Definition 3.2.1. Let T be a theory. We say that T has *quantifier elimination (QE)* if for every formula $\varphi(\bar{x})$, where $\bar{x}$ is a non-empty tuple, there is a quantifier-free formula $\theta(\bar{x})$ which is equivalent to φ modulo T.

Note that the requirement that $\bar{x}$ be non-empty does *not* mean that φ cannot be a sentence: it just means that if φ is a sentence, we would have to write it as $\varphi(x)$ with a dummy variable x, so θ may have x as a free variable (the problem is that a signature without constant symbols may simply have no quantifier free sentences).

From now on, all tuples $\bar{x}$, $\bar{a}$, etc., are assumed to be non-empty, even if not said so explicitly.

Lemma 3.2.2. *Assume that for quantifier-free formula $\varphi(\bar{x}, y)$ (where $\bar{x}$ is non-empty) there is a quantifier-free formula $\theta(\bar{x})$ which is equivalent modulo T to $\exists y\, \varphi(\bar{x}, y)$. Then T has QE.*

Proof. We prove that every formula $\varphi(\bar{x})$ is equivalent modulo T for a quantifier-free formula $\theta(\bar{x})$ by induction on the structure of φ:

(i) If φ atomic it is quantifier-free.
(ii) If $\varphi = \neg\psi$: by the induction hypothesis ψ is equivalent modulo T to a quantifier-free formula θ and then φ is equivalent modulo T to $\neg\theta$ which is quantifier-free. Similarly for other connectives.
(iii) Assume $\varphi(\bar{x}) = \exists y\, \psi(\bar{x}, y)$. By the induction hypothesis ψ is equivalent modulo T to a quantifier-free formula $\theta(\bar{x}, y)$. By assumption, $\exists y\, \theta(\bar{x}, y)$ is equivalent modulo T to some quantifier-free $\theta'(\bar{x})$. Therefore:

$$\varphi(\bar{x}) \equiv_T \exists y\, \theta(\bar{x}, y) \equiv_T \theta'(\bar{x}).$$

■3.2.2

We can somewhat weaken the assumption of Lemma 3.2.2. Recall that a *literal* is an atomic formula or its negation; a *conjunctive clause* is a conjunction of literals; and a *DNF formula* is a disjunction of conjunctive clauses. Recall also that every quantifier-free formula is logically equivalent to a DNF formula.

COROLLARY 3.2.3. *Assume that for conjunctive clause $\varphi(\bar{x}, y)$ there is a quantifier-free formula $\theta(\bar{x})$ which is equivalent modulo T to $\exists y\, \varphi(\bar{x}, y)$. Then T has QE.*

PROOF. Let $\varphi(\bar{x}, y)$ be any quantifier-free formula. Then it is logically equivalent to a formula in DNF, which we may write as $\bigvee_{i<n} \psi_i(\bar{x}, y)$ where each ψ_i is a conjunctive clause. It is left to the reader to verify that:

$$\exists y\, \varphi(\bar{x}, y) \equiv \exists y \bigvee_{i<n} \psi_i(\bar{x}, y) \equiv \bigvee_{i<n} \exists y\, \psi_i(\bar{x}, y).$$

By assumption, each formula $\exists y\, \psi_i(\bar{x}, y)$ is equivalent modulo T to a quantifier-free formula $\theta_i(\bar{x})$. We conclude that $\exists y\, \varphi(\bar{x}) \equiv_T \bigvee_{i<n} \theta_i(\bar{x})$. As the latter is quantifier-free we can apply Lemma 3.2.2 to conclude. ■3.2.3

We start with a quantifier-elimination result involving getting one's hands dirty:

EXAMPLE 3.2.4. Let DLO (dense linear ordering) be the set of consequence of the following sentences in the signature $\{<\}$:

$$\forall x\, x \not< x$$
$$\forall xyz\, (x < y) \wedge (y < z) \to (x < z)$$
$$\forall xy\, (x < y) \vee (y < x) \vee (x = y)$$
$$\forall x \exists yz\, (y < x) \wedge (x < z)$$
$$\forall xy \exists y\, (x < y) \to ((x < z) \wedge (z < y))$$

This is the theory of dense linear orderings without endpoints.

Notice that modulo DLO (in fact, modulo the first three axioms) we have that $x \neq y$ is equivalent to $(x < y) \vee (x > y)$ and $x \not< y$ is equivalent to $(x = y) \vee (y < x)$. It follows that modulo DLO, every quantifier-free formula is equivalent to one in DNF in which all the literals are positive. Therefore, as in Corollary 3.2.3, it suffices to show that if $\varphi(\bar{x}, y)$ is a positive conjunctive clause then it is equivalent modulo DLO to quantifier-free formula. We can write $\varphi(\bar{x}, y) = \varphi_1(\bar{x}) \wedge \varphi_2(\bar{x}, y)$, where φ_1 is the conjunction of all the literals which do no mention y and φ_2 is the conjunction of those which do. Clearly $\exists y\, \varphi \equiv \varphi_1 \wedge \exists y\, \varphi_2$, so we may assume that all the literals in φ involve y. There are several cases:

(i) If $y < y$ appears in φ then $\exists y\, \varphi \equiv_{DLO} x_0 \neq x_0$.
(ii) If $y = x_i$ appears in φ then $\exists y\, \varphi \equiv \varphi(x_i, \bar{x})$.
(iii) Otherwise, φ only contain literals of the form $y = y$, $y < x_i$ and $x_i < y$. The first kind are always true, so we ignore them. If φ contains no literals of the second kind then y larger than all the x_i would always satisfy φ. Similarly, if φ

contains no literals of the third kind then y smaller than all the x_i would always satisfy φ. Since DLO says there is no maximal or minimal element it follows that in either case $\exists y\, \varphi(\bar{x}, y) \equiv_{DLO} x_0 = x_0$.

(iv) The last case is that φ contains both literals of the form $y < x_i$ and $x_i < y$. Let

$$\theta(\bar{x}) = \bigwedge \{x_i < x_j \colon \text{ “}x_i < y\text{” and “}y < x_j\text{” appear in } \varphi\}.$$

Since DLO says the order is dense: $\exists y\, \varphi(\bar{y}, x) \equiv_{DLO} \psi(\bar{x})$.

It follows that DLO has QE.

The following result depends heavily on the Compactness Theorem, although in a manner essentially different than that used, say, in the proof of the upward Löwenheim-Skolem theorem.

Definition 3.2.5. Let T be a theory. Let Φ be a set of formulae in a fixed tuple of free variables $\bar{x}$ (i.e., every $\varphi \in \Phi$ is of the form $\varphi(\bar{x})$), which is closed under connectives.

We say that a formula $\psi(\bar{x})$ is *determined by* Φ *modulo* T if for every two models $\mathfrak{M}, \mathfrak{N} \vDash T$, and $\bar{a} \in M$, $\bar{b} \in N$ of the appropriate length:

$$\big[\forall \varphi \in \Phi \quad \mathfrak{M} \vDash \varphi(\bar{a}) \iff \mathfrak{N} \vDash \varphi(\bar{b})\big] \implies \big[\mathfrak{M} \vDash \psi(\bar{a}) \iff \mathfrak{M} \vDash \psi(\bar{b})\big].$$

Lemma 3.2.6. *Assume ψ is determined by Φ modulo T. Then whenever $\mathfrak{M} \vDash T$ and $\bar{a} \in M$ is of the correct length such that $\mathfrak{M} \vDash \psi(\bar{a})$, there is a formula $\varphi \in \Phi$ such that $\mathfrak{M} \vDash \varphi(\bar{a})$ and $T \vDash \varphi \to \psi$.*

Proof. Assume that $\mathfrak{M} \vDash T$ and $\bar{a} \in M$ is such that $\mathfrak{M} \vDash \psi(\bar{a})$. Let:

$$\Phi_1 = \{\varphi \in \Phi \colon \mathfrak{M} \vDash \varphi(\bar{a})\}$$
$$\Gamma_1 = T \cup \Phi_1 \cup \{\neg\psi\}.$$

We claim that Γ_1 is unsatisfiable. Indeed, if it were then there would be a model $\mathfrak{N} \vDash T$ and a tuple $\bar{b} \in N$ such that $\mathfrak{N} \vDash \neg\psi(\bar{b})$ and yet for all $\varphi \in \Phi$: $\mathfrak{M} \vDash \varphi(\bar{a}) \implies \mathfrak{N} \vDash \varphi(\bar{b})$. Since Φ is closed under $\neg$, this means that for all $\varphi \in \Phi$: $\mathfrak{M} \vDash \varphi(\bar{a}) \iff \mathfrak{N} \vDash \varphi(\bar{b})$. This contradicts the assumption.

So Γ_1 is not satisfiable, and by compactness there is a finite subset $\Phi_1' \subseteq \Phi_1$ such that $T \cup \Phi_1' \cup \{\neg\psi\}$ is not satisfiable. Let $\varphi_1 = \bigwedge \Phi_1'$: then $\mathfrak{M} \vDash \varphi_1(\bar{a})$ and $T \cup \{\varphi_1, \neg\psi\}$ is not satisfiable, i.e., $T \vDash \varphi_1 \to \psi$. Since Φ is closed under $\wedge$ we have $\varphi_1 \in \Phi$, as required. ■3.2.6

Proposition 3.2.7. *Let T be a theory. Let Φ be a set of formulae in a fixed tuple $\bar{x}$, closed under connectives, and let $\psi(\bar{x})$ be a formula. Then ψ is determined by Φ modulo T if and only if ψ is equivalent modulo T to some $\varphi \in \Phi$.*

Proof. One direction is clear. For the other, assume ψ is determined by Φ modulo T. Let:

$$\Phi_2 = \{\varphi \in \Phi \colon T \vDash \varphi \to \psi\}$$
$$\Gamma_2 = T \cup \{\psi\} \cup \{\neg\varphi \colon \varphi \in \Phi_2\}.$$

Lemma 3.2.6 says precisely that Γ_2 is not satisfiable. Therefore there is a finite subset $\Phi_2' \subseteq \Phi_2$ such that $T \cup \{\psi\} \cup \{\neg\varphi \colon \varphi \in \Phi_2'\}$ is not satisfiable. Let $\varphi_2 = \bigvee \Phi_2'$. Then $\varphi_2 \in \Phi$, and $T \vDash \varphi_2 \to \psi$. Also, $\neg\varphi_2$ is logically equivalent to $\bigwedge\{\neg\varphi \colon \varphi \in \Phi_2'\}$, so $T \cup \{\neg\varphi_2, \psi\}$ is not satisfiable, i.e., $T \vDash \psi \to \varphi_2$.

Therefore $\varphi_2 \equiv_T \psi$ as required. ■3.2.7

THEOREM 3.2.8. *Let T be a theory. Then the following are equivalent:*

(i) *T has quantifier elimination.*
(ii) *For every non-empty tuple of free variables $\bar{x}$, the set of quantifier-free formulae in $\bar{x}$ determines modulo T every formula of the form $\exists y\, \varphi(\bar{x}, y)$ where φ is conjunctive clause.*

PROOF. Follows immediately from Corollary 3.2.3 and Proposition 3.2.7. ■3.2.8

Let ACF be the theory of algebraically closed fields, in the signature $\mathcal{L}_{ring} = \{0, 1, -, +, \cdot\}$:

$$\begin{array}{ll}
\forall xy\, x + y = y + x & \forall xyxy = yx \\
\forall xyz\, (x + y) + z = x + (y + z) & \forall xyz(xy)z = x(yz) \\
\forall x\, x + 0 = x & \forall x\, x1 = x \\
\forall x\, x + (-x) = 0 & \forall x \exists y\, x \neq 0 \to xy = 1 \\
\forall xyz\, (x + y)z = xz + yz & \\
\forall x_0 \ldots x_{n-1} \exists y\, y^n + x_{n-1}y^{n-1} + \ldots + x_1 y + x_0 = 0 &
\end{array}$$

All the axioms but the last form the theory of fields. The last axiom is an axiom scheme, repeated for every $0 < n < \omega$, saying the field is algebraically closed.

THEOREM 3.2.9. *The theory ACF eliminates quantifiers.*

PROOF. Let K and L be two algebraically closed fields, and $\bar{a} \in K$, $\bar{b} \in L$ two finite tuples of the same length satisfying the same quantifier free formulae. We need to show that they satisfy the same formulae of the form $\exists y\, \varphi(y, \bar{x})$ where φ is a conjunctive clause.

The only atomic formulae in $\mathcal{L}_{ring}$ are of the form $t = t'$, where t, t' are terms. It is equivalent (modulo the theory of fields) to $t'' = 0$ where $t'' = t - t'$. Also, every term in $\mathcal{L}_{ring}$ evaluates to a polynomial with integer coefficients. Therefore, every atomic formula is equivalent to one of the form $f(\bar{x}) = 0$ where $f(\bar{X}) \in \mathbb{Z}[\bar{X}]$. A conjunctive clause is therefore a conjunction of polynomial equalities and inequalities.

Let $A_0 \subseteq K$ be the sub-ring generated by K, and $A \subseteq K$ the generated sub-field, i.e., the quotient field of A_0; similarly, let $B_0 \subseteq L$ be the ring generated by $\bar{b}$ and $B \subseteq L$ the generated field. The fact that $\bar{a}$ and $\bar{b}$ satisfy the same quantifier-free formulae means precisely that there is a (unique) isomorphism of rings $\theta_0 \colon A_0 \to B_0$ which extends (again, uniquely) to an isomorphism $\theta \colon A \to B$.

Assume now that $K \vDash \exists y\, \varphi(y, \bar{a})$, where φ is a conjunctive clause, and let $c \in K$ be such that $K \vDash \varphi(c, \bar{a})$. We need to find $d \in L$ such that $L \vDash \varphi(d, \bar{b})$. We consider two cases:

(i) If c is algebraic over A, it satisfies a minimal polynomial $f(Y) \in A[Y]$. Let $g(Y) = \theta(f) \in B[Y]$: then there is in L a root for g, call it d, and θ extends uniquely to an isomorphism $\theta' \colon A[c] \to B[d]$ sending c to d. As φ is quantifier-free, this implies in particular that $L \vDash \varphi(d, \bar{b})$.

(ii) If c is transcendental over A, write φ as

$$\varphi(y, \bar{x}) = \bigwedge_{i<k} f_i(y, \bar{x}) \neq 0 \wedge \bigwedge_{j<\ell} g_j(y, \bar{x}) = 0.$$

Since c is transcendental, each $g_j(Y, \bar{a})$ is the zero polynomial in $A[Y]$, whereby $g_j(Y, \bar{b}) = 0$ in $B[Y]$. Also, each $f_i(Y, \bar{a}) \in A[Y]$ must be non-zero. Therefore $h(Y) = Y \cdot \prod_{i<k} f_i(Y, \bar{b}) + 1 \in B[Y]$ is non-constant, and has a root $d \in L$. Clearly $f_i(d, \bar{b}) \neq 0$ for all $i < k$, whereby $L \vDash \varphi(d, \bar{b})$. ■3.2.9

Definition 3.2.10. A theory T is *model-complete* if whenever $\mathfrak{M} \subseteq \mathfrak{N}$ are both models of T then $\mathfrak{M} \preceq \mathfrak{N}$.

Lemma 3.2.11. *If T eliminates quantifiers then it is model-complete.*

Proof. Immediate. ■3.2.11

Fact 3.2.12. *All rings under consideration are commutative with a unit.*

(i) *Every proper ideal of a ring is contained in a maximal ideal.*
(ii) *If R is a ring and $I \subseteq R$ is a maximal ideal then R/I is a field.*
(iii) *Every field extends to an algebraically closed one.*
(iv) *If K is a field and $\bar{X}$ is a finite tuple of unknowns, the polynomial ring $K[\bar{X}]$ is* Noetherian*, i.e., every ideal $I \subseteq K[\bar{X}]$ is finitely generated.*

Corollary 3.2.13 (Hilbert's Nullstellensatz). *Let K be an algebraically closed field, $\bar{X} = X_0, \ldots, X_{n-1}$, $R = K[\bar{X}]$ and $I \subseteq R$ a proper ideal. Then I has a common root in K (i.e., a tuple $\bar{a} \in K^n$ such that $f(\bar{a}) = 0$ for all $f \in I$).*

Proof. Since $K[\bar{X}]$ is Noetherian, we can write $I = (f_0, \ldots, f_{m-1})$, where each $f_i(\bar{X}) \in K[\bar{X}]$. Since I is proper, it extends to a maximal proper ideal $J \subseteq R$. Let $F = R/J$, which is a field as J is maximal. Then we can view F as an extension of K via the embedding $a \mapsto (a + J)$. As every field embeds in an algebraically closed field, let L be an algebraically closed extension of F. Then $K \subseteq L$, and as ACF is model-complete: $K \preceq L$.

For $i < n$ let $b_i = X_i + J \in F \subseteq L$. For each $f(\bar{X}) \in J$ we have $f(\bar{b}) = f(\bar{X}) + J = 0 + J = 0_F$, so $\bar{b} \in L^n$ is a common root of J, and therefore of I. Therefore $L \vDash \exists \bar{y} \bigwedge_{i<m} f_i(\bar{y})$, and this is a formula with parameters in K, so as $K \preceq L$: $K \vDash \exists \bar{y} \bigwedge_{i<m} f_i(\bar{y})$ Since the f_i generate I, I has a common root in K. ■3.2.13

Exercises

EXERCISE 3.1. (i) Show that if $\mathcal{K}$ is a class of structures then $\mathrm{Th}(\mathcal{K})$ is a theory.
(ii) We could have defined $\mathrm{Mod}(\Sigma)$ for any set of sentences Σ (which is not closed under implication). Show that $\mathrm{Th}(\mathrm{Mod}(\Sigma))$ is the minimal theory containing Σ.

EXERCISE 3.2. Show that a theory T is complete if and only if there is a structure $\mathfrak{M}$ such that $T = \mathrm{Th}(\mathfrak{M})$.

EXERCISE 3.3 (Ultrapowers). Let $\mathfrak{M}$ be a structure, I a set, and $\mathscr{U}$ an ultrafilter on I. Let $\mathfrak{M}_i = \mathfrak{M}$ for all $i \in I$. Then the ultraproduct $\prod_{i\in I} \mathfrak{M}_i/\mathscr{U} = \prod_{i\in I} \mathfrak{M}/\mathscr{U}$ is called an *ultrapower* of $\mathscr{U}$, also denoted $\mathfrak{M}^I/\mathscr{U}$ or simply $\mathfrak{M}^{\mathscr{U}}$.
Show there exists a canonical elementary embedding of $\mathfrak{M}$ in $\mathfrak{M}^{\mathscr{U}}$.

EXERCISE 3.4. Prove Lemma 3.1.3.

EXERCISE 3.5. Finish the proof of Example 3.1.6.

EXERCISE 3.6. Let $\mathcal{L}$ be a signature (as usual, with equality). Recall from Definition 3.0.16 the notion of an elementary class of structures.
Show that the class of all infinite $\mathcal{L}$-structures is elementary, but the class of all finite such structures is not. (Hint: use the Compactness Theorem for the second item.)

EXERCISE 3.7. Let $\mathfrak{M}_0$, $\mathfrak{M}_1$ and $\mathfrak{M}_2$ be $\mathcal{L}$-structures, and assume that $\mathfrak{M}_0, \mathfrak{M}_1 \preceq \mathfrak{M}_2$, and that moreover $M_0 \subseteq M_1$. Then $\mathfrak{M}_0 \preceq \mathfrak{M}_1$.

EXERCISE 3.8. Let $\mathfrak{M}$ be a finite structure. Show that $\mathfrak{M}$ has no proper elementary extensions or substructures.

EXERCISE 3.9. Complete the proof of Proposition 3.1.9.

EXERCISE 3.10 (Application of the Löwenheim-Skolem Theorems). (i) Let T be a theory. Show that if T has arbitrarily large finite models then it has an infinite model, and that if it has an infinite model then it as a model of size κ for every infinite cardinal $\kappa \geq |\mathcal{L}|$.
(ii) (Vaught's Test)
Let T be a theory with no finite models, and assume that T is κ-categorical for some infinite cardinal $\kappa \geq |\mathcal{L}|$. Show that T is complete.

EXERCISE 3.11. Assume that the language $\mathcal{L}$ is countable. We say that a structure $\mathfrak{M}$ is *weakly* $\aleph_0$*-homogeneous* if for every two finite tuples $\bar{a}, \bar{b} \in M$ of the same length which satisfy the same formulae in $\mathfrak{M}$, and every $c \in M$, there is $d \in M$ such that $\bar{a}, c$ and $\bar{b}, d$ satisfy the same formulae in $\mathfrak{M}$.
(i) Let $\mathfrak{M}$ be any structure, $\bar{a}, \bar{b} \in M$ two finite tuples satisfying the same formulae. Let $c \in M$. Show there exists $\mathfrak{N} \succeq \mathfrak{M}$ such that $|N| = |M|$ and there is $d \in N$ such that $\bar{a}, c$ and $\bar{b}, d$ satisfy the same formulae in $\mathfrak{N}$.

(ii) Show that every countable structure admits a countable elementary extension which is weakly $\aleph_0$-homogeneous.

(iii) A structure $\mathfrak{M}$ is *strongly* $\aleph_0$*-homogeneous* if whenever there are two tuples $\bar{a}, \bar{b} \in M$ which satify the same formula, there is an automorphism $f \in \mathrm{Aut}(\mathfrak{M})$ (i.e., an isomorphism of $\mathfrak{M}$ with itself) sending $\bar{a}$ to $\bar{b}$. Show that a countable weakly $\aleph_0$-homogeneous is strongly $\aleph_0$-homogeneous.

EXERCISE 3.12. For p prime, let ACF_p be ACF along with $1+1+\ldots+1$ (p times) $= 0$. Let ACF_0 be ACF along with $1 + 1 + \ldots + 1$ (p times) $\neq 0$ for each p.

Show that for p prime or zero the theory ACF_p is complete.

EXERCISE 3.13. Let F be your favourite field. Let $\mathcal{L} = \{0, -, +\} \cup \{m_a\}_{a \in F}$, where 0 s a constant symbol, $-$ a unary function symbol, $+$ a binary function symbol, and m_a is a unary function symbol for each $a \in F$. This is the language of vector spaces over F.

If V is a vector space, it can be naturally identified with an $\mathcal{L}$-structure, where m_a is scalar multiplication by $a \in F$. (Note that the field F is part of the language, not of the structure).

Show that the class of vector spaces over F (i.e., the structures with which they are identified as above) is elementary. Do this by writing down a list Σ (possibly infinite) of $\mathcal{L}$-sentences such that $\mathfrak{M} \vDash \Sigma$ if and only if $\mathfrak{M}$ comes from a vector space as in the preceding paragraph.

Similarly, show that the class of infinite vector spaces over F is elementary.

EXERCISE 3.14. Show that for every fields F, the theory of infinite vector spaces over F eliminates quantifiers. (You may find that if you assume that F is finite the proof is somewhat easier.)

EXERCISE 3.15. Show that the theory of infinite vector spaces over a fixed field F is complete.

CHAPTER 4

Incompleteness

The goal of this chapter is to prove several results about decidability in Mathematics. The most famous is probably Gödel's Incompleteness Theorem, which roughly says that we can never give a complete set of axioms for Mathematics. That is to say that there is no set of sentences Σ such that:

- A sentence is true (in the "real world" of Mathematics) if and only if it is a consequence of Σ.
- The set Σ is *decidable*, i.e., there is a procedure, or algorithm, by which we can decide for each sentence φ whether $\varphi \in \Sigma$ or not (so there is a practical way to "give" Σ).

In fact, since we do not really know for every sentence whether it is true or not in the real world (or else we could shut down most of the Mathematics departments and research institutes), we need to prove a stronger result: no complete theory extending a basic theory we know is true can have a decidable axiomatisation.

What do we mean by "mathematics"? The standard answer to that would be set theory, as all of mathematics can indeed be developed therein. However, set theory is way stronger than what we need here: we can show that incompleteness already arises if we restrict our attention to *arithmetic*, i.e., the structure formed by the natural numbers. Even though infinite mathematical structures cannot live within arithmetic, which deals after all with finite objects, all the mathematical *reasoning* can be viewed as taking place entire inside arithmetic, and this will be enough. Of course, once there is no complete axiom system for arithmetic, there can be none for set theory or any other mathematical theory which is sufficiently strong to contain arithmetic in one form or another, which is what we want to prove.

We also need to define formally what we mean by an algorithm. In order to define an algorithm precisely, one usually defines what we call a *computation model*. This consists of the following information:

(i) What kind of input an algorithm is expected to take (the computation model's domain), and what kind of output it is expected to give (its range).
(ii) What the atomic computations are.
(iii) How an algorithm is constructed from these simple building blocks (how algorithms are executed).

There are many conceivable computation models. Among the best know are:

– The model of *Turing machines* (after Allan Turing) is essentially the one implemented by modern computers (with the difference that Turing machines have infinite memory). It is noteworthy that this model preceded computers by many years.

– The model of *recursive functions* is more mathematical in nature: there is no corresponding physical representation of the model as in the previous two, just functions that we construct according to certain rules.

The interesting thing is all these computation models and others that attempt to capture our intuitive idea of an algorithm are equivalent, in the sense that they can calculate the same functions. This serves as strong evidence to the somewhat vague (and therefore unprovable) conjecture that the "calculable" functions are precisely the recursive ones, know as *Church's thesis*.

Therefore, the choice of a computation model is not very important. As mathematicians, we naturally opt for that of recursive functions.

4.1. Recursive functions

The recursive functions will be defined formally below. Informally, each recursive function represents an algorithm, or a computer program, that takes as input finite tuples of a fixed length of natural numbers and performs a certain calculation on them. If the calculation ever stops, it yields a value which is itself a natural number; if the computation does not stop, which may well happen, the function is not defined for this specific input. Therefore, the recursive functions are going to be *partial* functions.

DEFINITION 4.1.1. Let $n < \omega$, $A \subseteq \mathbb{N}^n$, and let $f : A \to \mathbb{N}$. Then f is a *partial function* from $\mathbb{N}^n$ to $\mathbb{N}$, denoted $f\colon \mathbb{N}^n \dashrightarrow \mathbb{N}$. The set A is the *domain* of f, denoted $\mathrm{dom}(f)$. We consider A to be part of the information contained in f, which is why we allow ourselves to omit it in the notation. If $x \in \mathbb{N}^n \setminus \mathrm{dom}(f)$, then we say that $f(x)$ is not defined.

If $\mathrm{dom}(f) = \mathbb{N}^n$, then f is *total*, denoted as usual $f\colon {}^n \to \mathbb{N}$.

If $P \subseteq \mathbb{N}^n$ is a predicate, we define its *characteristic function* $\chi_P\colon \mathbb{N}^n \to \mathbb{N}$ by:

$$\chi_P(\bar{a}) = \begin{cases} 1 & \bar{a} \in P \\ 0 & \bar{a} \notin P \end{cases}$$

Projections: for every $i < n < \omega$, $\pi_{n,i} : \mathbb{N}^n \to \mathbb{N}$ is defined by: $\pi_{n,i}(x_0, \ldots, x_{n-1}) = x_i$. In particular, $\pi_{1,0}$ is the identity: $\pi_{1,0}(x) = x$.

If $f\colon \mathbb{N}^n \dashrightarrow \mathbb{N}$ and $g_i\colon \mathbb{N}^m \dashrightarrow \mathbb{N}$ are partial functions for $i < n$, we define the composition:

$$h = f \circ (g_0, \ldots, g_{n-1})\colon \mathbb{N}^m \dashrightarrow \mathbb{N}$$
$$\mathrm{dom}(h) = \{\bar{a} \in \mathbb{N}^m\colon \bar{a} \in \bigcap_{i<n} \mathrm{dom}(g_i) \text{ and } (g_i(\bar{a})\colon i < n) \in \mathrm{dom}(f)\}$$

And for $\bar{a} \in \mathrm{dom}(h)$:

$$h(\bar{a}) = f(g_i(\bar{a}) \colon i < n).$$

Another way to construct functions from others is the *μ-operator*. Let $f \colon \mathbb{N}^{n+1} \dashrightarrow \mathbb{N}$. We define $h(\bar{y}) = \mu x\,(f(\bar{y}, x) = 0)$ as a partial function $h \colon \mathbb{N}^n \dashrightarrow \mathbb{N}$. For $\bar{a} \in \mathbb{N}^n$, $h(\bar{a}) = b$ if and only if $f(\bar{a}, c)$ is defined for all $c \leq b$, $f(\bar{a}, c) > 0$ for all $c < b$, and $f(\bar{a}, b) = 0$. If no such b exists then $h(\bar{a})$ is not defined. (Think of a computer programme calculating $f(\bar{a}, b)$ for $b = 0, 1, \ldots$, stopping the moment it finds such a b for which the result is 0. A function not being defined corresponds to the programme never stopping. Indeed this can happen in one of two cases: either one of the calculations of $f(\bar{a}, b)$ never stops, or they all stop but yield non-zero results.)

Definition 4.1.2. The family *recursive functions* is the smallest family of partial functions from powers of $\mathbb{N}$ to $\mathbb{N}$, containing $\chi_{\leq}$, $+$, $\cdot$ and all the projections, and closed under composition and the μ-operator.

In other words, the family of recursive functions is generated by $\chi_{\leq}$, $+$, $\cdot$ and projections by composition and the μ-operator. Notice that all the basic recursive functions are total, and that the composition of total functions is total, so the only source for non-total recursive functions is the μ-operator.

Constant functions. Let $c_n(x)$ denote the function equal to n for all x. Then $c_1(x) = \chi_{\leq}(x, x)$, and the latter can be obtained as $\chi_{\leq} \circ (\mathrm{id}, \mathrm{id})$. As $\chi_{\leq}$ and $\mathrm{id} = \pi_{1,0}$ are recursive, so is c_1. Then we get $c_2 = c_1 + c_1$ (i.e., $+ \circ (c_1, c_1)$), etc. Finally, $c_0 = \chi_{\leq} \circ (c_2, c_1)$. These are all functions in a single variable. Then constant function n in m variables is recursive as it can be written as $c_n \circ \pi_{m,0}$ From now on we will identify the constant functions with their values and write n instead of c_n.

Recursive predicates. We define:

Definition 4.1.3. A predicate $P \subseteq \mathbb{N}^n$ is *recursive* if its characteristic function χ_P is a (total) recursive function.

Note that the binary predicate $\leq$ is recursive by definition.

Let $P \subseteq \mathbb{N}^n$ be a recursive predicate, $f_i \colon \mathbb{N}^m \to \mathbb{N}$ total recursive functions for $i < n$. Define $Q \subseteq \mathbb{N}^m$ by:

$$Q(\bar{a}) \iff P(f_0(\bar{a}), \ldots, f_{n-1}(\bar{a})).$$

Then Q is recursive. Indeed, we have:

$$\chi_Q = \chi_P \circ (f_i \colon i < n).$$

For example, we conclude that the unary predicate $\{0\}$ (i.e., "$x = 0$") is recursive. Indeed:

$$x = 0 \iff x \leq 0 (\iff \mathrm{id}(x) \leq c_0(x)).$$

Boolean combinations of recursive predicates. Let $P, Q \subseteq \mathbb{N}^n$ be recursive predicates. Note that $\chi_{P \wedge Q} = \chi_P \cdot \chi_Q$, and $\chi_{\neg P} = \chi_{\{0\}} \circ \chi_P$, so $\neg P$ and $P \wedge Q$ are recursive. It follows that $P \vee Q = \neg(\neg P \wedge \neg \chi)$ is recursive as well, and using disjunctive normal form, if $P_i \colon i < m$ are recursive of the same arity and $g \colon \{T, F\}^m \to \{T, F\}$ is any (Boolean) function, then $g \circ (P_i \colon i < m)$ is also a recursive predicate.

Since $\leq$ is recursive, it follows that $<$, $=$, $\neq$ are also recursive.

μ-operator for recursive predicates. Let $P \subseteq \mathbb{N}^{n+1}$ be a recursive predicate. Define $f(\bar{y}) = \mu x \, P(\bar{y}, x) \colon \mathbb{N}^n \dashrightarrow \mathbb{N}$ by letting $f(\bar{a})$ be the least b such that $P(\bar{a}, b)$ holds, or if no such b exists then $f(\bar{a})$ is undefined. Then f is recursive. Indeed,

$$f(\bar{y}) = \mu x (\chi_{\neg P}(\bar{y}, x) = 0).$$

Bounded μ-operator and quantifiers. Let $P \subseteq \mathbb{N}^{n+1}$ be recursive, and define $f(\bar{x}, z) = \mu y_{<z} \, P(\bar{x}, y)$ as the least y smaller than z such that $P(\bar{x}, y)$, or z if no such y exists. Then f is a total recursive function:

$$f(\bar{x}, z) = \mu y \, (y \geq z \vee P(\bar{x}, y)).$$

Similarly, we can define $Q \subseteq \mathbb{N}^{n+1}$ by: $Q(\bar{x}, z) \iff \exists y_{<z} \, P(\bar{x}, y)$, which is true if and only if there is some $y < z$ such that $P(\bar{x}, y)$. This is a recursive predicate, as:

$$\exists y_{<z} \, P(\bar{x}, y) \iff (\mu y_{<z} \, P(\bar{x}, y)) < z.$$

We define $\exists y_{\leq z}$, $\forall y_{<z}$ and $\forall y_{\leq z}$ similarly.

Definition by cases. Let $P_i \colon i < m$ be n-art recursive predicates such that for each tuple $\bar{a} \in \mathbb{N}^n$ exactly one of them is true, and let $f_i \colon i < m$ be total n-ary recursive functions. Define:

$$g(\bar{x}) = \begin{cases} f_0(\bar{x}) & \text{if } P_0(\bar{x}) \\ \dots & \\ f_{n-1}(\bar{x}) & \text{if } P_{n-1}(\bar{x}). \end{cases}$$

Then g is recursive. Indeed, $g(\bar{x}) = \chi_{P_0}(\bar{x}) \cdot f_0(\bar{x}) + \ldots + \chi_{P_{n-1}}(\bar{x}) \cdot f_{n-1}(\bar{x})$. We may replace "if $P_{n-1}(\bar{x})$" with "otherwise", so all we require of $P_0, \ldots, P_{n-2}$ is to be recursive and mutually exclusive, noting that then $P_{n-1} = \neg(P_0 \vee \ldots \vee P_{n-2})$ is recursive as well.

The same holds for definition of a predicate by cases:

$$R(\bar{x}) \iff \begin{cases} Q_0(\bar{x}) & \text{if } P_0(\bar{x}) \\ \dots & \\ Q_{n-2}(\bar{x}) & \text{if } P_{n-2}(\bar{x}) \\ Q_{n-1}(\bar{x}) & \text{otherwise.} \end{cases}$$

Miscellaneous functions. Subtraction cannot be recursive for the technical reason that its range contains negative numbers which we do not allow. Instead we define for $x, y \in \mathbb{N}$:

$$x \dot{-} y = \begin{cases} x - y & x \geq y \\ 0 & \text{otherwise.} \end{cases}$$

Then $\dot{-}$ is recursive. Indeed, $x \dot{-} y = \mu z\,(y + z \geq x)$.

Similarly, the binary relation $x \mid y$ (x divides y) is recursive. Indeed:

$$x \mid y \iff \exists z_{\leq y}\,(xz = y).$$

Ordered pairs. Let us define: $\mathrm{op}(x, y) = (x + y)^2 + x + 1$. Observe that $(x + y)^2 < \mathrm{op}(x, y) \leq (x + y + 1)^2$. This is a total recursive function, whose name stands for *ordered pair*. This is justified by the following:

LEMMA 4.1.4. *For all $a, b, c, d \in \mathbb{N}$:*

$$\mathrm{op}(a, b) = \mathrm{op}(c, d) \iff a = c \wedge b = d.$$

PROOF. Assume $\mathrm{op}(a, b) = \mathrm{op}(c, d)$. Then $(a+b)^2 < (c+d+1)^2$, whereby $a+b \leq c+d$. Similarly $c+d \leq a+b$, so $a+b = c+d$. But then $(a+b)^2+a+1 = (c+d)^2+c+1 \Longrightarrow a = c$, and $b = d$ ensues. ■4.1.4

The coding function β. The function op allows us to code pairs of natural numbers in a single natural number. We wish to code sequences of arbitrary finite length of natural numbers in single numbers.

LEMMA 4.1.5. *Let $m \in \mathbb{N}$, $c = m!$. Then $ac + 1$ and $bc + 1$ are relatively prime for all $a < b \leq m$.*

PROOF. Assume not, and let p be a common prime factor of $ac+1$ and $bc+1$. Then $p \mid (a - b)c$, so $p \leq m$. But then $p \mid ac \Longrightarrow p \nmid ac + 1$. ■4.1.5

We now define the following binary function.

$$\beta(x, y) = \mu z_{<x}\, \exists t_{<x} \exists w_{<x}\, \big(x = \mathrm{op}(t, w) \wedge t\,\mathrm{op}(z, y) + 1 \mid w\big)$$

PROPOSITION 4.1.6. *β is recursive, and for every tuple $a_i \colon i < n$ there is a number a such that for all $i < n$: $\beta(a, i) = a_i$.*

PROOF. Let $m = \mathrm{op}(\max\{a_i \colon i < n\}, n)$, $c = m!$, $d = \prod_{i<n}(c \cdot \mathrm{op}(a_i, i) + 1)$ and $a = \mathrm{op}(c, d)$ (yes, values here grow very fast...) We claim that a is as required.

Indeed, let us calculate $\beta(x, y)$ where $x = a$ and $y = i < n$.

Assume first that $z \leq a_i$ (clearly $a_i < a$), and $t, w < a$ are such that $x = \mathrm{op}(t, w) \wedge t\,\mathrm{op}(z, y) + 1 \mid w$. Then $t = c$ and $w = d$. Also, $\mathrm{op}(z, i) > 0$, so $c\,\mathrm{op}(z, i) + 1 > 1$. As $\mathrm{op}(z, i) \leq m$, it is relatively prime to $\mathrm{op}(a_j, j)$ for all $j < n$, unless $j = i$ and $a_i = z$. Therefore $z = a_i$.

Thus the least z for which $\exists t_{<x}\exists w_{<x}\big(x = \mathrm{op}(t,w) \wedge t\,\mathrm{op}(z,y)+1 \mid w\big)$ can possibly be true is $z = a_i$. On the other hand, letting $t = c < a$ and $w = d < a$ we see that this is true for $z = a_i < a$, whereby $\beta(a,i) = a_i$. ■4.1.6

Coding and decoding of finite sequences. For each n and tuple $\bar{a} = a_{<n} = a_0,\dots,a_{n-1}$ we define $\langle\bar{a}\rangle$ as the least a such that:

(i) $\beta(a,0) = n$,
(ii) $\beta(a,i+1) = a_i$.

Note that we always have $\beta(a,i) \le a$, so $n, a_i \le \langle a_{<n}\rangle$ for all $i < n$. We call $\langle a_0,\dots,a_{n-1}\rangle$ the *sequence number* of the finite sequence $a_0,\dots,a_{n-1}$.

For every fixed n, the function $f_n(x_0,\dots,x_{n-1}) = \langle x_0,\dots,x_{n-1}\rangle$ is recursive:

$$f_n(\bar{x}) = \mu y\,(\beta(y,0) = n \wedge \beta(y,1) = x_0 \wedge \ldots \wedge \beta(y,n) = x_{n-1}).$$

Conversely, we can decode sequence numbers using the following recursive functions:

$$\mathrm{len}(x) = \beta(x,0)$$
$$(x)_y\beta(x,y+1).$$

Thus $\mathrm{len}(\langle a_0,\dots,a_{n-1}\rangle) = n$ and $(\langle a_0,\dots,a_{n-1}\rangle)_i = a_i$ for $i < n$.

Operations on sequence numbers. We define $\mathrm{Seq} \subseteq \mathbb{N}$ as the set of sequence numbers. This is recursive:

$$\mathrm{Seq}(x) \iff \neg\exists y_{<x}\big(\mathrm{len}(y) = \mathrm{len}(x) \wedge \forall_{i<\mathrm{len}(x)}(x)_i = (y)_i\big).$$

We can extract initial sub-sequences. Indeed, define

$$\mathrm{Init}(x,y) = \mu z\big(\mathrm{len}(z) = y \wedge \forall i_{<y}(z)_i = (x)_i\big).$$

Then Init is a total recursive function, satisfying $\mathrm{Init}(x,y) = \langle(x)_0,\dots,(x_{y-1})\rangle$. If $m \le n$ then $\mathrm{Init}(\langle a_{<n}\rangle) = \langle a_{<m}\rangle$.

We can similarly concatenate sequences:

$$\begin{aligned} x * y = \mu z\big(&\ \mathrm{len}(z) = \mathrm{len}(x) + \mathrm{len}(y) \\ &\wedge \forall i_{<\mathrm{len}(x)}(z)_i = (x)_i \\ &\wedge \forall i_{<\mathrm{len}(y)}(z)_{\mathrm{len}(x)+i} = (x)_i\big). \end{aligned}$$

Inductive definitions. Let $f\colon \mathbb{N}^{n+1} \to \mathbb{N}$ be a total function. Define

$$\tilde{f}(\bar{a},b) = \langle f(\bar{a},0),\dots,f(\bar{a},b-1)\rangle.$$

Then $\tilde{f}$ is total, and is recursive if and only if f is. Indeed, if $\tilde{f}$ is recursive then we can recover f as:

$$f(\bar{x},y) = (\tilde{f}(\bar{x},y+1))_y.$$

Conversely, if f is recursive, then:

$$\tilde{f}(\bar{x},y) = \mu z\,(\mathrm{len}(z) = y \wedge \forall i_{<y}(z_i) = f(\bar{x},i)).$$

Let $g\colon \mathbb{N}^{n+2} \to \mathbb{N}$ be a total recursive function. Then there exists a unique total function $f\colon \mathbb{N}^{n+1} \to \mathbb{N}$ satisfying:

$$f(\bar{x}, y) = g(\tilde{f}(\bar{x}, y), \bar{x}, y).$$

Moreover, f is recursive. Indeed, a function f satisfies this equation if and only if $\tilde{f}$ satisfies:

$$\tilde{f}(\bar{x}, y) = \mu z \left(\mathrm{len}(z) = y \wedge \forall i_{<y}(z)_i = g(\mathrm{Init}(z, i), \bar{x}, i) \right).$$

This is an explicit definition, so such an $\tilde{f}$ exists, is unique, and is recursive, so f exists, and is unique and recursive.

This means we can use an explicit definition for $f(\bar{x}, y)$ which uses the value of $f(\bar{x}, z)$ for $z < y$ (since these values can be extracted from the value of $\tilde{f}(\bar{x}, y)$). Such a definition would be called *inductive*.

Primitive recursion. Let us see this through a common example. Let $g\colon \mathbb{N}^n \to \mathbb{N}$ and $h\colon \mathbb{N}^{n+2} \to \mathbb{N}$ be total recursive functions. Define $f\colon \mathbb{N}^{n+1} \to \mathbb{N}$ by:

$$f(\bar{x}, y) = \begin{cases} g(\bar{x}) & y = 0 \\ h(\bar{x}, f(\bar{x}, z), z) & y = z + 1. \end{cases}$$

We then say that f is constructed from g and h through *primitive recursion*.

We claim that f is recursive. Indeed, define

$$g'(t, \bar{x}, y) = \begin{cases} g(\bar{x}) & y = 0 \\ h(\bar{x}, (t)_{y \dot{-} 1}, y \dot{-} 1) & \text{otherwise.} \end{cases}$$

Then g is total recursive and

$$f(\bar{x}, y) = g'(\tilde{f}(\bar{x}, y), \bar{x}, y).$$

Remark 4.1.7. One can define the family of *primitive recursive* functions as the minimal family of functions which:

- Contains the constant function $x \mapsto 0$, the successor function $s(x) = x + 1$, and all the projections $\pi_{n,m}\colon \mathbb{N}^n \to \mathbb{N}$.
- Is closed under composition.
- Is closed under primitive recursion.

Note that all the primitive recursive functions are total. By the arguments above, every primitive recursive function is recursive.

4.2. Coding syntax in Arithmetic

Let $\mathcal{L}$ be a finite signature. We will assign numerical codes to symbols and expressions of $\mathcal{L}$. These codes are called *Gödel numbers* or *codes*.

- To the mth variable x_m we associate the code $\ulcorner x_m \urcorner = \langle 0, m \rangle$.

- For each n we enumerate the n-ary function and predicate symbols as $\{f_{n,m} \colon m < \ell_n\}$. To the mth n-ary function symbol $f_{n,m}$ we associate the code $\ulcorner f_{n,m} \urcorner = \langle 1, n, m \rangle$.
- We numerate the n-ary predicate symbols similarly, and to $P_{n,m}$ we associate the code $\ulcorner P_{n,m} \urcorner = \langle 2, n, m \rangle$.
- We also define $\ulcorner \neg \urcorner = 3$, $\ulcorner \to \urcorner = 4$, and $\ulcorner \forall \urcorner = 5$.
- Once we have defined the Gödel codes of variables and function symbols, we can define the Gödel codes of terms inductively:

$$\ulcorner f t_0, \ldots, t_{n-1} \urcorner = \langle \ulcorner f \urcorner, \ulcorner t_0 \urcorner, \ldots, \ulcorner t_{n-1} \urcorner \rangle.$$

- We define Gödel codes for atomic formulae similarly:

$$\ulcorner P t_0, \ldots, t_{n-1} \urcorner = \langle \ulcorner P \urcorner, \ulcorner t_0 \urcorner, \ldots, \ulcorner t_{n-1} \urcorner \rangle.$$

- For convenience, we will restrict our syntax to $\neg$, $\to$, $\forall$. We define:

$$\ulcorner \neg \varphi \urcorner = \langle \ulcorner \neg \urcorner, \ulcorner \varphi \urcorner \rangle$$
$$\ulcorner \varphi \to \psi \urcorner = \langle \ulcorner \to \urcorner, \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner \rangle$$
$$\ulcorner \forall x \, \varphi \urcorner = \langle \ulcorner \forall \urcorner, \ulcorner x \urcorner, \ulcorner \varphi \urcorner \rangle.$$

We also use $Arity(x)$ as shorthand for $(x)_1$. This is recursive.

Recall we showed that $\beta(x, y) \leq x$ for all x, y. Rename this function β to be β', and re-define β as $\beta(x, y) = \beta'(x, y) \dot{-} 1$. Then everything we proved for the old β still holds for the new β, and in addition, if $x > 0$ then $(x)_i < x$ for all i.

LEMMA 4.2.1. *The following relations and functions are recursive (and in fact primitive recursive):*

(i) $Var(x) =$ *"x is the code of a variable".*
(ii) $FSymb(x) =$ *"x is the code of a function symbol.*
(iii) $PSymb(x) =$ *"x is the code of a predicate symbol.*
(iv) $Term(x) =$ *"x is the code of a term".*
(v) $AF(x) =$ *"x is the code of an atomic formula".*
(vi) $Form(x) =$ *"x is the code of a formula".*

PROOF. (i) $Var(x) = \exists y_{<x} \, x = \langle 0, y \rangle$ (since $\ulcorner x_i \urcorner > i$).
(ii) $FSymb$ is finite by assumption and therefore recursive.
(iii) $PSymb$ is finite by assumption and therefore recursive.
(iv) We have an inductive definition: $Term(x)$ if and only if:
- $x = \ulcorner v \urcorner$ for some variable v (formally: $Var(x)$); or:
- $x = \langle \ulcorner f \urcorner, y_0, \ldots, y_{n-1} \rangle$, where f is an n-ary function symbol and y_i is the code of a term for all $i < n$ (formally: $FSymb((x)_0)$, $\text{len}(x) = Arity((x)_0) + 1$, and $\forall i_{<Arity((x)_0)} \, Term((x)_{i+1})$.)

Since $\text{len}(x) \geq 1 \implies x \neq 0 \implies (x)_i < x$ for all i, this is a legitimate inductive proof.

(v) $AF(x)$ if and only if $x = \langle \ulcorner P \urcorner, \ulcorner t_0 \urcorner, \ldots, \ulcorner t_{n-1} \urcorner \rangle$, where P is an n-ary function symbol and t_i is a term for all $i < n$.

(vi) $Form(x)$ if and only if:
- $x = \ulcorner \varphi \urcorner$, where φ is an atomic formula; or:
- $x = \ulcorner \neg \varphi \urcorner = \langle \ulcorner \neg \urcorner, \ulcorner \varphi \urcorner \rangle$, where φ is a formula (i.e., $(x)_0 = \ulcorner \neg \urcorner$, $\mathrm{len}(x) = 2$ and $Form((x)_1)$); or:
- $x = \langle \ulcorner \to \urcorner, \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner \rangle$, where φ and ψ are formulae; or:
- $x = \langle \ulcorner \forall \urcorner, \ulcorner v \urcorner, \ulcorner \varphi \urcorner \rangle$, where v is a variable and φ a formula.

As in the case of $Term$, the only uses of $Form$ in its own definition are for lower values (if $x = \langle \ldots, y, \ldots \rangle$ then $y < x$) so this is a legitimate inductive definition.

■4.2.1

We may also define more sophisticated syntax-related recursive functions and predicates:

Let us start with defining a predicate $Free(x, y)$. This is an inductive definition by cases:

$$Free(x,y) \iff \begin{cases} x = y & Var(y) \\ \exists i_{<Arity((y)_0)} Free(x, (y)_{i+1}) & (Term(y) \wedge \neg Var(y)) \vee AF(y) \\ Free(x, (y)_1) & (y)_0 = \ulcorner \neg \urcorner \\ Free(x, (y)_1) \vee Free(x, (y)_2) & (y)_0 = \ulcorner \to \urcorner \\ Free(x, (y)_2) x \neq (y)_1 & (y)_0 = \ulcorner \forall \urcorner \\ 0 = 1 & \text{otherwise.} \end{cases}$$

Then $Free(x)$ is a recursive predicate, and if x is a variable, t a term, and φ a formula, then $Free(\ulcorner x \urcorner, \ulcorner t \urcorner)$ if and only if x appears in t, and $Free(\ulcorner x \urcorner, \ulcorner \varphi \urcorner)$ if and only x is free in φ.

We obtain as a consequence the following recursive predicate:

$$\begin{aligned} Sent(x) &\iff Form(x) \wedge \forall y_{<x} \neg (Var(y) \wedge Free(y, x)) \\ &\iff x \text{ is the code of a sentence.} \end{aligned}$$

We can define free substitutions similarly:

$$FrSub(x,y,z) = \begin{cases} z & x = y \wedge Var(x) \\ \mu w\big(\mathrm{len}(w) = \mathrm{len}(x) \wedge (w)_0 = (x)_0 \wedge \\ \qquad \forall i_{<Arity((x)_0)}(w)_{i+1} = FrSub((x)_{i+1}, y, z)\big) & (Term(x) \wedge \neg Var(x)) \vee AF(x) \\ \langle \ulcorner\neg\urcorner, FrSub((x)_1, y, z)\rangle & (x)_0 = \ulcorner\neg\urcorner \\ \langle \ulcorner\rightarrow\urcorner, FrSub((x)_1, y, z), FrSub((x)_2, y, z)\rangle & (x)_0 = \ulcorner\rightarrow\urcorner \\ \langle \ulcorner\forall\urcorner, (x)_1, FrSub((x)_2, y, z)\rangle & (x)_0 = \ulcorner\forall\urcorner \wedge (x)_1 \neq y \\ x & (x)_0 = \ulcorner\forall\urcorner \wedge (x)_1 = y \\ 17 & \text{otherwise.} \end{cases}$$

Then $FrSub$ is recursive, and $FrSub(\ulcorner t'\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner) = \ulcorner t'[t/x]\urcorner$, $FrSub(\ulcorner\varphi\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner) = \ulcorner\varphi[t/x]\urcorner$.

We can similarly test whether a free substitution to a formula is correct:

$$CFrSub(x,y,z) \iff \begin{cases} 0 = 0 & AF(x) \\ CFrSub((x)_1, y, z) & (x)_0 = \ulcorner\neg\urcorner \\ CFrSub((x)_1, y, z) \wedge CFrSub((x)_2, y, z) & (x)_0 = \ulcorner\rightarrow\urcorner \\ \neg Free((x)_1, z) & (x)_0 = \ulcorner\forall\urcorner \wedge (x)_1 \neq y \\ 0 = 0 & (x)_0 = \ulcorner\forall\urcorner \wedge (x)_1 = y \\ 0 = 0 & \text{otherwise.} \end{cases}$$

We now observe we can tell, using recursive predicates, whether a (code for a) formula is (the code of) a logical axioms:

- First, x is a code of an instance of A1 if and only if it is a formula and:

$$\exists y_{<x} \exists z_{<x}\, x = \langle \ulcorner\rightarrow\urcorner, y, \langle \ulcorner\rightarrow\urcorner, z, y\rangle\rangle.$$

  Similarly for A2-4.
- It is an instance of A5 if and only if it is a formula and:

$$\exists y_{<x} \exists z_{<x} \left(\neg Free(z,y) \wedge x = \langle \ulcorner\rightarrow\urcorner, y, \langle \ulcorner\forall\urcorner, z, y\rangle\rangle\right).$$

- It is an instance of A6 if and only if it is a formula and:

$$\exists y_{<x} \exists z_{<x} \exists w_{<x} \left(CFrSub(y,z,w) \wedge x = \langle \ulcorner\rightarrow\urcorner, \langle \ulcorner\forall\urcorner, z, y\rangle, FrSub(y,z,w)\rangle\right).$$

- Axiom schemes A7-11 are dealt with similarly and left as an exercise.
- Therefore "x is the code of an instance of one of A1-11" is recursive, as a finite disjunction of recursive predicates.

- Finally, define $LogAx(x)$ as saying that either x is an instance of one of A1-11, or there are $y, z < x$ such that $Var(y)$, $LogAx(z)$, and $x = \langle \ulcorner \forall \urcorner, y, z \rangle$. This inductive definition shows that $LogAx$ is recursive, and $LogAx(x)$ is true if and only if $x = \ulcorner \forall v \dots \forall u \, \varphi \urcorner$, where φ is an instance of one of A1-11, i.e., if and only if x is the code of a logical axiom.

DEFINITION 4.2.2. We say that a set of formulae Γ is *decidable* if $\hat{\Gamma} = \{\ulcorner \varphi \urcorner : \varphi \in \Gamma\}$ is recursive.

Let Γ be a decidable set of formulae. Define $DedSeq_\Gamma(x, y)$ to say that x is a sequence number, and for all $i < \mathrm{len}(x)$ one of the following holds:

- $(x)_i$ is a logical axiom; or:
- $(x)_i \in \hat{\Gamma}$; or:
- $\exists j, k < i \, (x)_k = \langle \ulcorner \to \urcorner, (x)_j, (x_i) \rangle$.

Then $DedSeq_\Gamma$ is recursive, and holds precisely when x codes a deduction sequences from Γ.

Define

$$Ded_\Gamma(x, y) \iff DedSeq_\Gamma(y) \wedge \mathrm{len}(y) > 0 \wedge x = (y)_{\mathrm{len}(y) \dot{-} 1}.$$

Then Ded_Γ is recursive, and holds precisely when y codes a deduction of y from Γ.

DEFINITION 4.2.3. Let T be a theory (i.e., a set of sentences closed under deduction). We say that T is *axiomatised* if it has a decidable set of axioms, i.e., if there exists a decidable set of sentences $\Sigma \subseteq T$ such that T is the set of sentences which are consequences of Σ.

Say that T is axiomatised, and let $\Sigma \subseteq T$ be a decidable set of axioms. Then:

$$\varphi \in T \iff Sent(\ulcorner \varphi \urcorner) \wedge \exists y \, Ded_\Sigma(\ulcorner \varphi \urcorner, y).$$

Unfortunately the right hand side has no particular reason to be recursive, as it contains an unbounded quantifier.

DEFINITION 4.2.4. A set $P \subseteq \mathbb{N}$ is *recursively enumerable (r.e.)* if it is empty, or the range of a total recursive function.

We say that a set of formulae Γ is *enumerable* if $\hat{\Gamma}$ is r.e.

(Compare this with Exercise 4.1.)

PROPOSITION 4.2.5. *A predicate $P \subseteq \mathbb{N}$ is r.e. if and only if there is a recursive predicate $Q \subseteq \mathbb{N}^2$ such that $P(x) \iff \exists y \, Q(x, y)$.*

PROOF. Assume first that P is r.e. If P is empty let $Q = \varnothing$. Otherwise, P is the range of a recursive function f, and let $Q(x, y) \iff x = f(y)$. Either way Q is recursive and $P(x) \iff \exists y \, Q(x, y)$.

Conversely, assume Q is recursive and $P(x) \iff \exists y\, Q(x,y)$ If P is empty then it is r.e. Otherwise, let $n \in P$. Define

$$f(x) = \begin{cases} (x)_0 & \text{if } Q((x)_0, (x)_1) \\ n & \text{otherwise.} \end{cases}$$

Then f is total recursive and P is the range of f. ■4.2.5

COROLLARY 4.2.6. *Every axiomatised theory is enumerable.*

PROPOSITION 4.2.7. *A set $P \subseteq \mathbb{N}$ is recursive if and only both P and its complement are recursively enumerable.*

PROOF. By Exercise 4.1, every recursive set is recursively enumerable. If P is recursive then so is its complement, and thus both are recursively enumerable.

Conversely, assume both P and $\mathbb{N} \setminus P$ are recursively enumerable. If either one is empty, clearly P is recursive. Otherwise, say they are the ranges of the total recursive functions f and g, respectively.

Let $h(x) = \mu y(f(y) = x \vee g(y) = x)$. Then h is recursive, and total since every $x \in \mathbb{N}$ is either in the range of f or of g. Then $P(x) \iff f \circ h(x) = x$. ■4.2.7

LEMMA 4.2.8. *Let $P \subseteq \mathbb{N}$ be r.e. and $f(x)$ be total recursive. Then the predicate $P(f(x))$ is r.e.*

PROOF. Say $P(x) \iff \exists y\, Q(x,y)$, where Q is recursive. Then $P(f(x)) \iff \exists y\, Q(f(x), y)$, and $Q(f(x), y)$ is recursive. ■4.2.8

COROLLARY 4.2.9. *Every complete axiomatised theory is decidable.*

PROOF. Let T be an axiomatised theory. Let $P = \{\ulcorner\varphi\urcorner \colon \varphi \in T\}$, $Q = \{\ulcorner\varphi\urcorner \colon \neg\varphi \in T\}$. Since T is axiomatised, P is r.e. Therefore Q is r.e. Since T is complete, $Q = \mathbb{N} \setminus P$, so P is recursive. ■4.2.9

EXAMPLE 4.2.10. ACF_p is decidable for every p prime or zero.

4.3. Representation of recursive functions

We may now define our goal more precisely: we will show that the theory of Arithmetic $\mathrm{Th}(\mathbb{N}, 0, s, +, \cdot)$ cannot be axiomatised. Equivalently: no consistent set of axioms for the natural numbers axiomatises a complete theory.

The "standard" set of axioms for the natural numbers is called Peano's Arithmetic, or PA: $\langle \mathbb{N}, 0, s, +, \cdot \rangle$:

(PA1) $\forall x\,(sx \neq 0)$

(PA2) $\forall x \forall y\,(sx = sy \to x = y)$

(PA3) $\forall x\,(x + 0 = x)$

(PA4) $\forall x \forall y\,(x + sy = s(x + y))$

(PA5) $\forall x\,(x \cdot 0 = 0)$

(PA6) $\forall x \forall y\,(x \cdot sy = x \cdot y + x)$

(PA7) $\forall \bar{x}\,\big((\varphi(\bar{x}, 0) \wedge \forall y\,(\varphi(\bar{x}, y) \to \varphi(\bar{x}, sy))) \to \forall y\,\varphi(\bar{x}, y)\big)$

The last axiom is in fact a scheme, called the induction scheme (for obvious reasons). It is sometimes convenient to add another symbol $<$, and the axiom

$$\forall x \forall y\,((x < y) \leftrightarrow \exists z\,(y = x + s(z))).$$

Modulo this additional axiom, every formula with $<$ is equivalent to one without $<$, so this addition changes nothing essential.

Peano's Arithmetic captures, in some sense, all of our intuition about what *should* be true in $\mathbb{N}$. The set of axioms we gave is easily verified to be decidable, so PA is axiomatised and therefore enumerable.

NOTATION 4.3.1. For every natural number n, k_n is the $\mathcal{L}$-term $s^n 0$ (clearly, $k_n^{\mathbb{N}} = n$). Such a term is sometime called *numeral*.

DEFINITION 4.3.2. Let T be an $\mathcal{L}$-theory.

(i) We say that a partial function $f : \mathbb{N}^n \dashrightarrow \mathbb{N}$ is *representable* in T if there is a formula $\varphi(\bar{x}, y)$ such that for every tuple $\bar{a} \in \mathbb{N}^n$:

$$f(a_0, \ldots, a_{n-1}) = b \Longrightarrow T \vDash \forall y\,(\varphi(k_{a_0}, \ldots, k_{a_{n-1}}, y) \leftrightarrow y = k_b)$$

For tuples $\bar{a}$ for which $f(\bar{a})$ is not defined there is no requirement (thus a function with an empty domain is vacuously representable).

(ii) We say that a relation $P(\bar{x})$ is *representable* in T if there is a formula $\varphi(\bar{x})$ such that:

$$P(a_0, \ldots, a_{n-1}) \Longrightarrow T \vDash \varphi(k_{a_0}, \ldots, k_{a_{n-1}})$$
$$\neg P(a_0, \ldots, a_{n-1}) \Longrightarrow T \vDash \neg\varphi(k_{a_0}, \ldots, k_{a_{n-1}})$$

(If φ uses connectives and quantifiers other than $\neg, \to, \forall$, and $\tilde{\varphi}$ is a logically equivalent formula which is restricted to $\neg, \to, \forall$, then φ represents a function or a predicate if $\tilde{\varphi}$ does. Note that this does not depend on the choice of $\tilde{\varphi}$.)

Say that a set $P \subseteq \mathbb{N}^n$ is r.e. if $\{\langle \bar{a} \rangle : \bar{a} \in P\}$ is.

LEMMA 4.3.3. *Let $f\colon \mathbb{N}^n \to \mathbb{N}$ be a total function, and assume its graph $\{\bar{a}, f(\bar{a})\colon \bar{a} \in \mathbb{N}^n\}$ is r.e. Then f is recursive (and its graph is therefore recursive as well).*

PROOF. Since the graph is r.e., there is a recursive Q such that $f(\bar{a}) = b \iff \exists y\, Q(\langle \bar{a}, b\rangle, y)$. Define

$$f_1(\bar{x}) = \mu y\, Q(\langle \bar{a}, (y)_0\rangle, (y)_1).$$

Then f_1 is recursive, and for all $\bar{a}$, $f_1(\bar{a})$ is a pair $\langle b, c\rangle$, where $b = f(\bar{a})$ and c is such that $Q(\langle \bar{a}, b\rangle, c)$ (i.e., c witnesses that $f(\bar{a}) = b$.

Now $f(\bar{x}) = (f_1(\bar{x}))_0$. ■4.3.3

PROPOSITION 4.3.4. *Assume that $f(\bar{x})$ is a total function and is representable in an enumerable theory T. Then f is recursive.*

PROOF. Since T is enumerable, $\hat{T} = \{\ulcorner\varphi\urcorner\colon \varphi \in T\}$ is r.e. Assume that f is represented by the formula $\varphi(\bar{x}, y)$. Then the function $h(\bar{a}, b) = \ulcorner\forall y\, (\varphi(\bar{k_a}, y) \leftrightarrow y = k_b)\urcorner$ is recursive, and therefore the graph of f is given by:

$$Gr(f) = \{(\bar{a}, b)\colon f(\bar{a}) = b\} = \{(\bar{a}, b)\colon h(\bar{a}, b) \in \hat{T}\}.$$

By Lemma 4.2.8, $Gr(f)$ is r.e., whereby f is recursive. ■4.3.4

In order to prove a converse to this result we need to show that certain sentences are provable from T. This requires that T have some minimal strength. Peano's Arithmetic is much stronger than is really needed for this. We will axioms for a theory N, chosen to be just strong enough for the purpose of representing recursive functions.

Axioms $N1-6$ are the same as $PA1-6$, and we replace the axiom scheme $PA7$ with three new axioms (not schemes):

(N1) $\forall x\, (sx \neq 0)$

(N2) $\forall x \forall y\, (sx = sy \to x = y)$

(N3) $\forall x\, (x + 0 = x)$

(N4) $\forall x \forall y\, (x + sy = s(x + y))$

(N5) $\forall x\, (x \cdot 0 = 0)$

(N6) $\forall x \forall y\, (x \cdot sy = x \cdot y + x)$

(N7) $\forall x\, \neg(x < 0)$

(N8) $\forall x \forall y\, (x < sy \leftrightarrow (x < y \vee x = y))$

(N9) $\forall x \forall y\, (x < y \vee x = y \vee y < x)$

This theory is very weak (try and prove something useful from it...)

LEMMA 4.3.5. *Say that the term $\tau(\bar{x})$ represents a total function $f(\bar{x})$ in T if for every $\bar{a}$: $T \vdash \tau(\bar{k_a}) = k_{f(\bar{a})}$. In this case, the formula $\tau(\bar{x}) = y$ represents f in T.*

PROOF. The formula $\forall y \left((\tau(\bar{k_a}) = y) \leftrightarrow y = k_{f(\bar{a})}\right)$ is logically equivalent to $\tau(\bar{k_a}) = k_{f(\bar{a})}$. By the Completeness Theorem, T proves one if and only if T proves the other. ■4.3.5

LEMMA 4.3.6. *Fix $T = N$.*

(i) *The relation $=$ is represented by the formula $x = y$.*
(ii) *The function $+$ is represented by the term $x + y$ (and therefore by the formula $x + y = z$).*
(iii) *The function $\cdot$ is represented by the term $x \cdot y$ (and therefore by the formula $x \cdot y = z$).*
(iv) *The relation $<$ is represented by the formula $x < y$.*
(v) *The projection function $\pi_{n,m}$ is represented by the variable x_m viewed as a term $t(x_{<n})$.*

PROOF. (i) We need to prove that $n = m \Longrightarrow N \vdash k_n = k_m$ and $n \neq m \Longrightarrow N \vdash k_n \neq k_m$. The first is clear. For the second, assume that $n < m$, and prove by induction on n: For $n = 0$, this follows from N1; and if we assume that $N \vdash k_n \neq k_m$, then by N2: $N \vdash k_{n+1} \neq k_{m+1}$.

(ii) We need to prove that for every m, n: $N \vdash k_m + k_n = k_{m+n}$. We proceed by induction on n: For $n = 0$, this is by N3; and if $N \vdash k_m + k_n = k_{m+n}$, then by N4: $N \vdash k_m + k_{n+1} = k_{m+n+1}$.

(iii) Similarly, using N5 and N6.

(iv) We need to prove that:

$$n < m \Longrightarrow N \vdash k_n < k_m \tag{1}$$

$$n \geq m \Longrightarrow N \vdash \neg(k_n < k_m) \tag{2}$$

We do so by induction on m. For $m = 0$, (1) is vacuously true, and (2) follows from N7. Assume now that (1) and (2) hold for a fixed m (and for every n), and let us prove for $m + 1$. Note that $k_{m+1} = sk_m$.

If $n < m + 1$, then either $n < m$ or $n = m$. In the former case we have $N \vdash k_n < k_m$ by (1), and in the latter $\vdash k_n = k_m$. In either case, it follows from N8 that $N \vdash k_n < k_{m+1}$. On the other hand, if $n \geq m+1$, then $N \vdash \neg(k_n < k_m)$ by (2), and $N \vdash k_n \neq k_m$ since $x = y$ represents equality. Thus by N8: $N \vdash \neg(k_n < k_{m+1})$.

(v) Immediate.

■4.3.6

LEMMA 4.3.7. *A relation $P(\bar{x})$ is representable (in N) if and only if its characteristic function χ_P is. In fact, this is true for every theory T satisfying $T \vdash k_0 \neq k_1$.*

PROOF. Assume that $\varphi(\bar{x})$ represents P in T. Then $(\varphi(\bar{x}) \wedge y = k_1) \vee (\neg\varphi(\bar{x}) \wedge y = k_0)$ represents χ_P in T.

Conversely, assume that $\psi(\bar{x}, y)$ represents χ_P in T. Then $\psi(\bar{x}, k_1)$ represents P, since we said that $T \vdash k_0 \neq k_1$.

Since $N \vdash k_0 \neq k_1$, this is true in particular for $T = N$. ■4.3.7

LEMMA 4.3.8. *For every n:*

$$N \vdash \forall x \, (x < k_n \leftrightarrow \bigvee_{i<n} x = k_i)$$

(For $n = 0$, the empty disjunction is "false", so replacing it with $x \neq x$ will do.)

PROOF. By induction on n. For $n = 0$, we need to prove that $N \vdash \forall x \, (x < 0 \leftrightarrow x \neq x)$ which is true by N7. Assume now for n, and prove for $n + 1$. By N8: $N \vdash \forall x \, (x < k_{n+1} \leftrightarrow (x < k_n \vee x = k_n))$, and by the induction hypothesis: $N \vdash \forall x \, (x < k_{n+1} \leftrightarrow (\bigvee_{i<n} x = k_i \vee x = k_n))$ as required. ■4.3.8

LEMMA 4.3.9. *Assume that $f(\bar{x}) = h(g_0(\bar{x}), \ldots, g_{m-1}(\bar{x}))$, that $h(x_0, \ldots, x_{m-1})$ is represented by $\psi(x_0, \ldots, x_{m-1})$ and that each $g_i(x_0, \ldots, x_{n-1})$ is represented by $\varphi_i(x_0, \ldots, x_{n-1})$ for all $i < m$. Then f is represented by the formula:*

$$\exists z_0 \ldots \exists z_{m-1} \left(\psi(\bar{z}, y) \wedge \bigwedge_{i<m} \varphi_i(\bar{x}, z_i) \right).$$

PROOF. Easy. ■4.3.9

LEMMA 4.3.10. *Assume that $f(\bar{x}, y)$ is represented by $\varphi(\bar{x}, y, z)$, and $g(\bar{x}) = \mu y \, (f(\bar{x}, y) = 0)$. Then g is represented by the following formula:*

$$\psi(\bar{x}, y) \stackrel{\text{def}}{=} \varphi(\bar{x}, y, k_0) \wedge \forall z \, ((z < y) \rightarrow \neg\varphi(\bar{x}, z, k_0)).$$

PROOF. Assume that $g(\bar{a}) = \mu y \, (f(\bar{a}, y) = 0) = b$. This means that $f(\bar{a}, b) = 0$ and $f(\bar{a}, c) > 0$ for all $c < b$. As we know that if $m > 0$ then $N \vdash k_m \neq k_0$, the assumption that φ represents f tells us that:

$$N \vdash \neg\varphi(\bar{k}_a, k_c, k_0) \qquad \text{for } c < b \tag{3}$$

$$N \vdash \varphi(\bar{k}_a, k_b, k_0) \tag{4}$$

As we know that $N \vdash \forall x \, (x < k_b \leftrightarrow \bigvee_{c<b} x = k_c)$, it follows that $N \vdash \psi(\bar{k}_a, k_b)$.

Assume now that $\mathfrak{M} \vDash N$, $r \in M$, and $\mathfrak{M} \vDash \psi(\bar{k}_a, r)$. By N9: $\mathfrak{M} \vDash r < k_b \vee r = k_b \vee r > k_b$. $\mathfrak{M} \vDash r < k_b$ is excluded since then $r = k_c^{\mathfrak{M}}$ for some $c < b$, so $\mathfrak{M} \vDash \varphi(\bar{k}_a, r, k_0)$ would contradict (3). $\mathfrak{M} \vDash r > k_b$ is excluded, since $\mathfrak{M} \vDash \forall z \, ((z < r) \rightarrow \neg\varphi(\bar{k}_a, z, k_0))$ would contradict (4). So necessarily $\mathfrak{M} \vDash r = k_b$, which shows that:

$$N \vdash \forall y \, (\psi(\bar{k}_a, y) \leftrightarrow y = k_b).$$

■4.3.10

THEOREM 4.3.11. *Every recursive function and relation is representable in N.*

PROOF. By Lemma 4.3.7, it would suffice to prove for every recursive function.

We know that $+$, $\cdot$, $\chi_=$, $\chi_<$ and all the projections are representable in N, and that the family of functions representable in N is closed under composition and the μ-operator. It follows that $\chi_\leq = \chi_= + \chi_<$ is representable in N, so all the basic recursive functions are representable. Therefore all the recursive functions are representable. ■4.3.11

COROLLARY 4.3.12. *A total function is recursive if and only if it is representable in N.*

4.4. Incompleteness

We now have the tools necessary to prove that the theory N is undecidable (see below) and incomplete; moreover, every consistent axiomatisable extension of N is incomplete.

DEFINITION 4.4.1. Two disjoint sets $P, Q \subseteq \mathbb{N}$ are *recursively inseparable* if there is no recursive set $R \subseteq \mathbb{N}$ such that $P \subseteq R \subseteq \mathbb{N} \setminus Q$.

THEOREM 4.4.2. *Let $P = \{\ulcorner\varphi\urcorner : N \vdash \varphi\}$ and $Q = \{\ulcorner\varphi\urcorner : N \vdash \neg\varphi\}$. Then P and Q are recursively inseparable.*

PROOF. Assume that there is such a recursive set R. Define:

$$S = \{n \in \mathbb{N} : FrSub(n, \ulcorner x\urcorner, \ulcorner k_n\urcorner) \notin R\}$$

(Recall that $FrSub(\ulcorner\varphi(x)\urcorner, \ulcorner x\urcorner, \ulcorner k_n\urcorner) = \ulcorner\varphi(k_n)\urcorner$.) Since R, $FrSub$ and $n \mapsto \ulcorner k_n\urcorner$ are all recursive, so is S. Therefore it is represented by a formula $\psi(x)$:

$$n \in S \Longrightarrow N \vdash \psi(k_n)$$
$$n \notin S \Longrightarrow N \vdash \neg\psi(k_n)$$

So, is $\ulcorner\psi\urcorner \in S$? Let us check both possibilities:

$$\begin{aligned}
\ulcorner\psi\urcorner \in S &\Longrightarrow N \vdash \psi(k_{\ulcorner\psi\urcorner}) \Longrightarrow \ulcorner\psi(k_{\ulcorner\psi\urcorner})\urcorner \in P \\
&\Longrightarrow FrSub(\ulcorner\psi\urcorner, \ulcorner x\urcorner, \ulcorner k_{\ulcorner\psi\urcorner}\urcorner) = \ulcorner\psi(k_{\ulcorner\psi\urcorner})\urcorner \in R \\
&\Longrightarrow \ulcorner\psi\urcorner \notin S \\
\ulcorner\psi\urcorner \notin S &\Longrightarrow N \vdash \neg\psi(k_{\ulcorner\psi\urcorner}) \Longrightarrow \ulcorner\psi(k_{\ulcorner\psi\urcorner})\urcorner \in Q \\
&\Longrightarrow FrSub(\ulcorner\psi\urcorner, \ulcorner x\urcorner, \ulcorner k_{\ulcorner\psi\urcorner}\urcorner) = \ulcorner\psi(k_{\ulcorner\psi\urcorner})\urcorner \notin R \\
&\Longrightarrow \ulcorner\psi\urcorner \in S
\end{aligned}$$

As neither $\ulcorner\psi\urcorner \in S$ nor $\ulcorner\psi\urcorner \notin S$ is possible, we have a contradiction. It follows that no recursive set can separate P and Q. ■4.4.2

DEFINITION 4.4.3. Recall that a consistent theory T is *decidable* if the set $\{\ulcorner\varphi\urcorner : T \vdash \varphi\}$ is recursive, otherwise it is undecidable. We say that T is *hereditarily undecidable* if every consistent extension $T' \supseteq T$ is undecidable.

COROLLARY 4.4.4. *N is hereditarily undecidable.*

PROOF. Assume the contrary, i.e., that there is a consistent theory $T \supseteq N$ which is decidable, namely that $R = \{\ulcorner\varphi\urcorner : T \vdash \varphi\}$ is recursive. Let P and Q be as in Theorem 4.4.2. Since T is consistent, $P \subseteq R \subseteq \mathbb{N} \setminus Q$, which is impossible since P and Q are recursively inseparable. ■4.4.4

Recall we showed (Corollary 4.2.9) that every complete axiomatised theory is decidable.

THEOREM 4.4.5. *No consistent axiomatisable extension of N is complete.*

PROOF. Such an extension would be decidable, but N is hereditarily undecidable. ■4.4.5

COROLLARY 4.4.6. *If T is a theory such that $T \cup N$ is consistent, then T is undecidable. If T is axiomatised, then it is incomplete.*

PROOF. Here we use the fact that N is finitely axiomatised. Let φ be the conjunction of all the axioms of N. Then we have $T \cup N \vdash \psi \iff T \vdash \varphi \to \psi$. Thus, if T were decidable, so would be the theory $\{\psi \colon T \cup N \vdash \psi\}$, but we know the latter is undecidable. Since T is undecidable, it cannot be both axiomatised and complete. ■4.4.6

COROLLARY 4.4.7. *Peano Arithmetic is undecidable and incomplete.*

We conclude with a similar result:

THEOREM 4.4.8 (Tarski). *Truth is not definable in $(\mathbb{N}, 0, s, +, \cdot)$, in the sense that there is no formula $\varphi(x)$ satisfying for all ψ:*

$$\mathbb{N} \vDash \psi \iff \mathbb{N} \vDash \varphi(\ulcorner\psi\urcorner).$$

PROOF. Assume there is such a formula $\varphi(x)$. There is a total recursive function f such that:

$$f(\ulcorner\chi(x)\urcorner) = \ulcorner\neg\chi(k_{\ulcorner\chi\urcorner})\urcorner.$$

Let $\theta(x, y)$ represent f in N, and let

$$\psi(x) = \exists y\,(\theta(x, y) \wedge \varphi(y)).$$

Then, as θ represents f in N, we have for all $\chi(x)$:

$$N \vDash \psi(k_{\ulcorner\chi\urcorner}) \leftrightarrow \varphi(k_{\ulcorner\neg\chi(k_{\ulcorner\chi\urcorner})\urcorner}).$$

As $\mathbb{N} \vDash N$, and letting $\chi = \psi$ we have:

$$\begin{aligned}\mathbb{N} \vDash \psi(k_{\ulcorner\psi\urcorner}) &\iff \mathbb{N} \vDash \varphi(k_{\ulcorner\neg\psi(k_{\ulcorner\psi\urcorner})\urcorner}) \\ &\iff \mathbb{N} \vDash \neg\psi(k_{\ulcorner\psi\urcorner}).\end{aligned}$$

A contradiction. ■4.4.8

4.5. A "physical" computation model: register machines

While we cannot formally prove Church's thesis, due to its vagueness, we can convince ourselves of its truth by the following intuitive argument. Assume that a function f is computable by some algorithm. Then regardless of the precise definition of the word algorithm, it should consist of a sequence of steps, starting with the input and ending with the output, and each step should be "easy" to compute. Thus the properties "x codes the initial state with input y", "x codes the state immediately following state y" and "x codes a terminal state" should be recursive relations, and the mapping of a code for a terminal state to its output should be a recursive function. Then "x code a full computation sequence" is recursive, and

$$f(x) = Output(h((x)_{\mathrm{len}(h(x))-1})).$$

Where:

$$h(x) = \mu y\,(y \text{ codes a computation sequence and } (y)_0 \text{ is initial with input } x).$$

We will give a concrete example of this using register machines. A register machine is an abstract computation model consisting of countable many registers $(r_i \colon i \in \mathbb{N})$, each of which capable of holding a natural number, and a finite sequence of instructions $(I_i \colon i < \ell)$. An instruction I_i can be any one of:

- "Increase r" (where r is a register).
- "Decrease r, else".
- "Go to I_n".

At every step of the execution of the programme, the "machine state" consists of the values (in $\mathbb{N}$) of the registers, as well as special instruction index which will be denoted $i \in \mathbb{N}$, indicating the next instruction to execute. As long as $i < \ell$ (the length of the programme), a single *execution step* consists of modifying the machine state according to the current instruction I_i:

- If I_i is "increase r", increase r and i by 1 (i.e., increase r and move to the next instruction).
- If I_i is "decrease r, else":
  - If $r = 0$, increase i by 1.
  - If $r > 0$, decrease r by 1 and increase i by 2.

  Thus, if $r > 0$ the next instruction is skipped.
- If I_i is "go to I_n", assign n to i.

An *execution* of the machine M on input $a_0, \ldots a_{n-1}$ consists of initialising $r_0, \ldots, r_{n-1}$ to $a_0, \ldots, a_{n-1}$ and all other registers to 0, initialising i to 0, and then performing execution steps as long as $i < \ell$. If at any point $i \geq \ell$ then the execution stops, and the contents of r_0 is the *output*.

If the execution of M on input $\bar{a}$ stops at some point we say that M *stops* on $\bar{a}$, in symbols $M(\bar{a}) \downarrow$. Otherwise, M does not stop on $\bar{a}$, in symbols $M(\bar{a}) \uparrow$.

If M is a register machine and $n \in \mathbb{N}$, M defines a partial function $f_{M,n} \colon \mathbb{N}^n \dashrightarrow \mathbb{N}$ as follows: $\mathrm{dom}(f_{M,n}) = \{\bar{a} \in \mathbb{N}^n \colon M(\bar{a}) \downarrow\}$, and for every $\bar{a} \in \mathrm{dom}(f_{M,n})$, $f_{M,n}(\bar{a})$ is the output of the execution of M on $\bar{a}$. We call $f_{M,n}$ the partial n-ary function *calculated* by M.

We would like to show that the partial recursive functions are precisely the ones which can be calculated by register machines.

One direction is essentially an exercise in programming. We start by observing that as there are infinitely many registers we can always use a register no other part of the programme uses.

We start by observing that we can always assign zero to a register:

I_0. Decrease r, else
I_1. Go to I_3.
I_2. Go to I_0.
I_3. ...

Once $r = 0$, the "go to I_3" is reached and the execution continues after the loop. We can of course place this piece of code anywhere in a programme (adjusting the "go to" instruction accordingly), shortening it to "let $r = 0$".

We can assign the value of r to r', r'' (all distinct), while setting r to zero:

I_0. Let $r' = 0$.
I_1. Let $r'' = 0$.
I_2. Decrease r, else
I_3. Go to I_7
I_4. Increase r'.
I_5. Increase r''.
I_6. Go to I_2
I_7. ...

Now, if r and r' are any two distinct registers, we can always choose a register s which is used nowhere else in the programme and first assign r to r', s, while setting r to zero, then assign back s to r, r' (setting s to zero). Then r remains unchanged, while r' is now equal to r. Again, we may place this anywhere in a programme, shortening it to "let $r' = r$".

We can now verify that some basic functions can indeed be calculated by register machines. To perform "let $r'' = r + r'$", we choose unused registers s, s':

I_0. Let $s = r$.
I_1. Let $s' = r'$.
I_2. Decrease s', else
I_3. Go to I_6
I_4. Increase s.
I_5. Go to I_2
I_6. Let $r'' = s$.

Note that there is no requirement here for r, r', r'' to be distinct.

Similarly for "let $r'' = r \cdot r'$":

I_0. Let $s = 0$.
I_1. Let $s' = r'$.
I_2. Decrease s', else
I_3. Go to I_6
I_4. Let $s = s + r$.
I_5. Go to I_2
I_6. Let $r'' = s$.

For "let $r'' = r \dot{-} r'$":

I_0. Let $s = r$.
I_1. Let $s' = r'$.
I_2. Decrease s', else
I_3. Go to I_7
I_4. Decrease s, else
I_5. Go to I_7.
I_6. Go to I_2.
I_7. Let $r'' = s$.

Finally, "let $r'' = \chi_{\leq}(r, r')$" is given by:

I_0. Let $s = r \dot{-} r'$.
I_1. Let $r'' = 0$.
I_2. Decrease s, else
I_3. Increase r''.

We conclude that all the basic recursive functions are calculable by register machines: for $+$, $\cdot$ and $\chi_{\leq}$ we showed this explicitly, while each of the projections $\pi_{n,m}$ is calculated by the programme "let $r_0 = r_m$".

We also claim that the family of functions calculable by register machines is closed under composition. Indeed, assume that $f\colon \mathbb{N}^n \dashrightarrow \mathbb{N}$ and $g_i\colon \mathbb{N}^m \dashrightarrow \mathbb{N}$ are all calculable by register machines for $i < n$. Then we can calculate $f \circ (g_0, \ldots, g_{n-1})\colon \mathbb{N}^m \dashrightarrow \mathbb{N}$ by:

I_0. Let $r_m = g_0(r_0, \ldots, r_{m-1})$.
I_1. Let $r_{m+1} = g_1(r_0, \ldots, r_{m-1})$.
...
I_{n-1}. Let $r_{m+n-1} = g_{n-1}(r_0, \ldots, r_{m-1})$.
I_n. Let $r_0 = f(r_m, \ldots, r_{m+n-1})$.

Note that this programme stops on input $\bar{a} \in \mathbb{N}^m$ if and only if $\bar{a} \in \mathrm{dom}(g_i)$ for all $i < n$ and $(g_0(\bar{a}), \ldots, g_{n-1}(\bar{a})) \in \mathrm{dom}(f)$, i.e., if and only if $\bar{a} \in \mathrm{dom}(f \circ \bar{g})$.

Finally, we claim that if $f\colon \mathbb{N}^{n+1} \dashrightarrow \mathbb{N}$ is calculable by a register machine, then so is $h(\bar{x}) = \mu y\,(f(\bar{x}, y) = 0)$. Indeed, we can calculate h with the programme:

I_0. Let $s = f(r_0, \ldots, r_{n-1}, r_n)$.
I_1. Decrease s, else

I_2. Go to I_5.
I_3. Increase r_n.
I_4. Go to I_0.
I_5. Let $r_0 = r_n$.

Again, we verify easily that this stops on $\bar{a}$ if and only if $\bar{a} \in \mathrm{dom}(h)$, and in this case the result is

We conclude that every partial recursive function is calculable by a register machine.

Now we turn to the converse. First, we observe we can code register machines, i.e., programmes:

$$\begin{aligned}
&\ulcorner \text{Increase } r_n \urcorner && = \langle 0, n\rangle,\\
&\ulcorner \text{Decrease } r_n, \text{ else} \urcorner && = \langle 1, n\rangle,\\
&\ulcorner \text{Go to } I_n \urcorner && = \langle 2, n\rangle,\\
&\ulcorner M \urcorner = \ulcorner (I_i \colon i < \ell) \urcorner && = \langle \ulcorner I_0 \urcorner, \ldots, \ulcorner I_{\ell-1} \urcorner \rangle.
\end{aligned}$$

In the last line, $\ulcorner M \urcorner$ is the code for the register machine M whose programme is $(I_i \colon i < \ell)$.

Similarly, given a machine state, i.e., an integer value for the instruction index i as well as to the registers $\{r_i \colon i < \omega\}$, all but finitely many of which being zero, we let $m < \omega$ be least such that $r_i = 0$ for all $i \geq m$, and code the state by $\langle i, r_0, \ldots, r_{m-1}\rangle$ (if $m = 0$ this is just $\langle i \rangle$). We leave it for the reader to verify that the following relations are recursive (and in fact primitive recursive):

- x codes a machine state.
- x codes a programme.
- x and y code machine states, z codes an instruction, and y is the result of executing z in state x.
- x and y code machine states, z codes a programme, and y is the state following x in the execution of z.
- x is a terminal state for the execution of z (i.e., the instruction index of state x lies outside the programme z).
- x codes an execution sequence for programme y on input z, i.e.:
  - x and z are sequence numbers.
  - $(x)_0$ is the initial machine state for input z: $i = 0$, $r_j = (z)_j$ for $j < \mathrm{len}(z)$, and $r_j = 0$ for $j \geq \mathrm{len}(z)$.
  - For all $i < \mathrm{len}(x) - 1$: $(x)_{i+1}$ is the state following $(x)_i$ in the execution of y.
  - $(x)_{\mathrm{len}(x)-1}$ is a terminal state for y.

We now define a partial recursive function $u_0(x, y)$ as:

$$u_0(x, y) = \mu z\, (z \text{ codes an execution sequence of programme } x \text{ on input } y).$$

Note that $u_0(\ulcorner M \urcorner, \langle a_0, \ldots, a_{n-1} \rangle)$ is defined if and only if M stops on input $a_0, \ldots, a_{n-1}$. Define now:

$$u(x, y) = \text{ value of } r_0 \text{ in the state } u_0(x, y).$$

Then $u(\ulcorner M \urcorner, \langle \bar{a} \rangle)$ is defined if and only if $M(\bar{a}) \downarrow$, in which case $u(\ulcorner M \urcorner, \langle \bar{a} \rangle)$ is equal to the output of M on input $\bar{a}$. In other words, for every $n < \omega$, the function $f_{M,n}$ is given by:

$$f_{M,n}(\bar{x}) = u(\ulcorner M \urcorner, \langle \bar{x} \rangle).$$

It is in particular recursive.

We conclude:

THEOREM 4.5.1. *A partial function $f \colon \mathbb{N}^n \dashrightarrow \mathbb{N}$ is recursive if and only if it is of the form $f_{M,n}$ for some register machine M.*

But in fact, we obtained more than that: the function u gives us a *uniform enumeration* of all recursive functions. For all $i < \omega$ we define $\varphi_i \colon \mathbb{N} \dashrightarrow \mathbb{N}$ by:

$$\varphi_i(x) = u(i, \langle x \rangle).$$

Then every φ_i is a partial recursive function, and every partial recursive function $f \colon \mathbb{N} \dashrightarrow \mathbb{N}$ is equal to some φ_i.

Exercises

EXERCISE 4.1. Show that every finite set $P \subseteq \mathbb{N}$ is recursive.

Show that if $P \subseteq \mathbb{N}$ is infinite, P is recursive if and only if there is a total recursive strictly increasing function $f \colon \mathbb{N} \to \mathbb{N}$ whose range is P.

EXERCISE 4.2. Recall the definition of primitive recursive functions from Remark 4.1.7.

Show (briefly) that all the basic recursive functions ($\chi_{\leq}$, $+$, $\cdot$, and projections) are primitive recursive.

Argue (again, briefly) why in Section 4.1, in the items concerning constant functions, recursive predicate, Boolean combinations and definition by cases, we could replace everywhere "recursive" with "primitive recursive" (where a predicate is primitive recursive if its characteristic function is).

Show that the factorial function is primitive recursive.

EXERCISE 4.3. Let $P(\bar{x}, y)$ be a primitive recursive predicate. Show that the function $f(\bar{x}, z) = \mu y_{<z} P(\bar{x}, y)$ is primitive recursive (remember, use of the μ-operator is not allowed).

Deduce that the coding function β is primitive recursive.

EXERCISE 4.4. Show that for every n, the function $(a_0, \ldots, a_{n-1}) \mapsto \langle a_0, \ldots, a_{n-1} \rangle$ is primitive recursive. (Hint: look at the proof of Proposition 4.1.6.)

EXERCISE 4.5. Let $P, Q \subseteq \mathbb{N}^n$ be r.e. Then there are recursive relations $P', Q' \subseteq \mathbb{N}^{n+1}$ such that $P(\bar{x}) \iff \exists y\, P'(\bar{x}, y)$ and $Q(\bar{x}) \iff \exists y\, Q'(\bar{x}, y)$ (why?) Let $\varphi(\bar{x}, y)$ and $\psi(\bar{x}, y)$ represent P' and Q' in N, respectively, and let:

$$\chi(\bar{x}) = \exists y\, (\varphi(\bar{x}, y) \wedge \forall z\, (z < y \to \neg\psi(\bar{x}, z))).$$

Show that:

$$\bar{a} \in P \smallsetminus Q \Longrightarrow N \vdash \chi(k_{\bar{a}})$$
$$\bar{a} \in Q \smallsetminus P \Longrightarrow N \vdash \neg\chi(k_{\bar{a}}).$$

EXERCISE 4.6. Let T be a consistent axiomatisable extension of N. Show there exists an r.e. predicate $Q \subseteq \mathbb{N}^{n+1}$ such that for every formula $\varphi(\bar{x}, y)$ (where $|\bar{x}| = n$) and $\bar{a} \in \mathbb{N}^n$:

$$Q(\bar{a}, \ulcorner\varphi\urcorner) \iff T \vdash \varphi(k_{\bar{a}}, k_{\ulcorner\varphi\urcorner}).$$

EXERCISE 4.7. Let $T \supseteq N$ be an axiomatisable consistent extension of the theory N. Say that a predicate $P \subseteq \mathbb{N}^n$ is *weakly represented* in T by a formula $\varphi(\bar{x})$ if for all $\bar{a} \in \mathbb{N}^n$: $\bar{a} \in P \iff T \vdash \varphi(k_{\bar{a}})$. We say that $P \subseteq \mathbb{N}^n$ is *weakly representable in* T if it is weakly represented in T by some formula.

Let $P \subseteq \mathbb{N}^n$ be r.e., T as above. Let $P_1 = P \times \mathbb{N} \subseteq \mathbb{N}^{n+1}$, and $Q \subseteq \mathbb{N}^{n+1}$ as in the previous exercise. As both P_1 and Q are r.e. (why?), there is a formula $\chi(\bar{x}, y)$ such that:

$$(\bar{a}, b) \in P_1 \smallsetminus Q \Longrightarrow N \vdash \chi(k_{\bar{a}}, k_b)$$
$$(\bar{a}, b) \in Q \smallsetminus P_1 \Longrightarrow N \vdash \neg\chi(k_{\bar{a}}, k_b).$$

Let $\varphi(\bar{x}) = \chi(\bar{x}, k_{\ulcorner\chi\urcorner})$. Show that φ weakly represents P in T.

EXERCISE 4.8. Conclude that if T is an axiomatisable consistent extension of N then P is weakly representable in T if and only if P is r.e. (there is a converse here to show as well).

EXERCISE 4.9. Show that a subset $A \subseteq \mathbb{N}$ is recursively enumerable if and only if it is the domain of a partial recursive function. (Hint: think in terms of execution of register machines.) The domain of φ_i (i.e., the ith r.e. set) is denoted by W_i.

CHAPTER 5

Set theory

We study the abstract notion of a set. Intuitively, sets are collections of objects: chairs, theorems, and possibly other sets. But: if we admit every conceivable collection of objects as a set we may encounter paradoxes, such as Russel's:

> Let A be the set of all sets which are not members of themselves. Then A is a member of itself if and only if it isn't.

The common solution to this is that not all collections are sets; rather, there are certain constructions that allow us to deduce that various collections of objects are indeed sets. Also, for the purposes of serving as a foundation for mathematics, we might as well assume that all sets are "pure" sets, namely that there are no non-set objects involved.

5.1. Axioms for set theory

Our language for sets will consist of a single relation symbol $\in$, where $x \in y$ means "x is a member of y". We will introduce as we go various shorthand notations such as $x \subseteq y$ for $\forall t(t \in x \to t \in y)$, etc.

5.1.1. Zermelo-Fraenkel axioms for set theory. Let us start with Zermelo's axioms for set theory, denoted Z. All free variables are quantified universally.

We start with two axioms which we call "structural", as they tell us something about the nature of sets:

- **Extensionality:**

  $$x = y \leftrightarrow \forall t(t \in x \leftrightarrow t \in y).$$

  This tells us that a set is indeed nothing but the collection of all its members: if two have the same members then they are the same. In particular, there exists (at most) one empty set which will be denoted by $\varnothing$.
- **Foundation (or regularity):**

  $$x \neq \varnothing \to \exists t \in x(t \cap x = \varnothing),$$

  i.e.,

  $$\exists t(t \in x) \to \exists t(t \in x \wedge \forall y \neg(y \in t \wedge y \in x)).$$

  This tells us that the universe of sets is well-founded. We will get back to that later.

A *class* is a collection of sets defined by a first order formula, possibly with parameters, i.e., something of the form $\{x\colon \varphi(x,\bar{a})\}$ where $\varphi(x,\bar{y})$ is a formula and $\bar{a}$ is a tuple of sets. If a is a set we identify it with the class $\{x\colon x \in a\}$ (this is legitimate by the extensionality axiom). If $C = \{x\colon \varphi(x,\bar{a})\}$ is a class, we write $x \in C$ as shorthand for $\varphi(x,\bar{a})$ A class which does not come from a set in this manner is called a *proper class*.

The class of all sets is traditionally denoted V.

REMARK 5.1.1. A word of caution: if a and b are two sets, then $x \in a$ and $x \in b$ are two formulae which are both instances of $x \in y$, and only differ in the parameter (a or b) assigned to the *parameter variable* y. On the other hand, if C and D are two distinct classes, then the "formulae" $x \in C$ and $x \in D$ are shorthands for two possibly very different formulae.

Most of the other axioms are "set existence" axioms, i.e., axioms telling us that certain classes are in fact sets:

- **Pairing:**
$$\exists\{x,y\},$$
i.e.,
$$\exists z\,\forall t\,(t \in z \leftrightarrow t = x \vee t = y).$$
- **Union:**
$$\exists \bigcup x,$$
where $\bigcup x = \bigcup_{z\in x} z$, i.e.,
$$\exists y \forall t\,(t \in y \leftrightarrow \exists z(t \in z \wedge z \in x)).$$
- **Power set:**
$$\exists \mathcal{P}(x),$$
where $\mathcal{P}(x) = \{t\colon t \subseteq x\}$, i.e.,
$$\exists y \forall t(t \in y \leftrightarrow t \subseteq x).$$
(We recall that $t \subseteq x$ is shorthand for $\forall z\,(z \in t \to z \in x)$.)
- **Subset (or separation) scheme:** For every formula $\varphi(t,\bar{w})$:
$$\exists\{t \in x\colon \varphi(t,\bar{w})\},$$
i.e.,
$$\exists y \forall t\,(t \in y \leftrightarrow (t \in x \wedge \varphi(t,\bar{w}))).$$
Alternatively, this can be restated as: "the intersection of a class with a set is a set".
- **Infinity:** Let us introduce further terminology: If x is a set then its *successor* is defined as $x \cup \{x\}$ (should it exist as a set). A set x is *inductive* if $\varnothing \in x$ and if $y \in x$ then $y \cup \{y\} \in x$. The infinity axioms says:
There exists an inductive set,

i.e.:

$$\exists x(\varnothing \in x \wedge \forall y(y \in x \to (y \cup \{y\}) \in x)).$$

While the infinity axiom does not specify the set x entirely, together with the other axioms it can be shown to be equivalent to the statement that the class of all natural numbers is a set (the minimal inductive set).

These axioms form what is called Zermelo set theory, denoted Z. They are not strong enough, and we usually add to them the following axiom scheme (again, a set existence axiom). Together they form the Zermelo-Fraenkel set theory, or ZF:

- **Replacement:** For every formula $\varphi(u, v, \bar{w})$:
  If $\bar{w}$ are such that $\{(u, v)\colon \varphi(u, v, \bar{w})\}$ defines the graph of a "partial function", then the image of every set x under this function exists,

i.e.,

$$\begin{aligned} &\forall uvv' \left(\varphi(u, v, \bar{w}) \wedge \varphi(u, v', \bar{w}) \to v = v'\right) \\ \to \quad &\exists y \forall v \left(v \in y \leftrightarrow \exists u(u \in x \wedge \varphi(u, v, \bar{w}))\right) \end{aligned}$$

5.1.2. Pairs and functions.

Definition 5.1.2. For any two sets x, y, let $(x, y) = \{\{x, y\}, \{x\}\}$. This is a set by the pairing axiom. We call a set of the form (x, y) an *ordered pair*.

Note that $\{x, x\} = \{x\}$ and $(x, x) = \{\{x\}\}$.

Lemma 5.1.3. *For all x, y, z, w: $(x, y) = (z, w)$ if and only if $x = z$ and $y = w$.*

Proof. Exercise. ■5.1.3

Let us observe a few trivial consequences of the axioms. First, if A and B are classes, we define the classes $A \cup B = \{x\colon x \in A \vee x \in B\}$ and $A \times B = \{(x, y)\colon x \in A \wedge y \in B\}$.

If A and B are sets $\{A, B\}$ is a set, whereby $\bigcup\{A, B\} = A \cup B$ is a set. Then $A \times B \subseteq \mathcal{P}(\mathcal{P}(A \cup B))$, so by the subset and power set axioms (and existence of finite unions observed earlier) $A \times B$ is a set.

Definition 5.1.4. A *function* is a set f, all of whose members are ordered pairs, and such that $\forall xyz\,(x, y) \in f \wedge (x, z) \in f \to y = z$.

If f is a function we define is *domain* and range as

$$\operatorname{dom}(f) = \{x\colon \exists y\,(x, y) \in f\} \qquad \operatorname{rng}(f) = \{x\colon \exists y\,(y, x) \in f\}.$$

If A is a set and B a class then the notation $f\colon A \to B$ means that f is a function, $\operatorname{dom}(f) = A$ and $\operatorname{rng}(f) \subseteq B$.

Lemma 5.1.5. *The domain and range of a function f (which are a priori classes) are sets.*

Proof. Let $A = \bigcup\bigcup f$. Then A is a set by the union axioms, and $A = \operatorname{dom}(f) \cup \operatorname{rng}(f)$. By the subset axiom $\operatorname{dom}(f)$ and $\operatorname{rng}(f)$ are sets. ■5.1.5

If A is a set and B a class we define B^A as the class of all functions $f\colon A \to B$. If B is also a set then $B^A \subseteq \mathcal{P}(B \times A)$ is a set as well.

5.1.3. The axiom of choice.

DEFINITION 5.1.6. Let x be a set. Define $\mathcal{P}^-(x) = \mathcal{P}(x) \setminus \{\varnothing\}$. A *choice function* for x is a function $f\colon \mathcal{P}^-(x) \to x$ such that $f(y) \in y$ for all $\varnothing \neq y \subseteq x$.

One last axiom is the Axiom of Choice, which is special since it is a set existence axiom which is non-constructive (i.e., we say that a set with a certain property exists without being able to say which are precisely its elements):

- **Choice:** Every set admits a choice function.

We will be very careful with our use of the Axiom of Choice (AC), and mention explicitly for which results it is needed.

The most common axiom system for set theory is ZFC, standing for Zermelo-Fraenkel plus Choice.

5.2. Well ordered sets

In this section we will intentionally avoid using the Foundation axiom.

5.2.1. Properties of ω.

LEMMA 5.2.1. *Let C be a non-empty set, or even a non-empty class. Then $\bigcap C = \bigcap_{y \in C} y$ is a set.*

PROOF. As every set is a class we may assume that C is a class, and as it is non-empty, let $b \in C$. Then

$$\bigcap C = \{x \in b\colon \forall y(y \in C \to x \in y)\},$$

which exists by the subset axiom. ■5.2.1

COROLLARY 5.2.2. *There exists a minimal inductive set, denoted ω.*

PROOF. The property "x is inductive" can be defined by a first order formula and is thus a class, call it Ind. This is a non-empty class by the infinity axiom, so its intersection $\omega := \bigcap Ind$ exists. Then $\varnothing \in \omega$, since $\varnothing$ belongs to all inductive sets, and if $y \in \omega$ then y belongs to all $x \in Ind$, so $y \cup \{y\}$ belongs to every $x \in Ind$, whereby $y \cup \{y\} \in \omega$. Therefore ω is inductive, and is minimal such. ■5.2.2

DEFINITION 5.2.3. A set a is *transitive* if $\forall x\,(x \in a \to x \subseteq a)$ (i.e., if $c \in b \in a \to c \in a$).

(i) ω is transitive.
Indeed, otherwise let $\omega' = \{x \in \omega\colon x \subseteq \omega\}$. Then it is easy to see that ω' is inductive whereby $\omega' = \omega$.

(ii) Every $n \in \omega$ is transitive.
Same argument with $\omega' = \{x \in \omega\colon x \text{ is transitive}\}$.

(iii) If $n \in \omega$ then $n \notin n$. It follows that $\omega \notin \omega$.
Same argument with $\omega' = \{x \in \omega \colon x \notin x\}$.
(iv) If $n \in \omega$ then for all $m \in n$: either $S(m) \in n$ or $S(m) = n$.
As usual, let $\omega' \subseteq \omega$ be the set of all $n \in \omega$ having this property and observe that ω' is inductive.

It follows that $\in$ defines a strict partial ordering (transitive, anti-reflexive relation) on ω. If $n \in \omega$ then $n \subseteq \omega$, and as n is transitive it is downward-closed in ω, i.e., it is an initial segment. It is a proper initial segment since $n \notin n$.

For $m, n \in \omega$ we will write $m < n$ and $m \in n$ interchangeably. Then for all $n \in \omega$: $n = \{m \in \omega \colon m < n\}$.

LEMMA 5.2.4. *Let $x \subseteq \omega$ be an initial segment. Then for all $n \in \omega$ precisely on of the following holds: $n \in x$, $n = x$ or $x \in n$.*

PROOF. Since $\in$ is transitive and anti-reflexive on ω the three possibilities are mutually exclusive. Let $\omega' \subseteq \omega$ be the set of all n such that one of the three condition holds.

If $x \neq \varnothing$ then $\varnothing \in x$, so $\varnothing \in \omega'$. Assume that $n \in \omega'$. If $x = n$ or $x \in n$ then $x \in S(n) = n \cup \{n\}$. So assume $n \in x$, which implies that $S(n) \subseteq x$. Assume that $S(n) \neq x$. Then there is $m \in x \smallsetminus S(n)$, and as x is downward-closed: $m \subseteq x$. Since $n \in m$, either $S(n) \in m \subseteq x$ or $S(n) = m \in x$. Thus, either way, $S(n) \in \omega'$.

We conclude that $\omega' = \omega$. ■5.2.4

LEMMA 5.2.5. *The ordering of ω defined by $\in$ is total. Also, for all $m, n \in \omega$: $m \leq n \iff m \subseteq n$ (so $m \in n \iff m \subsetneq n$).*

PROOF. Let m, n. Then both are initial segments of ω, so either $m \in n$, $m = n$ or $n \in m$. If $m \in n$ or $m = n$ then $m \subseteq n$. Conversely, if $m \subseteq n$ then $n \notin m$ so either $m = n$ or $m \in n$. ■5.2.5

LEMMA 5.2.6. *The members of ω are precisely its proper initial segments.*

PROOF. Indeed, one direction was observed above. For the other, if $x \subseteq \omega$ is a proper initial segment, then there is $n \in \omega \smallsetminus x$. As x is an initial segment and $n \notin x$: $x \in S(n) \subseteq \omega$. ■5.2.6

LEMMA 5.2.7. *Let $A \subseteq \omega$ be non-empty. Then A contains a minimal element, which is precisely $\bigcap A$.*

PROOF. Let $x = \bigcap A$. Then it is a proper initial segment of ω (as the intersection of a non-empty family of such). Therefore $x = n \in \omega$. For all $m \in A$ we have $n \subseteq m \implies n \leq m$.

If $n \notin A$ then $n < m$ for all $m \in A$. But then $n \in \bigcap A = n$, which is impossible. Therefore $n \in A$. ■5.2.7

5.2.2. Well-ordered sets and transfinite induction.

DEFINITION 5.2.8. Let $(A, <)$ be an ordered set, i.e., A is a set and $<\subseteq A^2$ a relation on A satisfying the usual axioms. We say that $<$ is a *well-ordering* of A, or that $(A, <)$ is *well-ordered*, if every non-empty subset $B \subseteq A$ contains a minimal element with respect to $<$.

We say that $(\omega, \in \restriction_\omega)$ is well-ordered, where $\in \restriction_\omega = \{(n, m) \in \omega^2 \colon n \in m\}$.

FACT 5.2.9. *A subset of a well-ordered set is well-ordered (with the induced ordering).*

NOTATION 5.2.10. If $(A, <)$ is a totally ordered set and $a \in A$ then $A_{<a} = \{b \in A \colon b < a\}$.

The following principle generalises proof by induction to arbitrary well-ordered sets:

PROPOSITION 5.2.11 (Proof by transfinite induction). *Let $(A, <)$ be well-ordered, $B \subseteq A$. Assume that for all $a \in A$, if $A_{<a} \subseteq B$ then $a \in B$. Then $B = A$.*

PROOF. If $B \neq A$ then $C = A \setminus B$ is non-empty. Let $a \in C$ be minimal. Then $A_{<a} \subseteq B \implies a \in B$, a contradiction. ■5.2.11

DEFINITION 5.2.12. A *class function* is a class F of pairs (x, y) such that $\forall xyz\,(x, y) \in F \wedge (x, z) \in F \to y = z$. Its domain $\mathrm{dom}(F) = \{x \colon \exists y\,(x, y) \in F\}$ is a class.

THEOREM 5.2.13 (Definition by transfinite induction). *Let $(A, <)$ be a well-ordered set, and F a class function whose domain contains all functions whose domain is of the form $A_{<a}$. Then there exists a unique function $f \colon A \to V$ such that for all $a \in A$:*

$$(*) \qquad f(a) = F(f \restriction_{A_{<a}}).$$

(As V is the class of all sets, the notation $f \colon A \to V$ just says that $\mathrm{dom}(f) = A$.)

PROOF. Let $\varphi(x, y, A, <)$ say that $x \in A$, y is a function, $\mathrm{dom}(y) = A_{<x}$, and y satisfies $(*)$ for all $a \in A_{<x}$. This can be expressed with a first order formula.

We prove by transfinite induction that $(\forall x \in A)(\exists! y)\varphi(x, y, A, <)$, i.e., that for every $b \in A$ there exists a unique function $f_b \colon A_{<b} \to V$ such that $(*)$ holds for all $a < b$.

Indeed, assume this is true for all $c < b$, so for all such c f_c exists and is unique.

Define g as the function $c \mapsto F(f_c)$ for all $c < b$, i.e., as the set

$$\left\{(x, y) \colon \exists z \left(x \in A \wedge x < b \wedge \varphi(x, z, A, <) \wedge y = F(z)\right)\right\}.$$

This is indeed a set by the replacement axiom and the uniqueness of f_c for all $c < b$.

We claim that for all $c < b$: $g \restriction_{A_{<c}} = f_c$. Indeed, let $d < c$. Then then $f_c \restriction_{A_{<d}} = f_d$ by uniqueness of f_d. Therefore $g(d) = F(f_d) = F(f_c \restriction_{A_{<d}}) = f_c(d)$. Thus for all $c < b$: $g(c) = F(f_c) = F(g \restriction_{A_{<c}})$, so $\varphi(b, g, A, <)$ holds.

For uniqueness, assume that $\varphi(b, g', A, <)$. Then $g' \restriction_{A_{<c}} = f_c$ for all $c < b$ by uniqueness of f_c, whereby $g'(c) = F(f_c) = g(c)$, so $g = g'$.

This concludes the proof of the existence and uniqueness of f_b for all $b \in A$.

To conclude it is convenient to replace $(A, <)$ with $(A^*, <^*)$, where $A^* = A \cup \{*\}$, $*$ is a new element (not in A), and $<^*$ says that $*$ is greater than all members of A. It is easy to verify that $(A^*, <^*)$ is well-ordered.

Then $A^*_{<^**} = A$, and applying to proof above to $(A^*, <^*)$ instead of $(A, <)$ we obtain that f_* is the unique function satisfying the requirements. ■5.2.13

Observation: if $(A, <)$ is well-ordered, and $a \in A$ is not maximal, then it has a successor in A: this is $\min\{b \in A : b > a\}$.

Let $(A, <)$ be a well-ordered set. By Theorem 5.2.13 there is a function f whose domain is A, and satisfying for all $a \in A$:

$$f(a) = \mathrm{rng}(f\restriction_{A_{<a}}) = \{f(b) : b < a\}.$$

Let $\alpha = \mathrm{rng}(f)$. We observe that α shares many properties of ω:

- If $a, b \in A$ and $a < b$ then $f(a) \in f(b)$: since $f(a) \in \mathrm{rng}(f\restriction_{A_{<b}})$.
- f is injective, i.e., if $b < a$ then $f(a) \neq f(b)$. Indeed, otherwise let $a \in A$ be minimal such that there is $b < a$ such that $f(a) = f(b)$. Then $b < a \implies f(b) \in f(a) = f(b)$, so there is $c < b$ such that $f(b) = f(c)$, contradicting the minimality of a.
- If $a, b \in A$ $f(a) \in f(b)$ then $a < b$. Indeed, if $f(a) \in f(b)$ then there is $c < b$ such that $f(a) = f(c)$, so $a = c < b$.
- α is transitive: Indeed, assume $\beta \in \alpha$. Then $\beta = f(b) = \{f(a) : a < b\} \subseteq \alpha$.

We conclude that $f : A \to \alpha$ is an order-preserving bijection between $(A, <)$ and $(\alpha, \in)$. In particular, $\in$ defines a total order on α, and it is a well-ordering.

Definition 5.2.14. Let $(A, <_A)$ and $(B, <_B)$ be two ordered sets. we say that they have the same *order type* ($otp(A) = otp(B)$) if there exists a bijection $f : A \to B$ which is order-preserving, i.e., for all $a, b \in A$:

$$a <_A b \iff f(a) <_B f(b).$$

Let $(A, <_A)$ and $(B, <_B)$ be two well-ordered sets. Construct $f : A \to \alpha$ as above, and similarly $g : B \to \beta$, so $\beta = \mathrm{rng}(g)$ and for all $a \in B$: $g(a) = \{g(b) : b <_B a\}$. Then f witnesses that $otp(A, <) = otp(\alpha, \in)$, and g witnesses that $otp(B, <) = otp(\beta, \in)$.

We claim that $\alpha = \beta$ if and only if $(A, <)$ and $(B, <)$ have the same order type. Indeed, if $\alpha = \beta$ then $g^{-1} \circ f : A \to B$ witnesses that $otp(A, <) = otp(B, <)$. Conversely, assume that $h : A \to B$ is an order preserving bijection. We claim that $f(a) = g(h(a))$ for all $a \in A$. We prove this by induction on a: if this is true for all $b <_A a$ then:

$$f(a) = \{f(b) : b <_A a\} = \{g(h(b)) : b <_A a\} = \{g(b) : b \in B, b <_B h(a)\} = g(h(a)).$$

In particular: $\alpha = \mathrm{rng}(f) = \mathrm{rng}(g \circ h) = \mathrm{rng}(g) = \beta$.

Thus $(\alpha, \in)$ is a canonical representative of its order type, and we might as well define $\alpha = otp(A, <)$ (unfortunately, such an elegant canonical Representative of the order type only exists for well-orderings).

5.2.3. Ordinals.

DEFINITION 5.2.15. An *ordinal* is a transitive set on which $\in$ defines a well-ordering. The class of all ordinals is denoted ON (ordinal numbers). Usually ordinals are denoted by lowercase Greek letters: $\alpha, \beta, \gamma, \ldots$ but sometimes also $i, j, k, \ldots$.

REMARK 5.2.16. Given the Foundation Axiom, the assumption that $\in$ defines a well-ordering can be weakened to the assumption that $\in$ defines a total ordering.

EXAMPLE 5.2.17. If $(A, <)$ is well-ordered and $\alpha = otp(A, <)$ as constructed above, then α is an ordinal.

EXAMPLE 5.2.18. ω is an ordinal, and every natural number $n \in \omega$ is an ordinal.

A few properties of ordinals:

- All members of an ordinal α are ordinals.
  Indeed, if $\beta \in \alpha$ then $\beta \subseteq \alpha$, so $\in$ induces a total well-ordering on β. To see that β is transitive assume that $\delta \in \gamma \in \beta$. Then, as α is transitive: $\beta \in \alpha \Longrightarrow \gamma \in \alpha \Longrightarrow \delta \in \alpha$, and as $\in$ is an ordering on α: $\delta \in \gamma \in \beta \Longrightarrow \delta \in \beta$.
- The members of an ordinal α are precisely its proper initial segments in the ordering defined by $\in$.
  Indeed, let $\beta \in \alpha$. Then $\beta = \{\gamma \in \alpha \colon \gamma \in \beta\}$ (i.e., $\{\gamma \in \alpha \colon \gamma < \beta\}$) is an initial segment of α. Since $\beta \not< \beta$, β is a proper initial segment. Conversely, let $\beta \subseteq \alpha$ be a proper initial segment of α, and let $\gamma \in \alpha \setminus \beta$ be minimal. Then for all $\delta \in \alpha$: $\delta \in \beta \Longleftrightarrow \delta \in \gamma$, so $\beta = \gamma \in \alpha$.
- For two ordinals $\alpha, \beta \in ON$: $\alpha \subseteq \beta$ if and only if $\alpha \in \beta$ or $\alpha = \beta$, these are mutually exclusive.
  Follows from the previous item.

LEMMA 5.2.19. *The relation $\in$ defines a strict total order on ON.*

PROOF. First, $\alpha \in ON \Longrightarrow \alpha \notin \alpha$ since α is not a proper subset of itself, and if $\alpha, \beta, \gamma \in ON$ and $\alpha \in \beta \in \gamma$ then $\alpha \in \gamma$ by transitivity of γ. To see the order is total, let $\alpha, \beta \in ON$, and assume $\alpha \nsubseteq \beta$ (i.e., $\alpha \neq \beta$ and $\alpha \notin \beta$). Let $\gamma \in \alpha \setminus \beta \subseteq \alpha$ be minimal in α. Since γ is minimal, $\gamma \cap (\alpha \setminus \beta) = \varnothing$, whereby $\gamma \subseteq \beta$. Since γ is an ordinal, and therefore transitive, it is an initial segment of β. But $\gamma \notin \beta$, so it cannot be a proper initial segment. Therefore $\beta = \gamma \in \alpha$. ■5.2.19

From now on if $\alpha, \beta \in ON$ we write $\alpha < \beta$ and $\alpha \in \beta$ interchangeably. Thus if $\alpha \in ON$ then $\alpha = \{\beta \in ON \colon \beta < \alpha\}$.

COROLLARY 5.2.20. *Let A be a non-empty class of ordinals. Then* $\min A = \bigcap A$.

PROOF. Let $\alpha \in A$ and $\beta = \bigcap A$. Then β is an initial segment of α, so β is an ordinal and $\beta \leq \alpha$. If $\beta < \alpha$ for all $\alpha \in A$ then $\beta \in \bigcap A = \beta$, a contradiction. Therefore $\beta = \alpha$ for some $\alpha \in A$. ■5.2.20

LEMMA 5.2.21. *A set x is an ordinal if and only if it is a transitive set of ordinals (i.e., if and only if it is an initial segment of $(ON, \in)$).*

PROOF. Indeed, left to right is already shown. For right to left, let x be a transitive set of ordinals. Then $x \subseteq ON$ implies that $\in$ defines a total well-ordering on x. $\blacksquare_{5.2.21}$

COROLLARY 5.2.22. *Let A be a set of ordinals, and let $\alpha = \bigcup A$. Then $\alpha \in ON$, and $\alpha = \sup A$, i.e., $\alpha = \min\{\beta \in ON \colon (\forall \gamma \in A)(\beta \geq \gamma)\}$.*

PROOF. Since A is a set, so is α. As every ordinal is an initial segment of ON, so is any union of ordinals. Therefore α is an initial segment of ON and therefore an ordinal.

Clearly, $(\forall \gamma \in A)(\gamma \subseteq \alpha)$. Conversely, if β satisfies $(\forall \gamma \in A)(\gamma \subseteq \beta)$ then $\alpha = \bigcup A \subseteq \beta$, so α is minimal among all such β. $\blacksquare_{5.2.22}$

Finally, for every $\alpha \in ON$ there are three possibilities:

- $\alpha = \varnothing = 0$.
- α has a maximal member β. In that case α is the successor of β in ON, and $\alpha = \beta \cup \{\beta\} = S(\beta)$. In this case we say that α is a *successor ordinal*. We will write from now on $\beta + 1$ for $\beta \cup \{\beta\}$.
- Neither of the above holds. In this case we say that α is a *limit ordinal*.

Note that ω is the least limit ordinal.

DEFINITION 5.2.23. An *ordered class* $(C, <)$ is a class C equipped with a a class $<$ of pairs of members of C satisfying the usual axioms of an order relation. (The pair $(C, <)$ is a pair in "our" sense, as neither C no $<$ are assumed to be sets.)

An ordered class $(C, <)$ is *well-ordered* if:

(i) For every $a \in C$: the class $C_{<a} = \{b \in C \colon b < a\}$ is a set.
(ii) The set $C_{<a}$ is well-ordered by $<$.

EXAMPLE 5.2.24. The class ON is well ordered by $\in$. Indeed, $ON_{<\alpha} = \alpha$ for all $\alpha \in ON$ and this is a well-ordered set.

The restriction that $C_{<a}$ be set is so that the following hold:

THEOREM 5.2.25 (Definition by transfinite induction on a class). *Let $(C, <)$ be a well-ordered class, and F a class function whose domain contains all functions whose domain is of the form $C_{<a}$. Then there exists a (unique) class function such that* $\mathrm{dom}(G) = C$ *and for all $a \in C$:*

$$(*) \qquad G(a) = F(G{\restriction}_{C_{<a}}).$$

(Note that even though G is a class, as $C_{<a}$ is a set so is $G{\restriction}_{C_{<a}}$ by the replacement axiom.)

PROOF. First we observe that if $b \in C$ then $C_{\leq b} = C_{<b} \cup \{b\}$ is also necessarily a well-ordered set. By Theorem 5.2.13, for all $b \in C$ there is a unique function $g_b \colon C_{\leq b} \to V$ such that $(*)$ holds for all $a < b$.

Let $D = \{g_b \colon b \in C\} = \{f \colon (\exists b \in C)(f = g_b)\}$. Then D is a class (whose defining formula makes use of the formulae defining C, $<$ and G, and therefore of any parameters they may use). Let $F = \bigcup D = \{(x, y) \colon (\exists b \in C)(x \in \mathrm{dom}(g_b) \wedge g_b(x) = y)\}$. Then F is the required class function. ■5.2.25

This means we are allows to define functions by induction on the class ON. For example we define operations of ordinal arithmetic:

DEFINITION 5.2.26. Let α, β be ordinals. We define $\alpha + \beta$ by induction on β:

$$\begin{aligned} &\beta = 0 : && \alpha + 0 = \alpha \\ &\beta = \gamma + 1 : && \alpha + (\gamma + 1) = (\alpha + \gamma) + 1 \\ &\beta \text{ limit} && \alpha + \beta = \sup\{\alpha + \gamma \colon \gamma < \beta\}. \end{aligned}$$

DEFINITION 5.2.27. Let α, β be ordinals. We define $\alpha \cdot \beta$ by induction on β:

$$\begin{aligned} &\beta = 0 : && \alpha \cdot 0 = 0 \\ &\beta = \gamma + 1 : && \alpha \cdot (\gamma + 1) = \alpha \cdot \gamma + \alpha \\ &\beta \text{ limit} && \alpha \cdot \beta = \sup\{\alpha \cdot \gamma \colon \gamma < \beta\}. \end{aligned}$$

DEFINITION 5.2.28. Let α, β be ordinals. We define α^β by induction on β:

$$\begin{aligned} &\beta = 0 : && \alpha^0 = 1 (= \{0\}) \\ &\beta = \gamma + 1 : && \alpha^{(\gamma+1)} = \alpha^\gamma \cdot \alpha \\ &\beta \text{ limit} && \alpha^\beta = \sup\{\alpha^\gamma \colon \gamma < \beta\}. \end{aligned}$$

Note that addition and multiplication are associative (requires proof!) but non-commutative: $1 + \omega = \omega \neq \omega + 1$, and $\omega \cdot 2 = \omega + \omega > \omega$ while $2 \cdot \omega = \omega$.

5.3. Cardinals

5.3.1. Basics.

DEFINITION 5.3.1. Let A and B be sets.

(i) We say that A and B have the *same cardinality*, in symbols $|A| = |B|$, if there exists a bijection $f \colon A \to B$.
(ii) We say that the cardinality of A is *smaller or equal* to that of B (in symbols $|A| \leq |B|$) if there is an injection $f \colon A \to B$.
(iii) We say that the cardinality of A is *strictly smaller* than that of B (in symbols $|A| < |B|$) if $|A| \leq |B|$ and $|A| \neq |B|$.

EXAMPLE 5.3.2. $|\omega| = |\omega + \omega|$. Indeed, the mapping send $2n \mapsto n$ and $2n+1 \mapsto \omega + n$ is a bijection.

Clearly the relation $|A| = |B|$ is an equivalence relation, and $|A| \leq |B|$ is reflexive and transitive. To show that it is a (partial) ordering, we still need to show it is antisymmetric, i.e., that $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

LEMMA 5.3.3. *Assume that $B \subseteq A$ and $f\colon A \to B$ is injective. Then $|A| = |B|$.*

PROOF. Define by induction: $C_0 = B \setminus \mathrm{rng}(f)$, $C_{n+1} = f[C_n] = \{f(a)\colon a \in C_n\}$, $C = \bigcup_{n<\omega} C_n = \bigcup_{n<\omega} f^n[C_0]$. It follows that for all $x \in A$: $x \in C$ if and only if $x \in f[C]$ or $x \notin \mathrm{rng}(f)$. Therefore if $x \notin C$ then $f(x) \notin C$.

Define $g\colon A \to B$ by:

$$g(x) = \begin{cases} x & x \in C (\subseteq B) \\ f(x) & x \notin C. \end{cases}$$

g is injective, since $x \notin C \implies f(x) \notin C$. It is onto B, since for all $y \in B$:

- If $y \in C$ then $y = g(y)$.
- If $y \notin C$ then $y \in \mathrm{rng}(f)$, say $y = f(x)$, and $x \notin C$, so $y = g(x)$.

Therefore g witnesses that $|A| = |B|$. ■5.3.3

THEOREM 5.3.4 (Schroeder-Cantor-Bernstein). *For any two sets A and B, $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$.*

PROOF. Left to right is clear. For right to left, let $f\colon A \to B$ and $g\colon B \to A$ be the two injections. Let $h = g \circ f$, and $C = \mathrm{rng}(g)$. Then $C \subseteq A$ and $h\colon A \to C$ is injective, so $|A| = |C|$ by Lemma 5.3.3. On the other hand g witnesses that $|B| = |C|$. Therefore $|A| = |B|$. ■5.3.4

As we shall see later, the statement that the relation $|A| \leq |B|$ is a total ordering is equivalent to *AC* (Axiom of Choice).

We start with a trivial observation: for every set there is a strictly bigger one, namely its power set.

LEMMA 5.3.5. *For no set x is there a surjective mapping $f\colon x \to \mathcal{P}(x)$.*

PROOF. Assume there is such a mapping. Let $y = \{t \in x\colon t \notin f(t)\}$. Then for all $t \in x$, $t \in y \iff t \notin f(t)$, so $y \neq f(t)$. It follows that $y \notin \mathrm{rng}(f)$ so f is not surjective. ■5.3.5

PROPOSITION 5.3.6. *For all x: $|x| < |\mathcal{P}(x)|$.*

PROOF. First, we have an injection $f\colon x \to \mathcal{P}(x)$, sending $y \in x$ to $\{y\}$. On the other hand there can be no bijection by Lemma 5.3.5. ■5.3.6

5.3.2. The Axiom of Choice.

LEMMA 5.3.7 (Hartog). *Let A be any set. Then there exists an ordinal α such $|\alpha| \not\leq |A|$.*

PROOF. We would like to define α to be the set of all ordinals β such that $|\beta| \leq |A|$, but then it is not at all clear that this is indeed a set, so we use a somewhat more complicated definition.

Let X be the set of all pairs $(B, <)$ where $B \subseteq A$ and $<$ is a well-ordering of B. Note that $X \subseteq \mathcal{P}(A) \times \mathcal{P}(A \times A)$, so it exists by the subset axiom.

Let $\alpha = \{otp(B, <) \colon (B, <) \in X\}$. Then α is a set by the replacement axiom.

Let $\beta \in \alpha$. Then β is an ordinal, and $\beta = otp(B, <)$ for some $B \subseteq A$ and well-ordering $<$ on B. Therefore there is an order preserving bijection $f \colon (\beta, \in) \to (B, <)$. If $\gamma < \beta$, then it particular $\gamma \subseteq \beta$. In that case let $C = \operatorname{rng}(f\restriction_\gamma)$. Then $f\restriction_\gamma$ is an order preserving bijection between $(\gamma, \in)$ and $(C, < \restriction_C)$, so $\gamma = otp(\gamma, \in) = otp(C, < \restriction_C) \in \alpha$ as well. This shows that α is a downward-closed set of ordinals and therefore an ordinal.

Finally, assume $f : \alpha \to A$ were injective. Let $B = \operatorname{rng}(f)$, and let $<_B$ be the image of $\in$ under f. Then $(B, <_B)$ is well ordered and $\alpha = otp(B, <_B)$, so $\alpha \in \alpha$ which is impossible. This contradiction concludes the proof. ■5.3.7

PROPOSITION 5.3.8. *Let A be a set Then A admits a choice function if and only if A admits a well ordering.*

PROOF. Assume first that A admits a well-ordering $<$. The we can define a choice function for A: for every $B \in \mathcal{P}^-(A)$ we define $f(B) = \min B$.

Conversely, let $f \colon \mathcal{P}^-(A) \to A$ be a choice function for A. Extend it to a function $f^* \colon \mathcal{P}(A) \to A \cup \{*\}$, where $f(\varnothing) = \times \notin A$. Let α be a Hartog ordinal for A (i.e., $|\alpha| \not\leq |A|$) and define $g \colon \alpha \to A \cup \{*\}$ by:

$$g(\beta) = f^*(A \setminus \operatorname{rng}(g\restriction_\beta)).$$

Assume first that $* \notin \operatorname{rng}(g)$. Then for all $\gamma < \beta < \alpha$, $* \neq g(\beta) \implies g(\beta) \in A \setminus \operatorname{rng}(g\restriction_\beta) \implies g(\beta) \neq g(\gamma)$. Then g is injective, contradicting the assumption that $|\alpha| \not\leq |A|$.

Therefore we must have $* \in \operatorname{rng}(g)$ and there is a minimal $\beta < \alpha$ such that $g(\beta) = *$. Let $h = g\restriction_\beta$. Then $* \notin \operatorname{rng}(h)$, so h is injective by the same argument as above. Also, $\operatorname{rng}(h) = A$ (since otherwise $g(\beta) \neq *$). We conclude that $h \colon \beta \to A$ is a bijection, and the image of $\in$ under h induces a well-ordering of A. ■5.3.8

THEOREM 5.3.9. *The following are equivalent:*

(i) *The axiom of choice.*
(ii) *The well-ordering principle: every set can we well-ordered.*

PROOF. By Proposition 5.3.8. ■5.3.9

COROLLARY 5.3.10. *The following are equivalent:*

(i) *The axiom of choice.*
(ii) *For every two sets A and B, at least one of $|A| \geq |B|$ or $|A| \leq |B|$ holds.*

PROOF. Assume the axiom of choice. Then every A and B can be well-ordered as $(A, <_A)$ and $(B, <_B)$. Let $\alpha = otp(A, <_A)$ and $\beta = otp(B, <_B)$. Then $|A| = |\alpha|$ and $|B| = |\beta|$. If $\alpha \leq \beta$ then $|\alpha| \leq |\beta|$, otherwise $\alpha \geq \beta$ in which case $|\alpha| \geq |\beta|$.

Conversely, assume every two cardinalities are comparable. Let A be any set, and α an ordinal such that $|\alpha| \not\leq |A|$. Then $|\alpha| \geq |A|$, so there is a bijection between A and a subset $B \subseteq \alpha$. Since $(B, \in)$ is well-ordered, we can pull this back to a well-ordering on A. Thus every set can be well-ordered. ■5.3.10

DEFINITION 5.3.11. A *cardinal number* (or simple a *cardinal*) is an ordinal α such that for all $\beta < \alpha$: $|\alpha| \neq |\beta|$. Cardinals are denoted by lowercase Greek letters κ, λ, μ,...

LEMMA 5.3.12. *Let λ and κ be two cardinals. Then $\lambda = \kappa$ f and only if $|\lambda| = |\kappa|$, and $\lambda < \kappa \iff |\lambda| < |\kappa|$.*

PROOF. Assume that $\lambda < \kappa$. Then $\lambda \subseteq \kappa \implies |\lambda| \leq |\kappa|$, and as κ is a cardinal, $\lambda < \kappa \implies |\lambda| \neq |\kappa|$, so $|\lambda| < |\kappa|$.

Conversely, assume that $|\lambda| < |\kappa|$. Then $\kappa \not\subseteq \lambda$, whereby $\kappa \not\leq \lambda$ so $\lambda < \kappa$.

If $\lambda \neq \kappa$ then either $\lambda < \kappa$ or $\lambda > \kappa$, and in either case $|\lambda| \neq |\kappa|$. ■5.3.12

Thus, for every set A there is at most one cardinal λ such that $|A| = |\lambda|$. If such exists we define $\lambda = |A|$. By the lemma, there will be no confusion about the meaning of $|A| < |B|$, $|A| = |B|$, etc.

LEMMA 5.3.13. *For every ordinal $\alpha \in ON$ there is a cardinal λ such that $|\alpha| = \lambda$.*

PROOF. The class (set, in fact, but it doesn't matter) $\{\beta \in ON : |\beta| = |\alpha|\}$ is non-empty and has am minimal member λ. Then $|\alpha| = |\lambda|$ and λ is a cardinal. It is unique by the previous lemma. ■5.3.13

THEOREM 5.3.14. *The following are equivalent:*

(i) *The axiom of choice.*
(ii) *For every set A there is a (unique) cardinal λ such that $|A| = |\lambda|$*

PROOF. By the axiom of choice, every set A can be well ordered as $(A, <)$, and let $\alpha = otp(A, \alpha)$. Then $|A| = |\alpha|$, and by the Lemma $|\alpha|$ is a cardinal.

Conversely, assume that for every set A, $|A|$ is a cardinal. Since every two cardinals are comparable (since all ordinals are) we conclude using Corollary 5.3.10. ■5.3.14

We conclude with:

THEOREM 5.3.15. *The following are equivalent:*

(i) *The axiom of choice.*
(ii) *Zorn's Lemma:*

> *Let $(X, <)$ be a partially ordered set, such that for every chain $C \subseteq X$ (i.e., a subset of X which is totally ordered by $<$) there is $x \in X$ such*

that $x \geq C$ (i.e., $(\forall y \in C)(x \geq y)$). Then X contains a maximal element (i.e., $x \in X$ such that $(\forall y \in X)(y \not> x)$).

PROOF. Assume the axiom of choice. Let $(X, <)$ satisfy the assumptions of Zorn's Lemma. Let $f\colon \mathcal{P}^-(X) \to X$ be a choice function, and extend it to $f^+\colon \mathcal{P}(X) \to X$ by $f^+(\varnothing) = f(X)$. Define by induction a function $g\colon ON \to X \cup \{*\}$:

$$g(\alpha) = f^+(\{x \in X\colon x > \operatorname{rng}(g\restriction_\alpha)\}).$$

By Hartog's theorem, g cannot be injective, and therefore cannot be strictly increasing. Let α be minimal such that $g(\alpha) \not> \operatorname{rng}(g\restriction_\alpha)$. Let $C = \operatorname{rng}(g\restriction_\alpha)$. Then by construction of g: $\{x \in X\colon x > C\} = \varnothing$. As α is minimal, $g\restriction_\alpha$ is strictly increasing and therefore C is a chain. Therefore there exists $x_0 \in X$ such that $x_0 \geq C$. Since for no $x \in X$ do we have $x > C$, neither can we have $x > x_0$, so x_0 is maximal in X.

For the converse see either Exercise 5.6 or Exercise 5.7. ■5.3.15

5.3.3. Cardinal arithmetic. We can define addition and multiplication of cardinals.

DEFINITION 5.3.16. Let A and B be sets.

(i) We define $|A| + |B|$ as $|A \times \{0\} \cup B \times \{1\}|$. Note that this is equal to $|C \cup D|$ for any C, D such that $C \cap D = \varnothing$, $|C| = |A|$, $|D| = |B|$.
(ii) We define $|A| \cdot |B|$ as $|A \times B|$.
(iii) We define $|A|^{|B|}$ as $|A^B|$ (where A^B is the set of all functions $f\colon B \to A$).

Note that $0^{|A|} = 0$ for $|A| \neq 0$, $0^0 = 1$.

Caution: even though cardinals are in particular ordinals, cardinal arithmetic does not extend ordinal arithmetic. For example: $\omega + 1, \omega \cdot 2 \neq \omega$ as ordinals, $\omega + 1 = \omega \cdot 2 = \omega$ as cardinals. Also, $2^\omega = \omega$ as ordinals, $2^\omega = |\mathcal{P}(\omega)| > \omega$ as cardinals.

It is not difficult to see that cardinal addition and multiplication are commutative and distributive. We can extend them to infinite families:

DEFINITION 5.3.17. Let $\{A_i\colon i \in I\}$ be an indexed family of set (formally given by a function f such that $\operatorname{dom}(f) = I$, and $f(i) = A_i$ for $i \in I$).

(i) We define

$$\sum_{i \in I} |A_i| = \left|\bigcup_{i<I} A_i \times \{i\}\right| = \left|\left\{(x, i)\colon i \in I, x \in A_i\right\}\right|.$$

(ii) We define

$$\prod_{i \in I} |A_i| = \left|\prod_{i \in I} A_i\right| = \left|\left\{g\colon \operatorname{dom}(g) = I \text{ and } (\forall i \in I)(g(i) \in A_i)\right\}\right|.$$

LEMMA 5.3.18. *The following identities are fairly easy to verify:*

(i) $\sum_{i \in B} |A| = |A||B|$.

(ii) $\prod_{i\in B}|A| = |A|^{|B|}$.
(iii) $\left(|A|^{|B|}\right)^{|C|} = |A|^{|B||C|}$.
(iv) $|\mathcal{P}(A)| = 2^{|A|}$.

LEMMA 5.3.19. *Addition, multiplication and exponentiation of cardinals are all monotone increasing with a single exception that* $0^0 = 1 > 0 = 0^{|A|}$ *where* $A \neq 0$.

DEFINITION 5.3.20. A set A is *finite* if $|A| < \omega$ (i.e., if it is in bijection with some $n \in \omega$). Otherwise it is *infinite*.

PROPOSITION 5.3.21. *Let* κ *be an infinite cardinal. Then* $\kappa^2 = \kappa$.

PROOF. We prove this by induction on the class of infinite cardinals (which is well ordered, as a subclass of that of cardinals).

Define an ordering on $\kappa \times \kappa$ as follows: $(\alpha, \beta) < (\gamma, \delta)$ if and only if

- $\max\{\alpha, \beta\} < \max\{\gamma, \delta\}$; or
- $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$ and $\alpha < \gamma$; or
- $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$ and $\alpha = \gamma$ and $\beta < \delta$.

This is indeed a total ordering: it is the lexicographic ordering on $\{(\max\{\alpha, \beta\}, \alpha, \beta) \colon (\alpha, \beta) \in \kappa \times \kappa\}$.

We claim that $(\kappa \times \kappa, <)$ is well-ordered. Indeed, let $\varnothing \neq A \subseteq \kappa \times \kappa$. First, let $\gamma_0 \in \{\max\{\alpha, \beta\} \colon (\alpha, \beta) \in A\}$ be minimal. Then, let $\alpha_0 \in \{\alpha \colon \exists \beta\, (\alpha, \beta) \in A \wedge \max\{\alpha, \beta\} = \gamma_0\}$ be minimal. Finally, let $\beta_0 \in \{\beta \colon (\alpha_0, \beta) \in A \wedge \max\{\alpha_0, \beta\} = \gamma_0\}$ be minimal. Then (α_0, β_0) is minimal in A.

Let $\gamma = otp(\kappa \times \kappa, <) \in ON$, and let $f \colon \gamma \to \kappa \times \kappa$ be the order-preserving bijection witnessing this. Then $\kappa^2 \geq \kappa \cdot 1 = \kappa$ implies that $|\gamma| \geq \kappa$, whereby $\gamma \geq \kappa$ (since κ is a cardinal). We claim that $\gamma = \kappa$. Indeed, otherwise we d have $\gamma > \kappa$, i.e., $\kappa \in \gamma$. Let $(\alpha, \beta) = f(\kappa) \in \kappa \times \kappa$, and let $\alpha' = \max\{\alpha, \beta\} + 1$. Then for all $i \in \kappa$: $f(i) < (\alpha, \beta) \Longrightarrow f(i) \in (\alpha' + 1) \times (\alpha' + 1)$, whereby $\mathrm{rng}(f\restriction_\kappa) \subseteq (\alpha' + 1) \times (\alpha' + 1)$. But $\alpha' < \kappa$, so:

- If $\alpha' < \omega$ then $|\alpha' + 1|^2 < \omega \leq \kappa$.
- If $\alpha' \geq \omega$, then $|\alpha' + 1| = |\alpha'| < \kappa$ is infinite, and by the induction hypothesis: $|\alpha' + 1|^2 = |\alpha'| < \kappa$.

On the other hand, as $f\restriction_\kappa \colon \kappa \to (\alpha' + 1) \times (\alpha' + 1)$ is injective: $|\alpha' + 1|^2 \geq \kappa$. A contradiction.

Therefore $\kappa = \gamma$, and f witnesses that $\kappa = |\kappa \times \kappa| = \kappa^2$ ■$_{5.3.21}$

COROLLARY 5.3.22. *(AC) For every infinite set* A: $|A|^2 = |A|$.

PROOF. By the axiom of choice $|A|$ is a cardinal. ■$_{5.3.22}$

REMARK 5.3.23. The converse can also be shown to be true, i.e., if for every infinite set $|A|^2 = |A|$, then the axiom of choice holds.

COROLLARY 5.3.24. *If κ is an infinite cardinal and λ is any cardinal then $\kappa + \lambda = \max\{\kappa, \lambda\}$. If in addition $\lambda > 0$ then $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$ as well.*

PROOF. Since cardinal addition and multiplication are commutative, we may assume that $\kappa \geq \lambda$. If $\lambda \geq 1$ then $\kappa = \kappa \cdot 1 \leq \kappa \cdot \lambda \leq \kappa^2 = \kappa$, so there is equality all the way. It follows that $2\kappa = \kappa$, so now if $0 \leq \lambda \leq \kappa$: $\kappa = \kappa + 0 \leq \kappa + \lambda \leq 2\kappa = \kappa$. ■5.3.24

COROLLARY 5.3.25. *The following are equivalent:*

(i) *The Axiom of Choice.*
(ii) *For every A and infinite B: $|A| + |B| = \max\{|A|, |B|\}$.*
(iii) *For every $A \neq \varnothing$ and infinite B: $|A| \cdot |B| = \max\{|A|, |B|\}$.*

PROOF. If the Axiom of Choice is true then $|A|$ and $|B|$ are cardinals and we can apply Corollary 5.3.24. Conversely, either of the other two items implies that every infinite cardinality is comparable with every cardinality. As every two finite cardinalities (i.e., natural numbers) are comparable, it follows that every two cardinalities are comparable, which implies the Axiom of Choice. ■5.3.25

COROLLARY 5.3.26. *For every infinite κ: $2^\kappa = \kappa^\kappa = (2^\kappa)^\kappa$.*

PROOF. $2^\kappa \leq \kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa$. ■5.3.26

We see that many times cardinal arithmetic operations are only weakly increasing (i.e., they are non-decreasing). The following result is one of the very few results in cardinal arithmetic which yield a strict inequality:

PROPOSITION 5.3.27. *Let I be a set, $\lambda_i < \kappa_i$ cardinals for each $i \in I$. Then $\sum_{i \in I} \lambda_i < \prod_{i \in I} \kappa_i$.*

PROOF. Let $A = \bigcup_{i \in I} \lambda_i \times \{i\}$ and $B = \{(\alpha_i \colon i \in I) \colon (\forall i \in I)(\alpha_i \in \kappa_i)\}$ (so $|A| = \sum_{i \in \lambda} \lambda_i$, $|B| = \prod_{i \in I} \kappa_i$).

Let $f \colon A \to B$ be defined by $f(\alpha, i) = (\beta_j \colon j \in I)$, where $\beta_j = \begin{cases} \alpha + 1 & j = i \\ 0 & j \neq i \end{cases}$. Then f is injective, whereby $|A| \leq |B|$.

Now let $g \colon A \to B$ be any function. For $i \in I$, let $C_i = \{(g(\alpha, i))_i \colon i < \lambda_i\} \subseteq \kappa_i$. Then $|C_i| \leq \lambda_i < \kappa_i$, and thus in particular $C_i \subsetneq \kappa_i$, and we may define $\gamma_i = \min(\kappa_i \setminus C_i)$. Then $\bar{\gamma} = (\gamma_i \colon i \in I) \in B$, and yet for all $(\alpha, i) \in A$: $g(\alpha, i)_i \neq \gamma_i \implies g(\alpha, i) \neq \bar{\gamma}$. In other words, $\bar{\gamma} \notin \operatorname{rng}(g)$.

We thus shows that there is no surjective function from A to B. In particular, $|A| \neq |B|$, and as $|A| \leq |B|$ we conclude that $|A| < |B|$. ■5.3.27

REMARK 5.3.28. Proposition 5.3.27 is in some sense the "only" strict inequality result in cardinal arithmetic. For example, the only other strict inequality we've shown $2^\kappa > \kappa$ is a special case, as:

$$\kappa = \sum_{i \in \kappa} 1 < \prod_{i \in \kappa} 2 = 2^\kappa.$$

DEFINITION 5.3.29. If κ is a cardinal, then the least cardinal greater than κ (i.e., its successor) is denoted κ^+. Such a cardinal always exists by Hartog's theorem.

LEMMA 5.3.30. *Let $\alpha \in ON$ and let A be a family of cardinals. Then the ordinal $\alpha = \sup A = \bigcup A$ is a cardinal, and it is the minimal cardinal greater than all members of A. In other words, $\alpha = \sup A$ also in the sense of cardinals.*

PROOF. Let $\alpha = \sup A$, and let $\beta < \alpha$. Then there is some $\kappa \in A$ such that $\beta < \kappa$. As κ is a cardinal and $\kappa \subseteq \alpha$: $|\beta| < |\kappa| \leq |\alpha|$. Therefore α is a cardinal. Clearly α is the least cardinal greater than all members of A. ■5.3.30

DEFINITION 5.3.31. We define by in induction on $\alpha \in ON$ the following sequence:

- $\aleph_0 = \omega$ (this is the first infinite cardinal).
- $\aleph_{\alpha+1} = \aleph_\alpha^+$.
- If δ is limit: $\aleph_\delta = \sup\{\aleph_\alpha : \alpha < \delta\}$.

LEMMA 5.3.32. (i) *For every $\alpha \in ON$: $\aleph_\alpha$ the least infinite cardinal strictly greater than $\aleph_\beta$ for all $\beta < \alpha$.*
(ii) *For all $\alpha \in ON$: $\aleph_\alpha \geq \alpha$.*
(iii) *If κ is any infinite cardinal then there exists a unique α such that $\kappa = \aleph_\alpha$.*

PROOF. (i) Immediate from the definition.
(ii) By easy induction on α.
(iii) Let κ be an infinite cardinal. Then $\kappa \leq \aleph_\kappa$, so $\{\alpha : \kappa \leq \aleph_\alpha\} \neq \varnothing$. Let α be least such that $\kappa \leq \aleph_\alpha$. Then $\kappa > \aleph_\beta$ for all $\beta < \alpha$ and κ is infinite, so $\kappa \geq \aleph_\alpha$ by the first item. Therefore $\kappa = \aleph_\alpha$.

■5.3.32

Similarly:

DEFINITION 5.3.33. (AC) We define by in induction on $\alpha \in ON$ the following sequence of cardinals:

- $\beth_0 = \aleph_0$.
- $\beth_{\alpha+1} = 2^{\beth_\alpha}$.
- If δ is limit: $\beth_\delta = \sup\{\beth_\alpha : \alpha < \delta\}$.

LEMMA 5.3.34. *For all $\alpha \in ON$: $\aleph_\alpha \leq \beth_\alpha$.*

PROOF. By induction. In successor stages use the fact that $2^\kappa > \kappa \implies 2^\kappa \geq \kappa^+$. ■5.3.34

FACT 5.3.35. $|\mathbb{R}| = 2^{\aleph_0}$.

PROOF. The cardinal $2^{\aleph_0}$ is the size of the set $2^{\aleph_0}$, i.e., the set of all sequences $(a_i \in \{0,1\} : i \in \aleph_0)$.

Define $f\colon 2^{\aleph_0} \to \mathbb{R}$ by:

$$f(a_i\colon i < \aleph_0) = \sum_{i<\aleph_0} 2 \cdot 3^{-i-1} \cdot a_i.$$

Then f is injective (it is in fact a bijection between $2^{\aleph_0}$ and the standard "middle third" Cantor set). Therefore $|\mathbb{R}| \geq 2^{\aleph_0}$.

Conversely, we observe that $|\mathbb{R}| = |(0,1)|$ through the bijection $x \mapsto \frac{1}{e^x+1}$. Define $g\colon (0,1) \to 2^{\aleph_0}$, assigning to each real number $x \in (0,1)$ its binary presentation $0.a_0a_1a_2\ldots$, such that if there are two such presentations we choose the one which is all zeros from some point onwards (and never the one which is all ones). Then g is injective, whereby $|\mathbb{R}| = |(0,1)| \leq 2^{\aleph_0}$. ■5.3.35

We call $2^{\aleph_0}$ ($= \beth_1$, and sometimes denoted by $\aleph$) the *continuum*.

By Cantor's theorem: $2^{\aleph_0} > \aleph_0$, whereby $2^{\aleph_0} \geq \aleph_1$. The statement "$2^{\aleph_0} = \aleph_1$" is called the *Continuum Hypothesis (CH)*. This can be generalised as follows: we know that for every κ: $2^\kappa > \kappa \Longrightarrow 2^\kappa \geq \kappa^+$. The statement "$2^\kappa = \kappa^+$ for all infinite cardinals κ" is called the *Generalised Continuum Hypothesis (GCH)*. It is equivalent to saying that $\forall\alpha\, \beth_\alpha = \aleph_\alpha$.

Kurt Gödel showed that CH, and in fact GCH, are relatively consistent with ZFC: if there is a model of ZFC, we can construct within it a submodel which is a model of ZFC+GCH. Much later, Paul Cohen showed that if ZFC is consistent then so is ZFC+¬CH (and thus ZFC+¬GCH). He did it by a method called forcing, by which one adds new sets to the universe of sets – in particular, one can add many real numbers, making the continuum arbitrarily big.

Exercises

Exercise 5.1. Let C be the class $\{x\colon x \notin x\}$. Show that C is a proper class. What is the relation to Russel's Paradox?

Use the foundation axiom to show that C is the class of all sets (i.e., $C = \{x\colon x = x\}$).

Exercise 5.2. Show that the Subset axiom scheme is a consequence of the Replacement axiom scheme.

(It is therefore redundant. Historically it is there because it was part of Zermelo's set theory before Fraenkel suggested to add replacement. Also, one can re-state replacement in a manner which does not imply the subset axiom, but which, together with the subset axiom, is equivalent to the replacement as stated here.)

Exercise 5.3. Show that ordinal addition is associative.

Exercise 5.4. Define by transfinite induction on $\alpha \in ON$:

- $V_0 = \varnothing$.
- $V_{\alpha+1} = \mathcal{P}(V_\alpha)$.
- $V_\delta = \bigcup_{\alpha<\delta} V_\alpha$ for δ limit.

(One can define alternatively $V_\alpha = \bigcup_{\beta<\alpha} \mathcal{P}(V_\beta)$ for all $\alpha \in ON$ – the two definitions coincide).

Define a class V_∞: $V_\infty = \bigcup_{\alpha\in ON} V_\alpha = \{x\colon \exists\alpha\, \alpha \in ON \wedge x \in V_\alpha\}$. Note that we made no use of the Foundation axiom throughout. Let ZF' be ZF minus the Foundation axioms. Thus we can construct the class V_∞ in a model of ZF'.

Show that if $(V, \in) \vDash ZF'$ then $(V_\infty, \in) \vDash ZF$.

This is a classical case of "relative consistency": we cannot show that ZF is consistent, but we can show that if ZF' is consistent then so is ZF. Thus in some sense the foundation axiom is a "benign" axiom.

Exercise 5.5. Conversely, show that if $V \vDash ZF$ (with the foundation axiom) then $V = V_\infty$.

Hint: given a set x, we define its *transitive closure* $tcl(x)$ as the minimal transitive set containing x. We can construct it as follows: $x_0 = x$, $x_{n+1} = x_n \cup \bigcup x_n$ for all $n < \omega$, and $tcl(x) = \bigcup\{x_n\colon n < \omega\}$. What can you say about $tcl(x) \setminus V_\infty$?

Exercise 5.6. Prove the Axiom of Choice directly from Zorn's Lemma.

Strategy: Let A be a set, and define X as a set of all partial choice functions for A, i.e., of all functions f satisfying $\mathrm{dom}(f) \subseteq \mathcal{P}^-(A)$ and $f(x) \in x$ for all $x \in \mathrm{dom}(f)$.

Show that $(X, \subseteq)$ contains a maximal element which is a choice function for A.

Exercise 5.7. Prove the well-ordering principle directly from Zorn's Lemma.

Let A be any set, and let X be the set of pairs $(B, <)$ such that $B \subseteq A$ and $<$ is a well-ordering of B. Find a partial ordering of X such that:

- $(X, \leq)$ admits a maximal element.
- Any maximal element of $(X, \leq)$ must be of the form $(A, <)$, i.e., a well-ordering of A.