LOGIC NOTES

YIANNIS N. MOSCHOVAKIS

July 16, 2012

CONTENTS

CHAPTER 1

FIRST ORDER LOGIC

Our main aim in this fist chapter is to introduce the basic notions of logic and to prove *Gödel's Completeness Theorem* 1I.1, which is the first, fundamental result of the subject. Along the way to motivating, formulating precisely and proving this theorem, we will also establish some of the basic facts of *Model Theory*, *Proof Theory* and *Recursion Theory*, three of the main parts of logic. (The fourth is *Set Theory.*)

1A. Examples of structures

The language of First Order Logic is interpreted in *mathematical structures*, like the following.

Definition 1A.1. A **graph** is a pair

$$\mathbf{G} = (G, E)$$

where $G \neq \emptyset$ is a non-empty set (the *nodes*) and $E \subseteq G \times G$ is a binary relation on G, (the *edges*); $\mathbf{G}$ is **symmetric** or **unordered** if

$$E(x, y) \Longrightarrow E(y, x).$$

A *path* in a symmetric graph $\mathbf{G} = (G, E)$ is a sequence of points (vertices)

$$(x_0, x_1, \dots , x_n)$$

such that there is an edge joining each x_i with x_{i+1}, i.e.,

$$E(x_0, x_1), E(x_1, x_2), \dots , E_(x_{n-1}, x_n);$$

a path *joins* its first vertex x_0 with its last x_n. The *distance* between two vertices x, y which can be joined in $\mathbf{G}$ is the length (number of edges, n above) of the shortest path joining them,

$$d(x, y) = \min\{n \mid \text{there exists a path } x_0, \dots , x_n \text{ with } x_0 = x, x_n = y\},$$

and (by convention) it is 0 from a vertex to itself, $d(x, x) = 0$ and ∞ if $x \neq y$ and there is no path from x to y. The *diameter* of a symmetric graph is the largest distance between two vertices, if there is a maximum distance, otherwise it is ∞:

$$\mathrm{diam}(\mathbf{G}) = \sup\{d(x,y) \mid x, y \in G\}.$$

A symmetric graph is **connected** if any two distinct points in it are joined by a path, otherwise it is **disconnected**.

Definition 1A.2. A **partial ordering** is a pair

$$\mathbf{P} = (P, \leq),$$

where P is a non-empty set and $\leq$ is a binary relation on P satisfying the following conditions:

1. For all $x \in P$, $x \leq x$ (reflexivity).
2. For all $x, y, z \in P$, if $x \leq y$ and $y \leq z$, then $x \leq z$ (transitivity).
3. For all $x, y \in P$, if $x \leq y$ and $y \leq x$, then $x = y$ (antisymmetry).

A **linear ordering** is a partial ordering in which every two elements are comparable, i.e., such that

4. For all $x, y \in P$, either $x \leq y$ or $y \leq x$.

A **wellordering** is a linear ordering $(U, \leq)$ in which every non-empty subset has a least element: i.e., for every $X \subseteq U$, if $X \neq \emptyset$, then there exists some $x_0 \in X$ such that for all $x \in X, x_0 \leq x$.

Definition 1A.3. The structure of **arithmetic** or the **natural numbers** is the tuple

$$\mathbf{N} = (\mathbb{N}, 0, S, +, \cdot)$$

where $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of (non-negative) integers and S, $+$, $\cdot$ are the operations of successor, addition and multiplication on $\mathbb{N}$. The structure $\mathbf{N}$ has the following characteristic properties:

(1) The successor function S is an injection, i.e.,

$$S(x) = S(y) \Longrightarrow x = y,$$

and 0 is not a successor, i.e., for all x, $S(x) \neq 0$.

(2) For all x, y, $x + 0 = x$ and $x + S(y) = S(x + y)$.

(3) For all x, y, $x \cdot 0 = 0$ and $x \cdot S(y) = x \cdot y + x$.

(4) *The Induction Principle*: for every set of numbers $X \subseteq \mathbb{N}$, if $0 \in X$ and for every x, $x \in X \Longrightarrow S(x) \in X$, then $X = \mathbb{N}$.

These properties (or sometimes just (1) and (4)) are called the *Peano Axioms* for the natural numbers.

Definition 1A.4. A **field** is a structure of the form

$$\mathbf{K} = (K, 0, 1, +, \cdot)$$

where $0, 1 \in K$, $+$ and $\cdot$ are binary operations on K and the following *field axioms* are true.

(1) $(K, 0, +)$ is a *commutative group*, i.e., the following hold:

1. For all x, $x + 0 = x$.
2. For all x, y, z, $x + (y + z) = (x + y) + z$.
3. For all x, y, $x + y = y + x$.
4. For each x there exists some y such that $x + y = 0$.

(2) $1 \neq 0$ and for all x, $x \cdot 0 = 0$, $x \cdot 1 = x$.
(3) The structure $(K \setminus \{0\}, 1, \cdot)$ is a commutative group, and in particular

$$x, y \neq 0 \Longrightarrow x \cdot y \neq 0.$$

Together with (2), this means that for all x, y in K,

$$x \cdot y = 0 \iff x = 0 \text{ or } y = 0.$$

(4) For all x, y, z, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Basic examples of fields are the *rational numbers* $\mathbf{Q}$, the *real numbers* $\mathbf{R}$ and the *complex numbers* $\mathbf{C}$, with universes $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively and the usual operations on these number sets.

Definition 1A.5. The **universe of sets** is the structure

$$\mathbf{V} = (V, \in)$$

where V is the collection of all sets and $\in$ is the binary relation of membership. We list here the most common set of axioms usually assumed about sets, not in the simplest way, but directly in terms of the basic membership relation, without introducing any auxiliary notions.

(1) Extensionality: two sets are equal exactly when they have the same members, in symbols:

$$x = y \iff (\forall u)[u \in x \iff u \in y].$$

(2) Emptyset and Pairing: there exists a set $\emptyset$ with no members, and for any two sets x, y, there is a set z whose members are exactly x and y, i.e., for all u,

$$u \in z \iff u = x \text{ or } u = y.$$

(3) Union: for each set x there exists a set z whose members are the members of members of x, i.e., for all u

$$u \in z \iff (\exists y \in x)[u \in y].$$

(4) Power: for each set x there exists a set z whose members are all the subsets of x, i.e., for all u,

$$u \in z \iff (\forall v \in u)[v \in x].$$

(5) Subsets: for each set x and each "definite condition" $P(u)$ on sets, there exists a set z whose members are the members of x which satisfy $P(u)$, i.e., for all u,

$$u \in z \iff u \in x \text{ and } P(u).$$

(6) Infinity: there exists a set z such that $\emptyset \in z$ and z is closed under the "singleton operation", i.e., for every x,

$$x \in z \Longrightarrow \{x\} \in z.$$

(7) Choice: for every set x whose members are all non-empty and pairwise disjoint, there exists a set z which intersects each member of x in exactly one point, i.e., if $y \in x$, then there exists exactly one u such that $u \in y$ and also $u \in z$.
(8) Replacement: for every set x and every "definite operation" F which assigns a set $F(v)$ to every set v, the image $F[x]$ of x by F is a set, i.e., there exists a set z such that for all u,

$$u \in z \iff (\exists v \in x)[u = F(v)].$$

(9) Foundation: every non-empty set x has a member z from which it is disjoint, i.e., there is no $u \in X$ such that also $u \in z$.

1B. The syntax of First Order Logic ($\mathbb{FOL}$)

The name $\mathbb{FOL}$ abbreviates *First Order Logic.* It is actually a family of languages $\mathbb{FOL}(\tau)$, one for each *vocabulary* τ, where τ provides names for the distinguished elements, relations and functions of the structures we want to talk about.

$\mathbb{FOL}$ is also known as *Lower Predicate Calculus (with Identity)*, or *Elementary Logic with Identity* or just *Elementary Logic.*

Definition 1B.1. A **vocabulary** or **signature** is a quadruple

$$\tau = (\mathrm{Const}, \mathrm{Rel}, \mathrm{Funct}, \mathrm{arity}),$$

where the sets of *constant symbols* Const, *relation symbols* Rel, and *function symbols* Funct have no common members and

$$\mathrm{arity} : \mathrm{Rel} \cup \mathrm{Funct} \to \{1, 2, \dots\}.$$

A relation or function symbol P is n-ary if $\mathrm{arity}(P) = n$. We will often assume that these sets of names are finite (as they are in the examples above), but it is convenient and useful to allow them to be arbitrary sets in the general case; and we should also keep in mind that any one—or all—of these sets may be empty. When they are all finite, we usually exhibit signatures by enumerating their symbols: for example,

$$\tau_g = (R) \qquad \text{(with } R \text{ binary)}$$

is a signature for graphs;

$$\tau_a = (0, S, +, .)$$

is a signature for arithmetic (with 0 a constant, S a unary function symbol and $+, \cdot$ binary function symbols);

$$\tau_f = (0, 1, +, \cdot)$$

(with the appropriate arities) is a signature for fields; and

$$\tau_\in = (\in)$$

(with $\in$ binary) is a signature for universe of sets. (We say *a* rather than *the* signature because the "symbols" $R, S, +, \in$ etc. are arbitrary.)

Definition 1B.2. The **alphabet** of the *first order language with identity* $\mathbb{FOL}(\tau)$ comprises the symbols in the vocabulary τ and the following, additional symbols which are common to all $\mathbb{FOL}(\tau)$.

1. The *logical symbols* $\neg\ \ \&\ \ \vee\ \ \rightarrow\ \ \forall\ \exists\ \ =$
2. The *punctuation symbols* ( ) ,
3. The (individual) *variables*: v_0, v_1, v_2, ...

Here $\neg$ (not), & (and), $\vee$ (or) and $\rightarrow$ (implies) are the *propositional symbols*, and $\forall$ (for all) and $\exists$ (there exists) are the *quantifiers*.

Words are finite strings of symbols and $lh(\alpha)$ is the length of the word α. We use $\equiv$ to denote identity of strings,

$$\alpha \equiv \beta \iff_{\mathrm{df}} \alpha \text{ and } \beta \text{ are the same string.}$$

We also set

$$\alpha \sqsubseteq \beta \iff_{\mathrm{df}} \alpha \text{ is an initial segment of } \beta,$$

so that e.g., $\forall \mathrm{v}_0 \sqsubseteq \forall \mathrm{v}_0 R(\mathrm{v}_0)$. The *concatenation* of two strings $\alpha\beta$ is the string produced by putting them together, with α first, so that $\alpha \sqsubseteq \alpha\beta$.

Definition 1B.3 (Terms and formulas)**.** **Terms** are defined by the recursion: (a) Each variable is a term. (b) Each constant symbol is a term. (c) If $t_1, \dots, t_n$ are terms and f is an n-ary function symbol, then $f(t_1, \dots, t_n)$ is a term. In abbreviated notation:

$$t :\equiv v \mid c \mid f(t_1, \dots, t_n),$$

where $\mid$ is read as "or".

Formulas are defined by the recursion: (a) If s, t are terms, then $s = t$ is a formula. (b) If $t_1, \dots, t_n$ are terms and R is an n-ary relation symbol, then $R(t_1, \dots, t_n)$ is a formula. (c) If ϕ, ψ are formulas and v is a variable, then the following are formulas:

$$\neg(\phi) \quad (\phi) \to (\psi) \quad (\phi) \mathbin{\&} (\psi) \quad (\phi) \vee (\psi) \quad \forall v\phi \quad \exists v\phi$$

In abbreviated form,

$$\begin{aligned}\chi :\equiv s = t \mid R(t_1, \dots, t_n) \quad &(\text{the } \textit{prime formulas})\\ &\mid \neg(\phi) \mid (\phi) \to (\psi) \mid (\phi) \mathbin{\&} (\psi) \mid (\phi) \vee (\psi) \mid \forall v\phi \mid \exists v\phi\end{aligned}$$

For the rigorous interpretations of these *recursive definitions* of sets see Problem x6.3.

A formula is **quantifier free** if neither of the quantifier symbols $\exists$, $\forall$ occurs in it. A formula is **in prenex normal form** (*prenex*) if it looks like

$$\phi \equiv Q_1 x_1 \cdots Q_n x_n \psi$$

where each $Q_i \equiv \forall$ or $Q_i \equiv \exists$ and ψ is quantifier free.

Terms and formulas are collectively called (well formed) **expressions**.

Proposition 1B.4 (Parsing for terms)**.** *Each term t satisfies exactly one of the following three conditions.*

1. *$t \equiv v$ for a uniquely determined variable v.*
2. *$t \equiv c$ for a uniquely determined constant c.*
3. *$t \equiv f(t_1, \dots, t_n)$ for a uniquely determined function symbol f and uniquely determined terms $t_1, \dots, t_n$.*

Proposition 1B.5 (Parsing for formulas)**.** *Each formula χ satisfies exactly one of the following conditions.*

1. *$\chi \equiv s = t$ for uniquely determined terms s, t.*
2. *$\chi \equiv R(t_1, \dots, t_n)$ for a uniquely determined relation symbol R and uniquely determined terms $t_1, \dots, t_n$.*
3. *$\chi \equiv \neg(\phi)$ for a uniquely determined formula ϕ.*
4. *$\chi \equiv (\phi) \mathbin{\&} (\psi)$ for uniquely determined formulas ϕ, ψ.*
5. *$\chi \equiv (\phi) \vee (\psi)$ for uniquely determined formulas ϕ, ψ.*
6. *$\chi \equiv (\phi) \to (\psi)$ for uniquely determined formulas ϕ, ψ.*
7. *$\chi \equiv \exists v\phi$ for a uniquely determined variable v and a uniquely determined formula ϕ.*
8. *$\chi \equiv \forall v\phi$ for a uniquely determined variable v and a uniquely determined formula ϕ.*

These propositions allow us to prove properties of expressions by **structural induction**, i.e., induction on the length of expressions; and we can also give definitions by **structural recursion**, i.e., recursion on the length of expressions, cf. Problem x6.4.

Definition 1B.6 (Free and bound variables)**.** Every occurrence of a variable in a term is **free**. The **free** occurrences of variables in formulas are defined by structural recursion as follows.

1. $\mathrm{FO}(s = t) = \mathrm{FO}(s) \cup \mathrm{FO}(t)$.
2. $\mathrm{FO}(\neg(\phi)) = \mathrm{FO}(\phi)$, $\mathrm{FO}((\phi)\ \&\ (\psi)) = \mathrm{FO}(\phi) \cup \mathrm{FO}(\psi)$, and similarly for the other connectives.
3. $\mathrm{FO}(\forall v\phi) = \mathrm{FO}(\exists v\phi) = \mathrm{FO}(\phi) \setminus \{v\}$, meaning that we remove from the free occurrences of variables in ϕ all the occurrences of the variable v.

An occurrence of a variable which is not free in an expression α is **bound** in α. The free variables of α are the variables which have at least one free occurrence in α; the bound variables of α are those which have at least one bound occurrence in α.

To illustrate what these notions mean, consider the three formulas in the language of arithmetic

$$\phi :\equiv \exists \mathrm{v}_1(+(\mathrm{v}_2, \mathrm{v}_1) = 0), \qquad \psi :\equiv \exists \mathrm{v}_5(+(\mathrm{v}_2, \mathrm{v}_5) = 0),$$
$$\chi :\equiv \exists \mathrm{v}_1(+(\mathrm{v}_5, \mathrm{v}_1) = 0)$$

As we read these formulas in English (unabbreviating the formal symbols), the first two of them say exactly the same thing: that we can add some number to v_2 and get 0—which is true exactly when v_2 is a name of 0. The third formula says the same thing about whatever number v_5 names, which need not be the same as the number named by v_2. In short, the "meaning" (and truth value) of a formula does not change if we replace its bound variables by others, but it may change when we change its free variables. A customary example from calculus is the notation we use for integrals: for $a \neq b$,

$$\int_0^a x^2 dx = \int_0^a y^2 dy = \frac{a^3}{3} \text{ but } \int_0^a x^2 dx \neq \int_0^b x^2 dx = \frac{b^3}{3},$$

which means that in the expression $\int_0^a x^2 dx$ the occurrences of x are bound, while a occurs freely.

An expression is **closed** if it has no free occurrences of variables. A closed formula is a **sentence**. The **universal closure** of a formula ϕ is the sentence

$$\vec{\forall}\, \phi \equiv_{\mathrm{df}} \forall \mathrm{v}_0 \forall \mathrm{v}_1 \dots \forall \mathrm{v}_n \phi,$$

where n is least so that all the free variables of ϕ are among $\mathrm{v}_0, \dots, \mathrm{v}_n$.

Note that a variable may occur both free and bound within a formula. For example, the following are well formed by the rules:

$$\exists \mathrm{v}_1 \forall \mathrm{v}_1 R(\mathrm{v}_1, \mathrm{v}_1), \quad (\exists \mathrm{v}_1 R(\mathrm{v}_1))\ \&\ (\forall \mathrm{v}_2 S(\mathrm{v}_1, \mathrm{v}_2))$$

(Think through what these formulas mean, and which variable occurrences are free or bound in them.)

1B.7. Abbreviations and misspellings. In practice we never write out terms and formulas in full: we use infix notation for terms, e.g.,

$$s + t \text{ for } +(s, t)$$

in arithmetic, we introduce and use abbreviations, we use "metavariables" (names) $x, y, z, u, v, \ldots$, for the specific formal variables of the language, we skip (or add) parentheses or replace parentheses by brackets or other punctuation marks, and (in general) we are satisfied with giving "instructions for writing out a formula" rather than exhibiting the actual formula. For example, the following sentence says about arithmetic that there are infinitely many prime numbers:

$$(\forall x)(\exists y)[x \leq y \;\&\; (\forall u)(\forall v)[(y = u \cdot v) \rightarrow (u = 1 \vee v = 1)]$$

where we have used the abbreviations

$$x \leq y :\equiv (\exists z)[x + z = y] \qquad 1 :\equiv S(0).$$

The correctly spelled sentence which corresponds to this is quite long (and unreadable).

Two useful logical abbreviations are for the "iff"

$$(\phi \leftrightarrow \psi) :\equiv ((\phi \rightarrow \psi) \;\&\; (\psi \rightarrow \phi))$$

and the quantifier "there exists exactly one"

$$(\exists! x)\phi :\equiv (\exists z)(\forall x)[\phi \leftrightarrow x = z],$$

where $z \not\equiv x$. (Think this through.) We also set

$$\bigvee_{0 \leq i \leq n} \phi_i :\equiv \phi_0 \vee \phi_1 \vee \cdots \vee \phi_n$$
$$\bigwedge_{0 \leq i \leq n} \phi_i :\equiv \phi_0 \;\&\; \phi_1 \;\&\; \cdots \;\&\; \phi_n$$

(and analogously for more complex sets of indices).

Definition 1B.8 (Substitution)**.** For each expression α, each variable v and each term t, the expression $\alpha\{v :\equiv t\}$ is the result of replacing all free occurrences of v in α by the term t; we say that t **is free for** v **in** α if no occurrence of a variable in t is bound in the result of the substitution $\alpha\{v :\equiv t\}$. The simultaneous substitution

$$\alpha\{v_1 :\equiv t_1, \ldots, v_n :\equiv t_n\}$$

is defined similarly: we replace simultaneously all the occurrences of each v_i in α by t_i. Note than in general

$$\alpha\{v_1 :\equiv t_1\}\{v_2 :\equiv t_2\} \not\equiv \alpha\{v_1 :\equiv t_1, v_2 :\equiv t_2\}.$$

If α is an expression, then $\alpha\{v_1 :\equiv t_1, \ldots, v_n :\equiv t_n\}$ is also an expression, and of the same kind—term or formula.

Definition 1B.9 (Extended expressions)**.** An **extended expression** is a pair $(\alpha, (v_1, \dots, v_n))$ of a (well formed) term or formula α and a list of distinct variables, We set

$$\alpha(v_1, \dots, v_n) :\equiv (\alpha, (v_1, \dots, v_n)),$$

and for any sequence of terms $t_1, \dots, t_n$, we set

$$\alpha(t_1, \dots, t_n) :\equiv \alpha\{v_1 :\equiv t_1, \dots, v_n :\equiv t_n\}.$$

This is essentially a notational convention, to facilitate dealing with substitutions, and the pedantic distinction between "expressions" and "extended expressions" is not always explicitly noted: we may refer to "a formula $\alpha(\vec{v})$", letting the notation indicate that we are really specifying both a formula α and a list $\vec{v} = (v_1, \dots, v_n)$.

An extended expression $\alpha(v_1, \dots, v_n)$ is **full** if the list $(v_1, \dots, v_n)$ includes all the variables which occur free in α.

Definition 1B.10 (Sublanguages)**.** If τ, τ' are vocabularies and each symbol of τ is a symbol (of the same kind and with the same arity) in τ', we say that τ is a **reduct** of τ' and we write $\tau \subseteq \tau'$.

1B.11. First order logic without identity. We will also work with the smaller language $\mathbb{FOL}^-$, which is obtained by removing the symbol $=$ and the clauses involving it in the definitions. There are no formulas in $\mathbb{FOL}^-(\tau)$, unless the signature τ has at least one relation symbol, and so when we state results about $\mathbb{FOL}^-(\tau)$, we will tacitly assume that the signature has at least one relation symbol.

1C. Semantics of $\mathbb{FOL}$

We interpret the terms and formulas of the language $\mathbb{FOL}(\tau)$ in structures of signature τ, which include the examples in Section 1A and are defined in general as follows:

Definition 1C.1 (Structures)**.** A **τ-structure** is a pair $\mathbf{A} = (A, I)$ where A is a non-empty collection of objects and I assigns to each constant symbol c a member $I(c)$ of A; to each n-ary relation symbol an n-ary relation $I(R) \subseteq A^n$; and to each n-ary function symbol f an n-ary function $I(f) : A^n \to A$. The set A is the **universe** of the structure $\mathbf{A}$, and the constants, relations and functions which interpret the symbols of the signature in $\mathbf{A}$ are its **primitives**. We set

$$c^{\mathbf{A}} = I(c), \quad R^{\mathbf{A}} = I(R), \quad f^{\mathbf{A}} = I(f),$$

so that the specification of a τ-structure can be given in the form

$$\mathbf{A} = (A, \{c^{\mathbf{A}}\}_{c \in \mathrm{Const}}, \{R^{\mathbf{A}}\}_{R \in \mathrm{Rel}}, \{f^{\mathbf{A}}\}_{f \in \mathrm{Funct}}).$$

In the typical case where there are only finitely many symbols in τ, we denote structures as tuples, as in Section 1A, so that a graph $\mathbf{G} = (G, R)$ is a (R)-structure and the structure $\mathbf{N} = (\mathbb{N}, 0, S, +, \cdot)$ of arithmetic is a $(0, S, +, \cdot)$-structure.

Definition 1C.2 (Homomorphisms and isomorphisms)**.** A **homomorphism**

$$\rho : \mathbf{A} \to \mathbf{B}$$

on one τ-structure $\mathbf{A} = (A, I)$ to another $\mathbf{B} = (B, J)$ is any mapping $\rho : A \to B$ which satisfies the following three conditions:

1. For each constant c, $\rho(c^{\mathbf{A}}) = c^{\mathbf{B}}$;
2. for each n-ary function symbol f and all $x_1, \dots, x_n \in A$,

$$\rho(f^{\mathbf{A}}(x_1, \dots, x_n)) = f^{\mathbf{B}}(\rho(x_1), \dots, \rho(x_n));$$

3. for each n-ary relation symbol R and all $x_1, \dots, x_n \in A$,

$$(1) \qquad R^{\mathbf{A}}(x_1, \dots, x_n) \Longrightarrow R^{\mathbf{B}}(\rho(x_1,), \dots, \rho(x_n));$$

it is a **strong homomorphism** if it also satisfies

$$(2) \qquad R^{\mathbf{A}}(x_1, \dots, x_n) \iff R^{\mathbf{B}}(\rho(x_1,), \dots, \rho(x_n)),$$

which is stronger than (1).

An **embedding** $\rho : \mathbf{A} \rightarrowtail \mathbf{B}$ is an injective strong homomorphism, and an **isomorphism** $\rho : \mathbf{A} \rightarrowtail\!\!\!\!\rightarrow \mathbf{B}$ is an embedding which is bijective (one-to-one and onto). We set

$$\mathbf{A} \simeq \mathbf{B} \iff \text{there exists an isomorphism } \rho : \mathbf{A} \rightarrowtail\!\!\!\!\rightarrow \mathbf{B},$$

and when these conditions hold, we say that $\mathbf{A}$ and $\mathbf{B}$ are **isomorphic**.

An isomorphism $\rho : \mathbf{A} \rightarrowtail\!\!\!\!\rightarrow \mathbf{A}$ of a structure $\mathbf{A}$ onto itself is an **automorphism** of $\mathbf{A}$, and a structure $\mathbf{A}$ is **rigid** if it has no automorphisms other than the (trivial) identity function $\mathrm{id} : A \rightarrowtail\!\!\!\!\rightarrow A$,

$$\mathrm{id}(x) = x.$$

The basic properties of homomorphisms in the next proposition are quite easy and we will leave the proof for Problem x1.4; here $\rho \circ \pi : V \to B$ is the composition of given $\pi : V \to A$ and $\rho : A \to B$,

$$(\rho \circ \pi)(v) = \rho(\pi(v)).$$

Proposition 1C.3. (a) *If $\rho : \mathbf{A} \to \mathbf{B}$ is a homomorphism, then for every term t and every assignment π into A,*

$$\mathrm{value}^{\mathbf{B}}(t, \rho \circ \pi) = \rho(\mathrm{value}^{\mathbf{A}}(t, \pi)).$$

(b) *If $\rho : \mathbf{A} \twoheadrightarrow \mathbf{B}$ is a surjective, strong homomorphism, then for every formula ϕ of $\mathbb{FOL}^-(\tau)$ and every assignment π into A,*

$$\mathbf{A}, \pi \models \phi \iff \mathbf{B}, \rho \circ \pi \models \phi, \tag{3}$$

so that, in particular, for every $\mathbb{FOL}^-(\tau)$-sentence χ,

$$\mathbf{A} \models \chi \iff \mathbf{B} \models \chi. \tag{4}$$

(c) *If $\rho : \mathbf{A} \rightarrowtail\!\!\!\twoheadrightarrow \mathbf{B}$ is an isomorphism, then* (3) *holds for all $\mathbb{FOL}(\tau)$-formulas ϕ, and* (4) *holds for all $\mathbb{FOL}(\tau)$-sentences χ.*

Definition 1C.4 (Substructures)**.** Suppose $\mathbf{A} = (A, I)$, $\mathbf{B} = (B, J)$ are τ-structures. We call $\mathbf{A}$ a **substructure** of $\mathbf{B}$ and $\mathbf{B}$ an **extension** of $\mathbf{A}$ and we write $\mathbf{A} \subseteq \mathbf{B}$ if the identity mapping $\mathrm{id} : A \rightarrowtail A$ an embedding of $\mathbf{A}$ to $\mathbf{B}$, i.e., if the following conditions hold.

1. $A \subseteq B$.
2. For each constant symbol c of τ, $c^{\mathbf{B}} = c^{\mathbf{A}} \in A$.
3. For each n-ary relation symbol R and all $x_1 \dots , x_n \in A$,
$$R^{\mathbf{B}}(x_1 \dots , x_n) \iff R^{\mathbf{A}}(x_1 \dots , x_n).$$
4. For each n-ary function symbol f and all $x_1 \dots , x_n \in A$,
$$f^{\mathbf{B}}(x_1 \dots , x_n) = f^{\mathbf{A}}(x_1 \dots , x_n) \in A.$$

For example, the field of rationals $\mathbf{Q}$ (the fractions) is a substructure of the field of real numbers $\mathbf{R}$ in the language of fields.

Definition 1C.5 (Expansions and reducts)**.** Suppose $\sigma \subseteq \tau$ are signatures, $\mathbf{A} = (A, I)$ is a σ-structure and $\mathbf{B} = (B, J)$ is a τ-structure. We call $\mathbf{A}$ a **reduct of** $\mathbf{B}$ and $\mathbf{B}$ an **expansion of** $\mathbf{A}$ if $A = B$ and for all symbols $C \in \sigma$, $I(C) = J(C)$. If $\mathbf{B}$ is a given τ-structure and $\sigma \subseteq \tau$, we define *the reduct of* $\mathbf{B}$ *to* σ by deleting from $\mathbf{B}$ the objects assigned to the symbols not in σ, formally

$$\mathbf{B} \upharpoonright \sigma = (B, J \upharpoonright \sigma).$$

Conversely, if $\tau \subseteq \sigma$, we can define expansions of $\mathbf{B}$ by assigning interpretations to the symbols in σ which are not in τ. The standard notation for this operation is

$$(\mathbf{B}, K) =_{\mathrm{df}} \text{the expansion of } \mathbf{B} \text{ by } K,$$

which is easier to understand in examples: $(\mathbb{N}, 0, S)$ and $(\mathbb{N}, 0, +)$ are reducts of the structure of arithmetic $\mathbf{N}$ obtained (in the first case) by deleting from the signature the symbols $+$ and $\cdot$, so that

$$(\mathbb{N}, 0, S) = \mathbf{N} \upharpoonright \{0, S\}.$$

A useful expansion of $\mathbf{N}$ is obtained by adding to the signature a symbol exp for exponentiation, and to $\mathbf{N}$ the corresponding operation,

$$(\mathbf{N}, \exp) = \text{ the expansion of } \mathbf{N} \text{ by exp.}$$

It is important to keep clear the (trivial) distinction between substructures-extensions and reducts-expansions.

Definition 1C.6 (Truth values). We will use the numbers 0 and 1 to denote the **truth values**, 0 for *falsity* and 1 for *truth*.

Definition 1C.7 (Assignments). An **assignment** into a structure $\mathbf{A}$ is any function $\pi : \text{Variables} \to A$. If v is a variable and $x \in A$, then $\pi\{v := x\}$ is the assignment which agrees with π on all variables except v, to which it assigns x:

$$\pi\{v := x\}(u) = \begin{cases} x, & \text{if } u \equiv v, \\ \pi(u), & \text{otherwise.} \end{cases}$$

We call $\pi\{v := x\}$ the **update** of π by (the reassignment) $v := x$.

Definition 1C.8 (Denotations and satisfaction). The **value** or **denotation** of a term for an assignment π is defined by structural recursion on the terms as follows:

1. $\text{value}(v, \pi) =_{\text{df}} \pi(v)$.
2. $\text{value}(c, \pi) =_{\text{df}} c^{\mathbf{A}}$.
3. $\text{value}(f(t_1, \dots, t_n), \pi) =_{\text{df}} f^{\mathbf{A}}(\text{value}(t_1, \pi), \dots, \text{value}(t_n, \pi))$.

In the same way, by structural recursion on formulas, we define the **truth value** or **denotation** of a formula for an assignment π:

1. $\text{value}(s = t, \pi) =_{\text{df}} \begin{cases} 1, & \text{if value}(s, \pi) = \text{value}(t, \pi), \\ 0, & \text{otherwise.} \end{cases}$
2. $\text{value}(R(t_1, \dots, t_n), \pi) =_{\text{df}} \begin{cases} 1, & \text{if } R^{\mathbf{A}}(\text{value}(t_1, \pi), \dots, \text{value}(t_n, \pi)), \\ 0, & \text{otherwise.} \end{cases}$
3. $\text{value}(\neg\phi, \pi) =_{\text{df}} 1 - \text{value}(\phi, \pi)$.
4. $\text{value}((\phi) \mathbin{\&} (\psi), \pi) = \min(\text{value}(\phi, \pi), \text{value}(\psi, \pi))$. For $\vee$ we take the maximum and for implication we use

$$\begin{aligned} \text{value}((\phi) \to (\psi), \pi) &=_{\text{df}} \text{value}((\neg(\phi)) \vee (\psi)) \\ &= \max(1 - \text{value}(\phi), \text{value}(\psi)). \end{aligned}$$

5. $\text{value}(\exists v\phi, \pi) =_{\text{df}} \max\{\text{value}(\phi, \pi\{v := x\}) \mid x \in A\}$.
6. $\text{value}(\forall v\phi, \pi) =_{\text{df}} \min\{\text{value}(\phi, \pi\{v := x\}) \mid x \in A\}$.

The denotation function depends on the structure, of course, although we suppressed this in the notation. When we need to exhibit the dependence we write

$$\text{value}^{\mathbf{A}}(\alpha, \pi) = \text{value}(\alpha, \pi),$$

and for formulas

$$\mathbf{A}, \pi \models \phi \iff_{\text{df}} \text{value}^{\mathbf{A}}(\phi, \pi) = 1.$$

If $\mathbf{A}, \pi \models \phi$, we say that **the assignment π satisfies ϕ in $\mathbf{A}$**.

Theorem 1C.9 (The Tarski truth conditions)**.** *The satisfaction relation on σ-structures, σ-formulas and assignments satisfies the following conditions:*

$$\begin{aligned}
\mathbf{A}, \pi \models s = t &\iff \text{value}^{\mathbf{A}}(t, \pi) = \text{value}^{\mathbf{A}}(s, \pi) \\
\mathbf{A}, \pi \models R(t_1, \dots, t_n) &\iff R^{\mathbf{A}}(\text{value}^{\mathbf{A}}(t_1, \pi), \dots, \text{value}^{\mathbf{A}}(t_n, \pi)) \\
\mathbf{A}, \pi \models \neg\phi &\iff \mathbf{A}, \pi \not\models \phi \\
\mathbf{A}, \pi \models \phi \mathbin{\&} \psi &\iff \mathbf{A}, \pi \models \phi \textit{ and } \mathbf{A}, \pi \models \psi \\
\mathbf{A}, \pi \models \phi \vee \psi &\iff \mathbf{A}, \pi \models \phi \textit{ or } \mathbf{A}, \pi \models \psi \\
\mathbf{A}, \pi \models \phi \to \psi &\iff \textit{either } \mathbf{A}, \pi \not\models \phi \textit{ or } \mathbf{A}, \pi \models \psi \\
\mathbf{A}, \pi \models \exists v\phi &\iff \textit{there exists an } x \in A \textit{ such that } \mathbf{A}, \pi\{v := x\} \models \phi \\
\mathbf{A}, \pi \models \forall v\phi &\iff \textit{for all } x \in A, \mathbf{A}, \pi\{v := x\} \models \phi
\end{aligned}$$

Proof is by structural induction on formulas. ⊣

Definition 1C.10 (Validity and semantic consequence)**.** . For any τ-formulas ϕ, we set:

$$\models \phi \iff (\text{for all } \mathbf{A}, \pi), \mathbf{A}, \pi \models \phi;$$

if $\models \phi$, we call ϕ **valid** or **logically true**, and if $\models \phi \to \psi$ we say that ϕ **logically implies** ψ or ψ **is a semantic** (or **logical**) **consequence of** ϕ. Two sentences are **semantically** (or **logically**) **equivalent** if each is a semantic consequence of the other.

Denotations of terms and formulas are defined in such a way that *the value of an expression is a function of the values of its subexpressions.* This is generally referred to as the **Compositionality Principle** for denotations, and it is the key to a mathematical analysis of denotations. The next theorem expresses it rigorously.

Theorem 1C.11 (Compositionality)**.** (1) *If the σ-structure $\mathbf{A}$ is a reduct of the τ-structure $\mathbf{B}$ where $\sigma \subseteq \tau$, then for every σ-expression α and every assignment π,*

$$\text{value}^{\mathbf{A}}(\alpha, \pi) = \text{value}^{\mathbf{B}}(\alpha, \pi).$$

(2) *If π, ρ are two assignments into the same structure $\mathbf{A}$ and for every variable v which occurs free in an expression α, $\pi(v) = \rho(v)$, then*

$$\text{value}^{\mathbf{A}}(\alpha, \pi) = \text{value}^{\mathbf{A}}(\alpha, \rho),$$

so that, in particular, for any formula χ,

$$\mathbf{A}, \pi \models \chi \iff \mathbf{A}, \rho \models \chi.$$

Proof of both claims is by structural induction on α. ⊣

By appealing to compositionality, we set for each full extended term $\alpha(v_1, \dots, v_n)$ and each n-tuple $(x_1, \dots, x_n)$ from A,

$$\alpha^{\mathbf{A}}[\vec{x}] =_{\text{df}} \text{value}^{\mathbf{A}}(\alpha, \pi\{\vec{v} := \vec{x}\}) \quad \text{(for any assignment } \pi\text{)},$$

and similarly, for any full extended formula $\phi(\vec{v})$,

$$\begin{aligned} \mathbf{A} \models \phi[\vec{x}] &\iff_{\text{df}} \text{ for some assignment } \pi, \mathbf{A}, \pi\{\vec{\mathrm{v}} := \vec{x}\} \models \phi \\ &\iff \text{ for every assignment } \pi, \mathbf{A}, \pi\{\vec{\mathrm{v}} := \vec{x}\} \models \phi. \end{aligned}$$

These useful notations are even simpler for closed expressions:

$$\begin{aligned} \text{value}^{\mathbf{A}}(\alpha) &=_{\text{df}} \text{value}^{\mathbf{A}}(\alpha, \pi) \qquad (\alpha \text{ closed}), \\ \mathbf{A} \models \phi &\iff_{\text{df}} \phi \text{ is } \mathbf{true} \text{ in } \mathbf{A} (\phi \text{ a sentence}) \\ &\iff \mathbf{A}, \pi \models \phi \end{aligned}$$

where π is any assignment. A τ-sentence is **valid** if it is true in all τ-structures.

1D. First order definability

A proposition Φ of ordinary (mathematical) English, about a certain τ-structure $\mathbf{A}$ is *expressed* by a sentence ϕ of $\mathbb{FOL}(\tau)$ if Φ and ϕ "mean" the same thing; similarly, a proposition $\Phi(x)$ about an arbitrary object x in a structure $\mathbf{A}$ is *expressed* by a formula $\phi(x)$ with one free variable x, if for each $x \in A$, $\Phi(x)$ and $\phi(x)$ "mean" the same thing. For example,

$$(\forall x)[x + 0 = x] \text{ means "every number added to 0 yields itself".}$$

We cannot make this notion of "expressing" precise unless we first define *meaning* rigorously for both natural language and $\mathbb{FOL}$. On the other hand, we have a clear, intuitive understanding of it which is important for applications: roughly speaking, ϕ expresses Φ if we can construct the first from the second by straightforward translation, more-or-less word for word, "and", "but", "also" going to & , "all", "each", "any" going to $\forall$, etc. For example, "every number is either odd or even" refers to the structure of arithmetic and translates to something of the form

$$(\forall x)[\phi(x) \vee \psi(x)]$$

where $\phi(x)$ and $\psi(x)$ can be constructed to express the properties of being odd or even.

As it turns out, all mathematical propositions and properties can be expressed by $\mathbb{FOL}(\tau)$-sentences or formulas on appropriate structures. This is one of the main discoveries of modern mathematical logic and the source of its applications to mathematics. We will explain how it works in the sequel, starting in this section with the theory of first order definability on a fixed structure.

Definition 1D.1 (The basic local notions)**.** Suppose $\mathbf{A}$ is a τ-structure.

An n-ary relation $R \subseteq A^n$ on A is **first order definable** or **elementary** on $\mathbf{A}$, if there is a full extended formula $\chi(v_1, \dots, v_n)$ such that

$$R(\vec{x}) \iff \mathbf{A} \models \chi[\vec{x}] \quad (\vec{x} \in A^n).$$

A function $f : A^n \to A$ is **A-explicit** if for some full extended term $\alpha(\vec{v})$

$$f(\vec{x}) = \alpha^{\mathbf{A}}[\vec{x}] \quad (\vec{x} \in A^n).$$

A function $f : A^n \to A$ is **first order definable** or **elementary** on $\mathbf{A}$ if its **graph**

$$G_f(\vec{x}, w) \iff f(\vec{x}) = w$$

is elementary on $\mathbf{A}$, i.e., if there is a full extended formula $\chi(\vec{v}, u)$ such that

$$f(\vec{x}) = w \iff \mathbf{A} \models \chi[\vec{x}, w].$$

The elementary functions and relations of the standard structure $\mathbf{N}$ of arithmetic are called **arithmetical**.

The next theorem is useful, as it often frees us from needing to worry excessively about the formal syntax of $\mathbb{FOL}$.

Theorem 1D.2. *The collection $\mathcal{E}(\mathbf{A})$ of $\mathbf{A}$-elementary functions and relations on the universe of a structure*

$$\mathbf{A} = (A, \{c^{\mathbf{A}}\}_{c \in \mathrm{Const}}, \{R^{\mathbf{A}}\}_{R \in \mathrm{Rel}}, \{f^{\mathbf{A}}\}_{f \in \mathrm{Funct}})$$

has the following properties:

(1) *Each primitive relation $R^{\mathbf{A}}$ is $\mathbf{A}$-elementary; and the (binary) identity relation $x = y$ is $\mathbf{A}$-elementary.*

(2) *For each constant symbol c and each n, the n-ary constant function*

$$g(\vec{x}) = c^{\mathbf{A}}$$

is $\mathbf{A}$-elementary; each primitive function $f^{\mathbf{A}}$ is $\mathbf{A}$-elementary; and every projection function

$$P^n_i(x_1, \dots, x_n) = x_i \quad (1 \le i \le n)$$

is $\mathbf{A}$-elementary.

(3) $\mathcal{E}(\mathbf{A})$ *is closed under substitutions of* $\mathbf{A}$*-elementary functions: i.e., if* $h(u_1, \dots, u_m)$ *is an* m*-ary* $\mathbf{A}$*-elementary function and* $g_1(\vec{x}), \dots, g_m(\vec{x})$ *are* n*-ary,* $\mathbf{A}$*-elementary, then the function*

$$f(\vec{x}) = h(g_1(\vec{x}), \dots, g_m(\vec{x}))$$

is $\mathbf{A}$*-elementary; and if* $P(u_1, \dots, u_m)$ *is an* m*-ary* $\mathbf{A}$*-elementary relation, then the* n*-ary relation*

$$Q(\vec{x}) \iff P(g_1(\vec{x}), \dots, g_m(\vec{x}))$$

is $\mathbf{A}$*-elementary.*

(4) $\mathcal{E}(\mathbf{A})$ *is closed under the propositional operations: i.e., if* $P_1(\vec{x})$ *and* $P_2(\vec{x})$ *are* $\mathbf{A}$*-elementary,* n*-ary relations, then so are the following relations:*

$$\begin{aligned} Q_1(\vec{x}) &\iff \neg P_1(\vec{x}), \\ Q_2(\vec{x}) &\iff P_1(\vec{x}) \mathbin{\&} P_2(\vec{x}), \\ Q_3(\vec{x}) &\iff P_1(\vec{x}) \vee P_2(\vec{x}), \\ Q_4(\vec{x}) &\iff P_1(\vec{x}) \to P_2(\vec{x}). \end{aligned}$$

(5) $\mathcal{E}(\mathbf{A})$ *is closed under quantification on* A*, i.e., if* $P(\vec{x}, y)$ *is* $\mathbf{A}$*-elementary, then so are the relations*

$$\begin{aligned} Q_1(\vec{x}) &\iff (\exists y)P(\vec{x}, y), \\ Q_2(\vec{x}) &\iff (\forall y)P(\vec{x}, y). \end{aligned}$$

Moreover: $\mathcal{E}(\mathbf{A})$ *is the smallest collection of functions and relations on* A *which satisfies* (1) – (5).

Proof. To show that $\mathcal{E}(\mathbf{A})$ has these properties, we need to construct lots of formulas and appeal repeatedly to the definition of $\mathbf{A}$-elementary functions and relations; this is tedious, but not difficult.

For the second ("moreover") claim, we first make it precise by replacing $\mathcal{E}(\mathbf{A})$ by $\mathcal{F}$ throughout (1) – (5), and (temporarily) calling a class $\mathcal{F}$ of functions and relations *good* if it satisfies all these conditions—so what has already been shown is that $\mathcal{E}(\mathbf{A})$ is good. The additional claim is that *every good* $\mathcal{F}$ *contains all* $\mathbf{A}$*-elementary functions and relations*, and it is verified by structural induction on the formula χ such that some full extension of it $\chi(\vec{v})$ defines a given, $\mathbf{A}$-elementary relation—after showing, easily, that the graph of every $\mathbf{A}$-explicit function is in $\mathcal{F}$. ⊣

The theorem suggests that $\mathcal{E}(\mathbf{A})$ is a very rich class of relations and functions. As it turns out, this is true for "rich", "standard" structures like $\mathbf{N}$, but not true for structures with simple primitives—e.g., the plain (A) which has no primitives. We consider examples of these two kinds of structures in the next two sections.

1E. Arithmetical functions and relations

Is the exponential function

$$\exp(t, x) = x^t \quad (x, t \in \mathbb{N})$$

arithmetical? Not obviously—but it is, as a corollary of a basic result about *definition by recursion in* $\mathbf{N}$ which we will prove in this section, and which has many important applications.

Definition 1E.1 (Primitive recursion)**.** A function $f : \mathbb{N} \to \mathbb{N}$ is defined by **primitive recursion** from the number $w_0 \in \mathbb{N}$ and the binary function $h(w, t)$ if it satisfies the following two equations, for all t:

$$f(0) = w_0, \quad f(t + 1) = h(f(t), t); \tag{5}$$

in greater generality, a function $f : \mathbb{N}^{n+1} \to \mathbb{N}$ of $n + 1$ arguments on the natural numbers is defined by **primitive recursion** from the n-ary function g and the $(n + 2)$-ary function h if it satisfies the following two equations, for all $t, \vec{x}$:

$$f(0, \vec{x}) = g(\vec{x}), \quad f(t + 1, \vec{x}) = h(f(t, \vec{x}), t, \vec{x}). \tag{6}$$

For example, if we set

$$f(0, x) = x, \quad f(t + 1, x) = S(f(t, x)),$$

then (easily, by induction on t)

$$f(t, x) = t + x,$$

and so addition is defined by primitive recursion from the two, simpler functions

$$g(x) = x, \quad h(w, t, x) = S(w),$$

i.e., (essentially) the identity and the successor. Similarly, if we set

$$f(0, x) = 0, \quad f(t + 1, x) = f(t, x) + x,$$

then, easily, $f(t, x) = t \cdot x$, and so multiplication is defined by primitive recursion from the functions

$$g(x) = 0, \quad h(w, t, x) = w + t,$$

i.e., (essentially) the constant 0 and addition. More significantly (for our purposes here),

$$\exp(0, x) = x^0 = 1, \quad \exp(t + 1, x) = x^{t+1} = x^t \cdot x = \exp(t, x) \cdot x,$$

so that exponentiation is defined by primitive recursion from the functions

$$g(x) = 1, \quad h(w, t, x) = w \cdot x,$$

i.e., (essentially) the constant 1 and multiplication.

Theorem 1E.2. *If* $f : \mathbb{N}^{n+1} \to \mathbb{N}$ *is defined by the primitive recursion* (6) *above and* g, h *are arithmetical, then so is* f.

To prove this we must reduce the recursive definition of f into an explicit one, and this is done using *Dedekind's analysis of recursion*:

Proposition 1E.3. *If* $f : \mathbb{N}^{n+1} \to \mathbb{N}$ *is defined by the primitive recursion in* (6), *then for all* $t, \vec{x}, w$,

(7) $f(t,\vec{x}) = w \iff$ *there exists a sequence* $(w_0, \dots, w_t)$ *such that*

$$w_0 = g(\vec{x}) \;\&\; (\forall s < t)[w_{s+1} = h(w_s, s, \vec{x})] \;\&\; w = w_t.$$

PROOF. If $f(t,\vec{x}) = w$, set $w_s = f(s,\vec{x})$ for $s \leq t$, and verify easily that the sequence $(w_0, \dots, w_t)$ satisfies the conditions on the right. For the converse, suppose that $(w_0, \dots, w_t)$ satisfies the conditions on the right and prove by (finite) induction on $s \leq t$ that $w_s = f(s,\vec{x})$. ⊣

We can view the equivalence (7) as a theorem about recursive definitions which have already been justified in some other way; or we can see it as a definition of a function f which satisfies the recursive equations (6) and so justifies recursive definitions—which is how Dedekind saw it. In any case, it reduces proving Theorem 1E.2 to justifying *quantification over finite sequences* within the class of arithmetical relations, and we will do this by an *arithmetical coding* of finite sequences whose construction requires a couple of basic facts from arithmetic.

Proposition 1E.4 (The Division Theorem). *For every natural number* $y > 0$ *and every* $x \in \mathbb{N}$, *there exist exactly one* q *and one* r *such that*

(8) $$x = y \cdot q + r \text{ and } 0 \leq r < y.$$

This is verified easily by induction on x. If (8) holds, we set

$$\mathrm{quot}(x,y) = q, \quad \mathrm{rem}(x,y) = r,$$

and for completeness, we also let $\mathrm{quot}(x,0) = 0, \mathrm{rem}(x,0) = x$.

Theorem 1E.5 (The Chinese Remainder Theorem). *If* $d_0, \dots, d_t$ *are relatively prime numbers and* $w_0 < d_0, \dots, w_t < d_t$, *then there exists some number* a *such that*

$$w_0 = \mathrm{rem}(a, d_0), \dots, w_t = \mathrm{rem}(a, d_t).$$

PROOF. Consider the set D of all $(t+1)$-tuples bounded by the given numbers $d_0, \dots, d_t$,

$$D = \{(w_0, \dots, w_t) \mid w_0 < d_0, \dots, w_t < d_t\},$$

which has $|D| = d_0 d_1 \cdots d_t$ members, and let

$$A = \{a \mid a < |D|\}$$

which is equinumerous with D. Define the function $\pi : A \to D$ by

$$\pi(a) = (\mathrm{rem}(a, d_0), \mathrm{rem}(a, d_1), \ldots, \mathrm{rem}(a, d_t)).$$

Now π is injective (one-to-one), because if $f(a) = f(b)$ with $a < b < |D|$, then $b - a$ is divisible by each of $d_0, \ldots, d_t$ and hence by their product D (which is what their being relatively prime implies); hence $d \le b - a$, which is absurd since $a < b < |D|$. We now apply the Pigeonhole Principle: since A and D are equinumerous and $\pi : A \rightarrowtail D$ is an injection, it must be a surjection, and hence whatever $(w_0, \ldots, w_t)$ may be, there is an $a < d$ such that

$$\pi(a) = (\mathrm{rem}(a, d_0), \mathrm{rem}(a, d_1), \ldots, \mathrm{rem}(a, d_t)) = (w_0, \ldots, w_t). \qquad \dashv$$

The idea now is to code an arbitrary tuple $(w_0, \ldots, w_t)$ by a pair of numbers (d, a), where d can be used to produce uniformly $t + 1$ relatively prime numbers $d_0, \ldots, d_t$ and then a comes from the Chinese Remainder Theorem.

Lemma 1E.6 (Gödel's β-function)**.** *Set*

$$\beta(a, d, i) = \mathrm{rem}(a, 1 + (i + 1)d).$$

This is an arithmetical function, and for each sequence of numbers $w_0, \ldots, w_t$ there exist numbers a and d such that

$$\beta(a, d, 0) = w_0, \ldots, \beta(a, d, t) = w_t.$$

Proof. The β-function is arithmetical because it is defined by substitutions from addition, multiplication and the remainder function, which is arithmetical since

$$\mathrm{rem}(x, y) = r \iff (\exists q)[x = yq + r \;\&\; r < y].$$

To find the required a, d which code the tuple $(w_0, \ldots, w_t)$, set

$$s = \max(t + 1, w_0, \ldots, w_t), \quad d = s!$$

and verify that the $t + 1$ numbers

$$d_0 = 1 + (0 + 1)d, d_1 = 1 + (1 + 1)d, \ldots, d_t = 1 + (t + 1)d$$

are relatively prime. (If a prime p divides $1 + (1 + i)s!$ and also $1 + (1 + j)s!$ with $i < j$, then it must divide their difference $(j - i)s!$, and hence it must divide one of $(j - i)$ or $s!$; in either case, it divides $s!$, since $(j - i) \le s$, and then it must divide 1, since it is assumed to divide $1 + (1 + i)s!$, which is absurd.) It is also immediate that $w_i < d = s!$, by the definition of s, and so the Chinese Remainder Theorem supplies some a such that

$$(w_0, \ldots, w_t) = (\mathrm{rem}(a, d_0), \ldots, d_t) = (\beta(a, d, 0), \ldots, \beta(a, d, t))$$

as required. $\dashv$

PROOF OF THEOREM 1E.2. By the Dedekind analysis and using the β-function to code tuples, we have

$$f(t,\vec{x}) = w \iff (\exists a)(\exists d)\Big[\beta(a,d,0) = g(\vec{x})$$
$$\& \ (\forall s < t)[\beta(a,d,s+1) = h(\beta(a,d,s),s,\vec{x})] \ \& \ \beta(a,d,t) = w\Big]$$

Thus the graph of f is arithmetical, by the closure properties of the arithmetical functions and relations in Theorem 1D.2. $\dashv$

There is no standard definition of *rich structure*, but the following notion covers the most important examples:

Definition 1E.7 (Structures with tuple coding)**.** A *copy of* $\mathbf{N}$ in a structure $\mathbf{A}$ is a structure $\mathbf{N}' = (\mathbb{N}', 0', S', +', \cdot')$ such that:

1. $\mathbf{N}'$ is isomorphic with the structure of arithmetic $\mathbf{N}$.
2. $\mathbb{N}' \subseteq A$.
3. The set $\mathbb{N}'$, the object $0'$ and the functions $S', +'$ and $\cdot'$ are all $\mathbf{A}$-elementary.

A structure $\mathbf{A}$ **admits tuple coding** if it has a copy of $\mathbf{N}$ and there is an $\mathbf{A}$-elementary function $\gamma : A^{n+1} \to A$ such that for every tuple $w_0, \dots, w_t \in A$, there is some $\vec{a} \in A^n$ such that

$$\gamma(\vec{a}, 0) = w_0, \gamma(\vec{a}, 1) = w_1, \dots, \gamma(\vec{a}, t) = w_t,$$

where $0, 1, \dots, t$ are the "$\mathbf{A}$-numbers" $0, 1, \dots, t$ (i.e., the copies of these numbers into A by the given isomorphism of $\mathbf{N}$ with $\mathbf{N}'$).

In this definition, γ plays the role of the β-function in $\mathbf{N}$, and we have allowed for the possibility that triples ($n = 3$) or quadruples ($n = 4$) are needed to code tuples of arbitrary length in A using γ. We might have also allowed the natural numbers to be coded by pairs of elements of A or tweak the definition in various other ways, but this version captures all the interesting examples already. The key result is:

Proposition 1E.8. *Suppose* $\mathbf{A}$ *admits coding of tuples,*

$$g : A^n \to A, \quad h : A^{n+2} \to A;$$

are $\mathbf{A}$*-elementary,* $f : A^{n+1} \to A$*, and for* $t \in N', y \notin N'$*,*

$$f(0,\vec{x}) = g(\vec{x}), \quad f(t+1,\vec{x}) = h(f(t,\vec{x}),t,\vec{x})), \quad f(y,\vec{x}) = y; \tag{9}$$

it follows that f *is* $\mathbf{A}$*-elementary.*

It can be used to show that structures which admit tuple coding have a rich class of elementary functions and relations.

Example 1E.9 (The integers)**.** The ring of (rational) *integers*

$$\mathbf{Z} = (\mathbb{Z}, 0, 1, +, \cdot) \quad (\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}) \tag{10}$$

admits tuple coding.

To see this, we use the fact that $\mathbb{N} \subseteq \mathbb{Z}$, and it is a $\mathbf{Z}$-elementary set because of *Lagrange's Theorem*, by which *every natural number is the sum of four squares*:

$$x \in \mathbb{N} \iff (\exists u, v, s, t)[x = u^2 + v^2 + s^2 + t^2] \quad (x \in \mathbb{Z}).$$

We can then use the β-function (with some tweaking) to code tuples of integers.

Example 1E.10 (The fractions)**.** The field of *rational numbers* (fractions)

$$\mathbf{Q} = (\mathbb{Q}, 0, 1, +, \cdot)$$

admits tuple coding.

This is a classical theorem of Julia Robinson which depends on a non-trivial, $\mathbf{Q}$-elementary definition of $\mathbb{N}$ within $\mathbb{Q}$.

Example 1E.11 (The real numbers, with $\mathbb{Z}$)**.** The *structure of analysis*

$$(\mathbf{R}, \mathbb{Z}) = (\mathbb{R}, 0, 1, \mathbb{Z}, +, \cdot)$$

admits tuple coding.

This requires some work—and it is not a luxury that we have included the integers as a distinguished subset: the *field of real numbers*

$$\mathbf{R} = (\mathbb{R}, 0, 1, +, \cdot)$$

does not admit tuple coding. We will discuss this very interesting, classical structure later.

1F. Quantifier elimination

At the other end of the class of structures which admit tuple coding are some important, classical structures which are, in some sense, very "simple": the elementary functions and relations on them are quite trivial. We will consider some examples of such structures in this section, and we will isolate the property of *quantifier elimination* which makes them "simple"—much as tuple coding makes the structures in the preceding section complex.

We list first, for reference, some simple logical equivalences which we will be using, and to simplify notation, we set for arbitrary τ-formulas ϕ, ψ and any τ-structure $\mathbf{A}$:

$$\phi \asymp_{\mathbf{A}} \psi \iff \mathbf{A} \models \phi \leftrightarrow \psi,$$
$$\phi \asymp \psi \iff \models \phi \leftrightarrow \psi.$$

Proposition 1F.1 (Basic logical equivalences).

(1) *The distributive laws:*

$$\phi \mathbin{\&} (\psi \vee \chi) \asymp (\phi \mathbin{\&} \psi) \vee (\phi \mathbin{\&} \chi)$$
$$\phi \vee (\psi \mathbin{\&} \chi) \asymp (\phi \vee \psi) \mathbin{\&} (\phi \vee \chi)$$

(2) *De Morgan's laws:*

$$\neg(\phi \mathbin{\&} \psi) \asymp \neg\phi \vee \neg\psi$$
$$\neg(\phi \vee \psi) \asymp \neg\phi \mathbin{\&} \neg\psi$$

(3) *Double negation, implication and the universal quantifier:*

$$\neg\neg\phi \asymp \phi, \qquad \phi \rightarrow \psi \asymp \neg\phi \vee \psi, \quad \forall x\phi \asymp \neg(\exists x)\neg\phi$$

(4) *Renaming of bound variables: if y is a variable which does not occur in ϕ and $\phi\{x :\equiv y\}$ is the result of replacing x by y in all its free occurrences, then*

$$\exists x\phi \asymp \exists y\phi\{x :\equiv y\}$$
$$\forall x\phi \asymp \forall y\phi\{x :\equiv y\}$$

(5) *Distribution law for $\exists$ over $\vee$:*

$$\exists x(\phi_1 \vee \cdots \vee \phi_n) \asymp \exists x\phi_1 \vee \cdots \vee \exists x\phi_n$$

(6) *Pulling the quantifiers to the front: if x does not occur free in ψ, then*

$$\exists x\phi \mathbin{\&} \psi \asymp \exists x(\phi \mathbin{\&} \psi)$$
$$\exists x\phi \vee \psi \asymp \exists x(\phi \vee \psi)$$
$$\forall x\phi \mathbin{\&} \psi \asymp \forall x(\phi \mathbin{\&} \psi)$$
$$\forall x\phi \vee \psi \asymp \forall x(\phi \vee \psi)$$
$$\forall x\phi \rightarrow \psi \asymp \exists x[\phi \rightarrow \psi]$$
$$\exists x\phi \rightarrow \psi \asymp \forall x[\phi \rightarrow \psi]$$

(7) *The general distributive laws: for all natural numbers n, k and every doubly-indexed sequence of formulas $\phi_{i,j}$ with $i \leq n, j \leq k$,*

$$\bigwedge_{i\leq n} \bigvee_{j\leq k} \phi_{i,j} \asymp \bigvee_{f:\{0,\ldots,n\}\to\{0,\ldots,k\}} \bigwedge_{i\leq n} \phi_{i,f(i)}. \tag{11}$$

$$\bigvee_{i\leq n} \bigwedge_{j\leq k} \phi_{i,j} \asymp \bigwedge_{f:\{0,\ldots,n\}\to\{0,\ldots,k\}} \bigvee_{i\leq n} \phi_{i,f(i)}. \tag{12}$$

Proof. To see (11), fix a structure $\mathbf{A}$ and an assignment π and compute:

$$\begin{aligned}
&\mathbf{A}, \pi \models \bigwedge\!\!\!\bigwedge_{i \le n} \bigvee\!\!\!\bigvee_{j \le k} \phi_{i,j} \\
&\qquad \Longleftrightarrow \text{ for each } i \le n, \text{ there is some } j \le k \text{ such that } \mathbf{A}, \pi \models \phi_{i,j} \\
&\qquad\qquad \Longleftrightarrow \text{ there is a function } f : \{0, \dots, n\} \to \{0, \dots, k\} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{such that for all } i \le n, \mathbf{A}, \pi \models \phi_{i,f(i)},
\end{aligned}$$

where (in the implication from left to right) the function f in the last equivalence assigns to each $i \le n$ the least $j = f(i) \le k$ such that $\mathbf{A}, \pi \models \phi_{i,j}$. The dual (12) is established by taking the negation of both sides of (11) applied to $\neg\phi_{i,j}$, pushing the negation through the conjunctions and disjunctions using De Morgan's laws, and finally using the obvious $\neg\neg\phi_{i,j} \asymp \phi_{i,j}$. ⊣

1F.2 (Literals)**.** For the constructions in the remainder of this section, it is useful to enrich the language $\mathbb{FOL}(\tau)$ with propositional constants T, F for truth and falsity. We may think of these as abbreviations,

$$T :\equiv \exists x(x = x), \quad F :\equiv \forall x(x \neq x),$$

considered (by convention) as prime formulas.

A **literal** is either a prime formula $R(t_1, \dots, t_n)$, $s = t$, T, F, or the negation of a prime formula.

Proposition 1F.3 (Disjunctive normal form)**.** *Every quantifier-free formula χ is* (effectively) *logically equivalent to a disjunction of conjunctions of literals which has no more variables than χ: i.e., for suitable n, n_i, and literals ℓ_{ij} $(i = 1, \dots, n, j = 1, \dots, n_i)$ whose variables all occur in χ,*

$$\chi \asymp \chi^* \equiv \phi_1 \vee \cdots \vee \phi_n, \text{ where for } i = 1, \dots, n,\ \phi_i \asymp \ell_{i1} \ \&\ \cdots\ \&\ \ell_{in_i}.$$

By the definition in the proposition, $x = y \vee \neg(z = z)$ is not a disjunctive normal form of $x = y$ (if all three variables are distinct), even though

$$x = y \asymp x = y \vee \neg(z = z)$$

Proof. We show by structural induction that for every quantifier-free formula χ, both χ and its negation $\neg\chi$ are logically equivalent to a disjunction of conjunctions of literals, among which we count T (truth) and F (falsity).

The result is trivial in the Basis, when χ is prime, since χ and $\neg\chi$ are in disjunctive normal form with $n = 1$, $n_1 = 1$, and $\ell_{11} \equiv \chi$ or $\ell_{11} \equiv \neg\chi$.

In the Induction Step, the proposition is immediate for $\chi \equiv \neg\chi_1$, since the Induction Hypothesis gives us disjunctive normal form for $\chi_1 \asymp \neg\chi$ and $\neg\chi_1 \equiv \chi$.

If χ is a disjunction or conjunction of χ_1 and χ_2, we may assume that the disjunctive normal forms for χ_1 and χ_2

$$\chi_1 \asymp \bigvee_{i<n} \bigwedge_{j<k} \chi_{1,i,j}, \qquad \chi_2 \asymp \bigvee_{i<n} \bigwedge_{j<k} \chi_{2,i,j}$$

given by the induction hypothesis have the same number of disjuncts and conjuncts, by "padding"—adding harmless insertions of T and F. We get immediately a disjunctive normal form for the disjunction:

$$\begin{aligned}\chi_1 \vee \chi_2 &\asymp \Big(\bigvee_{i<n} \bigwedge_{j<k} \chi_{1,i,j}\Big) \vee \Big(\bigvee_{i<n} \bigwedge_{j<k} \chi_{2,i,j}\Big)\\ &\asymp \bigvee_{i<2n} \Big[\text{either } i<n \text{ and } \bigwedge_{j<k} \chi_{1,i,j} \text{ or } n \leq i \text{ and } \bigwedge_{j<k} \chi_{1,i-n,j}\Big]\\ &\asymp \bigvee_{i<2n} \bigwedge_{j<k} \widetilde{\chi}_{2,i,j}\end{aligned}$$

where

$$\widetilde{\chi}_{i,j} \equiv \begin{cases} \bar{\chi}_{1,i,j}, & \text{if } i<n,\\ \bar{\chi}_{2,i-n,j}, & \text{otherwise.}\end{cases}$$

To get a disjunctive normal form for the conjunction $\chi_1 \,\&\, \chi_2$, we use the distributive laws (11), (12) which give us equivalent *conjunctive normal forms*

$$\chi_1 \asymp \bigwedge_{i<\bar{n}} \bigvee_{j<\bar{k}} \bar{\chi}_{1,i,j}, \qquad \chi_2 \asymp \bigwedge_{i<\bar{n}} \bigvee_{j<\bar{k}} \bar{\chi}_{2,i,j}$$

for the conjuncts, and using these we compute as above:

$$\chi_1 \,\&\, \chi_2 \asymp \Big(\bigwedge_{i<\bar{n}} \bigvee_{j<\bar{k}} \bar{\chi}_{1,i,j}\Big) \,\&\, \Big(\bigwedge_{i<\bar{n}} \bigvee_{j<\bar{k}} \bar{\chi}_{2,i,j}\Big) \asymp \bigwedge_{i<2\bar{n}} \bigvee_{j<\bar{k}} \widetilde{\chi}_{i,j}$$

where

$$\widetilde{\chi}_{i,j} \equiv \begin{cases} \bar{\chi}_{1,i,j}, & \text{if } i<\bar{n},\\ \bar{\chi}_{2,i-\bar{n},j}, & \text{otherwise.}\end{cases}$$

We now use (11) again to get a disjunctive normal form for $\chi_1 \,\&\, \chi_2$.

These two computations also give us disjunctive normal forms for the negations of disjunction and conjunctions by appealing to the De Morgan Laws, and also for implication, using $\chi_1 \rightarrow \chi_2 \asymp \neg\chi_1 \vee \chi_2$. ⊣

Proposition 1F.4 (Prenex normal forms)**.** *Every formula χ is* (effectively) *logically equivalent to a formula*

$$\chi^* \equiv Q_1 x_1 \cdots Q_n x_n \psi \quad (\psi \textit{ quantifier-free})$$

in prenex form, whose free variables are among the free variables of χ.

Definition 1F.5 (Quantifier elimination for structures)**.** A *quantifier-free normal form* for a formula χ in a structure $\mathbf{A}$, is any quantifier-free formula χ^* (in which T or F may appear) whose variables are among the free variables of χ and such that

$$\chi \asymp_{\mathbf{A}} \chi^*.$$

A structure **A admits elimination of quantifiers**, if every formula χ has a quantifier-free normal form in **A**; and it **admits effective elimination of quantifiers**, if there is an effective procedure which will compute for each χ a quantifier-free normal form for χ in **A**.

1F.6. Quanitifier elimination and decidability. To see the importance of this notion, suppose the vocabulary τ is purely relational, i.e., it has no constant or function symbols. Now the only quantifier-free sentences are T and F; and so if a τ-structure **A** admits effective quantifier elimination, then we can effectively decide for each sentence χ whether it is logically equivalent in **A** to T or F—in other words, we have a **decision procedure for truth in A**.

More generally, suppose τ may have constants and function symbols and **A** admits effective quantifier elimination: if we have a decision procedure for quantifier-free *sentences* (with no variables), then we have a decision procedure for truth in **A**. The hypothesis is, in fact, satisfied in most structures that occur naturally in mathematics, including (trivially) the structure of arithmetic $\mathbf{N} = (\mathbb{N}, 0, 1, +, \cdot)$; so we cannot expect that **N** admits effective quantifier elimination, because we don't expect it to be decidable—and in time we will *prove* that it is not decidable.

Lemma 1F.7 (Quantifier elimination test). *If every formula of the form*

$$\chi \equiv \exists x[\chi_1 \ \& \ \cdots \ \& \ \chi_n] \quad (\textit{where } \chi_1, \dots, \chi_n \textit{ are literals})$$

is (effectively) equivalent in a structure **A** *to a quantifier-free formula whose variables are all among the free variables of* χ*, then* **A** *admits (effective) quantifier elimination.*

Proof. Let $\mathcal{F}$ be the set of formulas which (effectively) have quantifier free forms in **A**. By (3) of Proposition 1F.1, it is enough to show that $\mathcal{F}$ contains all literals, which it clearly does; that it is closed under $\neg$, & and $\vee$, which it clearly is; and that it is closed under existential quantification. For the latter, if

$$\chi \equiv \exists x \phi$$

with ϕ quantifier-free, we bring ϕ to disjunctive normal form, so that

$$\chi \asymp \exists x[\phi_1 \vee \cdots \vee \phi_n] \asymp \exists x \phi_1 \vee \cdots \vee \exists x \phi_n$$

where each ϕ_i is a conjunction of literals and then we use the hypothesis of the Lemma. ⊣

Proposition 1F.8. *For each infinite set* A*, the structure* $\mathbf{A} = (A)$ *in the language with empty vocabulary admits effective quantifier elimination.*

Proof. By the Basic Test 1F.7, it is enough to eliminate the quantifier from every formula of the form

$$\chi \asymp \exists x[(x = z_1 \ \&\ \cdots\ \&\ x = z_k)\ \&\ (u_1 = v_1\ \&\ \cdots u_l = v_l)$$
$$\&\ (x \neq w_1\ \&\ \cdots\ \&\ x \neq w_m)\ \&\ (s_1 \neq t_1\ \&\ \cdots\ \&\ t_o \neq s_o)]$$

where we have grouped the variable equations and inequations according to whether x occurs in them or not; i.e., x is none of the variables u_i, v_i, s_i, t_i. We can also assume that x is none of the variables z_i, since the equation $x = x$ can simply be deleted; and it is none of the variables w_i, since if $x \neq x$ is one of the conjuncts, then $\chi \asymp F$.

Case 1, $k = 0$, i.e., there is no equation of the form $x = z$ in the matrix of χ. In this case

$$\chi \asymp (u_1 = v_1\ \&\ \cdots u_l = v_l)\ \&\ (s_1 \neq t_1\ \&\ \cdots\ \&\ t_m \neq s_m).$$

This is because if π is any assignment which satisfies

$$(u_1 = v_1\ \&\ \cdots u_l = v_l)\ \&\ (s_1 \neq t_1\ \&\ \cdots\ \&\ t_m \neq s_m)$$

and t is any element in the (infinite) set A which is distinct from $\pi(w_1), \dots,$ $\pi(w_m)$, then $\pi\{x := t\}$ satisfies the matrix of χ.

Case 2, $k > 0$, so there is an equation $x = z_i$ in the matrix of χ. In this case,

$$\chi \asymp (x = z_1\ \&\ \cdots\ \&\ x = z_k)\{x :\equiv z_i\}\ \&\ (u_1 = v_1\ \&\ \cdots u_l = v_l)$$
$$\&\ (x \neq w_1\ \&\ \cdots\ \&\ x \neq w_m)\{x :\equiv z_i\}\ \&\ (s_1 \neq t_1\ \&\ \cdots\ \&\ t_m \neq s_m)]$$

since every assignment which satisfies χ must assign to x the same value that it assigns to z_i. $\dashv$

This proposition is about a structure of no interest whatsoever, but the method of proof is typical of many quantifier elimination proofs.

Definition 1F.9 (Dense linear orderings)**.** A linear ordering $\mathbf{L} = (L, \leq)$ is *dense in itself* if for every $x, y \in L$ such that $x < y$, there is a z such that $x < z < y$.

Standard examples are the usual orderings $(\mathbb{Q}, \leq)$ and $(\mathbb{R}, \leq)$ on the rational and the real numbers. They also have no least or greatest element, and so they are covered by the next result.

Theorem 1F.10. *If* $\mathbf{L} = (L, \leq)$ *is a dense linear ordering without least or greatest element, then* $\mathbf{L}$ *admits effective quantifier elimination.*

Proof. It is convenient to introduce a new symbol $<$ for strict inequality, so that

(13) $$x \leq y \asymp_{\mathbf{L}} x = y \vee x < y, \qquad x < y \asymp_{\mathbf{L}} x \leq y\ \&\ x \neq y.$$

We can use the first of these equivalences to eliminate the symbol $\leq$, so that every formula is logically equivalent in $\mathbf{L}$ to one in which only the symbols $=$ and $<$ occur. In particular, the literals which occur in disjunctive normal forms of quantifier free formulas are all in one of the forms

$$x = y, \quad x \neq y, \quad x < y, \quad \neg(x < y)$$

We now replace all the negated literals by quantifier free formulas which have no negation, using the equivalences

$$\text{(14)} \quad x \neq y \asymp_{\mathbf{L}} x < y \vee y < x, \quad \neg(x \leq y) \asymp_{\mathbf{L}} y < x,$$
$$\neg(x < y) \asymp_{\mathbf{L}} x = y \vee y < x$$

and then we apply repeatedly the Distributive Laws in Proposition 1F.1 (which do not introduce negations) to construct a disjunctive normal form with only positive literals $x = y$ and $x < y$. This means that in applying the basic test Lemma 1F.7, we need consider only formulas of the form

$$\begin{aligned}\chi \equiv \exists x[&(x = z_1 \;\&\; \cdots \;\&\; x = z_k)\\ &\& \;(x < u_1 \;\&\; \cdots \;\&\; x < u_l) \;\&\; (v_1 < x \;\&\; \cdots \;\&\; v_m < x)\\ &\quad \& \;(s_1 < s_1' \;\&\; \cdots \;\&\; s_n < s_n') \;\&\; (t_1 = t_1' \;\&\; \cdots \;\&\; t_o = t_o')]\end{aligned}$$

If some $u_i \equiv x$ of some $v_j \equiv x$, then $\chi \asymp_{\mathbf{L}} F$, so we may assume that these variables are all distinct from x.

Case 1, $k > 0$, so that some equation $x = z_i$ is present in the matrix. Now χ is equivalent to the quantifier-free formula which is constructed by replacing x by z_i in the matrix.

Case 2, $k = l = m = 0$, so that x does not occur in the matrix of χ. We simply delete the quantifier.

Case 3, $k = l = 0$ but $m > 0$. In this case

$$\chi \asymp_{\mathbf{L}} (s_1 < s_1' \;\&\; \cdots \;\&\; s_n < s_n') \;\&\; (t_1 = t_1' \;\&\; \cdots \;\&\; t_o = t_o')]$$

because whatever values are assigned to $v_1, \ldots, v_m$ by an assignment, some greater value can be assigned to x since $\mathbf{L}$ has no largest element.

Case 4, $k = m = 0$ but $l > 0$. This case is symmetric to Case 3, and we handle it using the fact that $\mathbf{L}$ has no least element.

Case 5, $k = 0$ but $m > 0, l > 0$. Since $\mathbf{L}$ is dense in itself, the restrictions on x in the matrix will be satisfied by some x exactly when

$$\max\{v_1, \ldots, v_m\} < \min\{u_1, \ldots, u_l\},$$

and we can say this formally by a big conjunction: i.e.,

$$\begin{aligned}\chi \asymp_{\mathbf{L}} &\textstyle\bigwedge\!\!\!\bigwedge_{1 \leq i \leq l, 1 \leq j \leq m}(v_j < u_i)\\ &\quad \& \;(s_1 < s_1' \;\&\; \cdots \;\&\; s_n < s_n') \;\&\; (t_1 = t_1' \;\&\; \cdots \;\&\; t_o = t_o')\end{aligned}$$

This completes the verification of the test, Lemma 1F.7 for dense linear orderings with no first and last element, and so these structures admit effective quantifier elimination. ⊣

There are many interesting structures which admit effective quantifier elimination, including the following:

Example 1F.11. The reduct $(\mathbb{N}, 0, S)$ of $\mathbf{N}$ without addition or multiplication admits effective quantifier elimination, as does the somewhat richer structure $(\mathbb{N}, 0, S, <)$.

Example 1F.12 (Presburger arithmetic)**.** The reduct $(\mathbb{N}, 0, S, +)$ of $\mathbf{N}$ does not quite admit quantifier elimination, but something quite close to it does. Let

$$x \equiv_m y \iff m \text{ divides } y - x \quad (x \text{ is congruent to } y \text{ mod } m),$$

and consider the expansion of $(\mathbb{N}, 0, S, +)$ by these infinitely many relations,

$$\mathbf{N}_P = (\mathbb{N}, 0, S, +, \{\equiv_m\}_{m \in \mathbb{N}}).$$

This structure admits effective quantifier elimination and there is a trivial decision procedure for quantifier free sentences, which involve only numerals and congruence assertions about them; and so it is a decidable structure, and then the structure $(\mathbb{N}, 0, S, +)$ of additive arithmetic is also decidable, since it is a reduct of $\mathbf{N}_P$.

This is a famous and not so simple theorem of Presburger, Theorem 32E in Enderton.

Note that the expansion of the language by these congruence relations is quite similar to the expansion with T and F which we have already assumed, because we need it. The congruence relations are simply definable in additive arithmetic, one-at-a-time:

$$x \equiv_m y :\equiv (\exists z)[(x + \underbrace{z + z + \cdots + z}_{m \text{ times}} = y) \vee (y + \underbrace{z + z + \cdots + z}_{m \text{ times}} = x)].$$

The quantifier elimination in Presburger's structure $\mathbf{N}_P$ yields for each χ a quantifier-free formula in which these new, prime formulas $x \equiv_m y$ occur, for various values of m; we can then replace all of them with their definition, which gives us a formula χ^* which is $\asymp_{\mathbf{N}_P}$ with χ and in which existential quantifiers occur only in the "literals". This is exactly the sort of "extended quantifier-free" formulas that we will get if we replace T and F by their definitions after the quantifier elimination procedure has been completed.

Example 1F.13 (The field of complex numbers)**.** The field of complex numbers

$$\mathbf{C} = (\mathbb{C}, 0, 1, +, \cdot)$$

admits effective quantifier elimination, and so it is decidable, since the quantifier-free sentences in the language involve only trivial equalities and inequalities about numerals.

Example 1F.14 (The ordered field of real numbers)**.** The structure

$$\mathbf{R}_o = (\mathbb{R}, 0, 1, +, \cdot, \leq)$$

admits effective quantifier elimination, and so it is decidable, as above.

This is a famous theorem of Tarski, especially important because it establishes the decidability of classical (ancient) Euclidean plane and space geometry: it is easy to see that if we use Cartesian coordinates, we can translate all the elementary propositions studied in Euclidean geometry into sentences in the language of $\mathbf{R}_o$, and then decide them by Tarski's algorithm. Contrast this result with Example 1E.11: if we just add a name for the set of integers $\mathbb{Z}$ to the language, we get a structure which admits tuple coding, in whose language we can formalize all the propositions of classical analysis—including calculus.

Problem x1.30* proves that the *linear reduct* $(\mathbb{R}, 0, 1, + \leq)$ of $\mathbf{R}_o$ (without multiplication) admits effective quantifier elimination.

1G. Theories and elementary classes

Next we consider how formal, $\mathbb{FOL}$ sentences can be used to define properties of structures.

Definition 1G.1 (Elementary classes of structures)**.** A property Φ of τ-structures is **basic elementary** if there exists a sentence ϕ in $\mathbb{FOL}(\tau)$ such that for every τ-structure $\mathbf{A}$,

$$\mathbf{A} \text{ has property } \Phi \iff \mathbf{A} \models \phi,$$

and it is **elementary** if there exists a (possible infinite) set of sentences T such that

$$\mathbf{A} \text{ has property } \Phi \iff \text{for every } \phi \in T, \mathbf{A} \models \phi.$$

Basic elementary properties of τ-structures are (obviously) elementary, but not always vice versa.

Instead of a "property" of τ-structures, we often speak of a *class* (collection) of τ structures and formulate these conditions for classes, in the form

$$\begin{aligned} &\mathbf{A} \in \Phi \iff \mathbf{A} \models \phi && \text{(basic elementary class)} \\ &\mathbf{A} \in \Phi \iff \text{for every } \phi \in T, \mathbf{A} \models \phi && \text{(elementary class).} \end{aligned}$$

Notice that by Proposition 1C.3, basic elementary and elementary classes are closed under isomorphisms.

The basic use for these notions is in defining the following, fundamental concept of a (first order) theories and their models:

Definition 1G.2 (Theories and models)**.** A (formal) **theory** in a language $\mathbb{FOL}(\tau)$ is any (possibly infinite) set of sentences T of $\mathbb{FOL}(\tau)$. The members of T are its **axioms**.

A τ-structure $\mathbf{A}$ is a **model** of T if every sentence of T is true in $\mathbf{A}$: we write

$$\mathbf{A} \models T \iff_{\text{df}} \text{for all } \phi \in T,\ \mathbf{A} \models \phi, \tag{15}$$

and we collect all the models of T into a class,

$$\mathrm{Mod}(T) =_{\text{df}} \{\mathbf{A} \mid \mathbf{A} \models T\}. \tag{16}$$

Notice that $\mathrm{Mod}(T)$ is an elementary class of structures—and if T is finite, then $\mathrm{Mod}(T)$ is a basic elementary class, axiomatized by the conjunction of all the axioms in T.

In the opposite direction, the **theory of a τ-structure $\mathbf{A}$** is the set of all $\mathbb{FOL}(\tau)$-sentences that it satisfies,

$$\mathrm{Th}(\mathbf{A}) =_{\text{df}} \{\chi \mid \chi \text{ is a sentence and } \mathbf{A} \models \chi\}. \tag{17}$$

And finally,

$$T \models \chi \iff \text{for every } \mathbf{A},\ \text{if } \mathbf{A} \models T,\ \text{then } \mathbf{A} \models \chi. \tag{18}$$

This is the fundamental notion of **semantic consequence** (from an arbitrary set of hypotheses) for the language $\mathbb{FOL}$.

One of the basic problems in logic is the relation between a structure $\mathbf{A}$ and its theory $\mathrm{Th}(\mathbf{A})$: how much of $\mathbf{A}$ is captured by "all the first-order facts about $\mathbf{A}$" collected in $\mathrm{Th}(\mathbf{A})$?

Definition 1G.3 (Elementary equivalence)**.** Two τ-structures are **elementarily equivalent** if they satisfy the same $\mathbb{FOL}(\tau)$-sentences, in symbols

$$\mathbf{A} \equiv \mathbf{B} \iff_{\text{df}} \mathrm{Th}(\mathbf{A}) = \mathrm{Th}(\mathbf{B}). \tag{19}$$

As an immediate consequence of Proposition 1C.3 we get:

Proposition 1G.4. *Isomorphic structures are elementarily equivalent.*

We will see later that (somewhat surprisingly) the converse of this Proposition does not hold.

Axiomatic theories are useful, because they allow us to prove properties of many, related structures simultaneously, for all of them, by deriving them "from the axioms". We formulate here a few, basic theories we can use for examples later on.

Definition 1G.5 (Graphs)**.** The theory SG of *symmetric graphs* is formulated in the language $\mathbb{FOL}(E)$ with just one, binary relation symbol E and one axiom,

$$\forall x \forall y [R(x,y) \leftrightarrow R(y,x)].$$

The symmetric graphs then are exactly the models of SG.

Definition 1G.6 (Theories of order)**.** The theories of *partial* and *linear orderings* are also formulated in the language with vocabulary just one, binary relation symbol, which, however, we now denote as $\leq$:

$$\begin{aligned}
\mathsf{PO} &=_{\mathrm{df}} \{\forall x(x \leq x),\ \forall x \forall y[(x \leq y \ \&\ y \leq x) \to x = y], \\
&\qquad\qquad\qquad\qquad \forall x \forall y \forall z[(x \leq y \ \&\ y \leq z) \to x \leq z]\} \\
\mathsf{LO} &=_{\mathrm{df}} \mathsf{PO} \cup \{\forall x \forall y[x \leq y \vee y \leq x]\} \\
\mathsf{DLO} &=_{\mathrm{df}} \mathsf{LO} \cup \{\forall x \forall y[x < y \to \exists z(x < z \ \&\ z < y)] \\
&\qquad\qquad\qquad\qquad \forall x \exists y[x < y],\ \forall y \exists x[x < y]\}
\end{aligned}$$

The last of these is the theory of *dense linear orderings without first and last element*, and we have shown that every model of DLO admits effective quantifier elimination, Theorem 1F.10. The proof, actually, was *uniform*, and so it shows that *the theory* DLO admits effective quantifier elimination, in the following, precise sense.

Definition 1G.7 (Quantifier elimination for theories)**.** A theory T in the language $\mathbb{FOL}(\tau)$ **admits elimination of quantifiers**, if for every τ-formula χ, there is a quantifier-free formula χ^* (whose variables are all among the free variables of χ) such that

$$T \models \chi \leftrightarrow \chi^*.$$

As with structures, we assume here that the language is expanded by the prime, propositional constants T and F which may occur in χ^*.

Corollary 1G.8. *The theory* DLO *of dense linear orderings without first or last element admits effective quantifier elimination, and so it is decidable.*

Proof follows immediately from the proof of Theorem 1F.10, which produces the same quantifier-free form $\mathbf{L}$-equivalent to a given χ, independently of the specific $\mathbf{L}$, just so long as $\mathbf{L} \models \mathsf{DLO}$.

The second claim simply means that we can decide for any given sentence χ whether or not $\mathsf{DLO} \models \chi$. It is true because the quantifier elimination procedure yields either T or F as $\mathbf{L}$-equivalent to χ, independently of the specific $\mathbf{L}$. ⊣

Definition 1G.9 (Fields)**.** The theory Fields comprises the formal expressions of the axioms for a field listed in Definition 1A.4, in the language $\mathbb{FOL}(0, 1, +, \cdot)$.

For each number $n \geq 1$ define the term $n \cdot 1$ by the recursion

$$1 \cdot 1 \equiv 1, \quad (n+1) \cdot 1 \equiv (n \cdot 1) + (1),$$

so that e.g., $3 \cdot 1 \equiv ((1) + (1)) + (1)$. (Make sure you understand here what is a term of $\mathbb{FOL}(0, 1, +, \cdot)$, what is an ordinary number, and which $+$ is meant in the various places.)

For each prime number p, the finite set of sentences

$$\mathsf{Fields}_p =_{\mathrm{df}} \mathsf{Fields},\ \neg(2 \cdot 1 = 0),\ \dots, \neg((p-1) \cdot 1 = 0),\ p \cdot 1 = 0$$

is the theory of *fields of characteristic* p. The theory of *fields of characteristic* 0 is defined by

$$\mathsf{Fields}_0 =_{\mathrm{df}} \mathsf{Fields},\ \neg(2 \cdot 1 = 0),\ \neg(3 \cdot 1 = 0), \dots\ .$$

In describing sets of formulas we use "," to indicate union, i.e., in set notation,

$$\mathsf{Fields}_0 =_{\mathrm{df}} \mathsf{Fields} \cup \{\neg(2 \cdot 1 = 0),\ \neg(3 \cdot 1 = 0), \dots\ \}.$$

The simplest example of a field of characteristic p is the finite structure

$$\mathbb{Z}_p = (\{0, 1, \dots, p-1\}, 0, 1, +, \cdot)$$

with the usual operations on it executed *modulo* p, but it takes some (algebra) work to show that this is a field. There are many other fields of characteristic p, both finite and infinite.

The standard examples of fields of characteristic 0 are the rationals $\mathbf{Q}$; the reals $\mathbf{R}$; and the complex numbers $\mathbf{C}$.

For each $p \in \mathbb{N}$, Fields_p is a finite set of sentences, while Fields_0 is infinite.

Definition 1G.10 (Peano Arithmetic, PA)**.** The axioms of Peano arithmetic PA are the universal closures of the following formulas, in the language $\mathbb{FOL}(0, S, +, \cdot)$ of the structure of arithmetic (which we will call from now on the *language of Peano arithmetic*).

1. $\neg[S(x) = 0]$.
2. $S(x) = S(y) \rightarrow x = y$.
3. $x + 0 = x,\ x + S(y) = S(x + y)$.
4. $x \cdot 0 = 0,\ x \cdot (Sy) = x \cdot y + x$.
5. For every extended formula $\phi(x, \vec{y})$,

$$\Big[\phi(0, \vec{y})\ \&\ (\forall x)[\phi(x, \vec{y}) \rightarrow \phi(S(x), \vec{y})]\Big] \rightarrow (\forall x)\phi(x, \vec{y}).$$

The last is the **Elementary Axiom Scheme of Induction** which approximates in $\mathbb{FOL}$ the intended meaning of the full Axiom of Induction in §1. It has infinitely many *instances*, one for each extended formula $\phi(x, \vec{y})$.

The *standard* (intended) model of PA is, of course, **N**, but we will see that it has many others!

Definition 1G.11 (The Robinson system Q)**.** This is a weak, finite theory of natural numbers in the language of Peano arithmetic, which replaces the Induction Scheme by the single claim that each non-zero number is a successor:

1. $\neg[S(x) = 0]$.
2. $S(x) = S(y) \rightarrow x = y$.
3. $x + 0 = x,\ x + (S(y) = S(x + y)$.
4. $x \cdot 0 = 0,\ x \cdot (Sy) = x \cdot y + x$.
5. $x = 0 \vee (\exists y)[x = S(y)]$.

It is clear that **N** is a model of Q, but Q is a weak theory, and so it is quite easy to construct many, peculiar models of it.

Definition 1G.12 (Axiomatic Set Theories)**.** Of the nine (informal) axioms of Zermelo-Fraenkel Set Theory listed in Definition 1A.5, all but (5) (Subsets) and (8) (Replacement) are easily expressible in the language $\mathbb{FOL}(\in)$ of sets. As with Peano arithmetic, we can write down formal axiom schemes which approximate those two, as follows:

Axiom Scheme of Subsets: For each extended formula $\phi(u)$ in which the variable z does not occur free and $u \not\equiv x$, the universal closure of the following is an axiom:

$$(\exists z)(\forall u)[u \in z \leftrightarrow (u \in x \ \&\ \phi(u))].$$

Axiom Scheme of Replacement: For each extended formula $\phi(u, v)$ in which the variable z does not occur and $x \not\equiv u, v$, the universal closure of the following is an axiom:

$$(\forall u)(\exists! v)\phi(u, v) \rightarrow (\exists z)(\forall v)[v \in z \leftrightarrow (\exists u)[u \in x \ \&\ \phi(u, v)].$$

The theory ZC (Zermelo Set Theory with Choice) is the set of (formal) axioms (1) - (4), (6) - (7) and all the instances of the Axiom Scheme (5) of Subsets.

The theory ZFC (Zermelo-Fraenkel Set Theory with Choice) is the set of (formal) axioms (1) - (4), (6) - (7), (9) and all the instances of the Axiom Schemes (5) of Subsets and (8) Replacement.

The theories Z and ZF are obtained from these by deleting the Axiom of Choice (7).

1H. The Hilbert-style proof system for $\mathbb{FOL}$

In this Section we will introduce *formal* $\mathbb{FOL}$*-proofs* (from a theory T), and in the next we will prove that they suffice to establish all semantic consequences of T. This is the first fundamental result of logic.

1H.1. Axioms and rules of inference. The *axioms* (or *axioms schemes*) and *rules of inference* of $\mathbb{FOL}(\tau)$ are the following, subject to the indicated restrictions:

Logical axioms.

(1) $\phi \to (\psi \to \phi)$
(2) $(\phi \to \psi) \to ((\phi \to (\psi \to \chi)) \to (\phi \to \chi))$
(3) $(\phi \to \psi) \to ((\phi \to \neg\psi) \to \neg\phi)$
(4) $\neg\neg\phi \to \phi$
(5) $\phi \to (\psi \to (\phi \;\&\; \psi))$
(6a) $(\phi \;\&\; \psi) \to \phi$ (6b) $(\phi \;\&\; \psi) \to \psi$
(7a) $\phi \to (\phi \vee \psi)$ (7b) $\psi \to (\phi \vee \psi)$
(8) $(\phi \to \chi) \to ((\psi \to \chi) \to ((\phi \vee \psi) \to \chi))$
(9) $\forall v\phi(v) \to \phi(t)$ (t free for v in $\phi(v)$)
(10) $\forall v(\phi \to \psi) \to (\phi \to \forall v\psi)$ (v not free in ϕ)
(11) $\phi(t) \to \exists v\phi(v)$ (t free for v in $\phi(v)$)

Rules of inference:

(12) $\phi, \quad \phi \to \psi \Longrightarrow \psi$ (Modus Ponens)
(13) $\phi \Longrightarrow \forall v\phi$ (Generalization)
(14) $\phi \to \psi \Longrightarrow \exists v\phi \to \psi$ (v not free in ψ) (Exists elimination)

Axioms for identity. For every n-ary relation symbol R in τ and every n-ary function symbol f in τ:

(15) $v = v \quad v = v' \to v' = v \quad v = v' \to (v' = v'' \to (v = v''))$
(16) $(v_1 = w_1 \;\&\; \ldots v_n = w_n) \to (R(v_1, \ldots, v_n) \to R(w_1, \ldots, w_n))$
(R n-ary relation symbol)
(17) $(v_1 = w_1 \;\&\; \ldots v_n = w_n) \to (f(v_1, \ldots, v_n) = f(w_1, \ldots, w_n))$
(f n-ary function symbol)

The Hilbert system for $\mathbb{FOL}^-$ is obtained from this by allowing only $\mathbb{FOL}^-(\tau)$-formulas and omitting the axioms for identity. We will skip noting explicitly in the sequel these natural restrictions which must be made to the definitions to get the right notions for $\mathbb{FOL}^-$ from those for $\mathbb{FOL}$, on which we will concentrate.

Definition 1H.2. A **proof** or **deduction** in $\mathbb{FOL}$ from a set of formulas T is any sequence of formulas

$$\phi_0, \phi_1, \ldots, \phi_n,$$

where each ϕ_i is either an axiom, or a formula in T, or follows from previously listed formulas by one of the rules of inference. We set

$$T \vdash \phi \iff_{\text{df}} \text{there exists a deduction } \phi_0, \dots, \phi_n \equiv \phi.$$

If $T = \emptyset$ we just write $\vdash \phi$.

A deduction is **propositional** if the axioms 9-11 and the rules 13, 14 are not used in it, and we write

$$T \vdash_{\text{prop}} \phi \iff_{\text{df}} \text{there exists a propositional deduction of } \phi \text{ from } T.$$

(The formulas in a propositional deduction may have quantifiers in them.)

If T is a theory (a set of sentences) and $T \vdash \phi$ we call ϕ a proof-theoretic consequence or just a **theorem** of T. A **propositional theorem** of T is any formula ϕ for which there is a propositional deduction from T. The proof-theoretic consequences of the empty theory are the theorems of $\mathbb{FOL}$; the propositional theorems of $\mathbb{FOL}$ are called **tautologies**.

Two formulas ϕ and ψ are *proof-theoretically equivalent* if their bi-implication $\phi \leftrightarrow \psi$ is a theorem of $\mathbb{FOL}$. We write

$$\phi \asymp_p \psi \iff_{\text{df}} \vdash \phi \leftrightarrow \psi$$

Theorem 1H.3 (Soundness)**.** *Every theorem of a theory T is a semantic consequence of T, i.e.,*

$$\textit{if } T \vdash \phi, \textit{ then } T \models \phi.$$

Proof is easy, by induction on a given deduction of ϕ from T. ⊣

The main result in the next section is the converse of the Soundness Theorem, which (in particular) will identify the valid with the provable sentences. We will (obviously) need to show the existence of many formal proofs, and in doing this we will assume without comment the following two trivial facts:

(1) If $T \subseteq T'$, then every proof from T is also a proof from T', and
(2) the concatenation

$$\phi_0, \dots, \phi_n, \psi_0, \dots, \psi_k$$

of two proofs from T is also a proof from T.

Lemma 1H.4 (Constant Substitution)**.** *Suppose T is a theory, the variable v does not occur bound in the sequence of formulas $\phi_1(v), \dots, \phi_n(v)$ of $\mathbb{FOL}(\tau)$ and c is a* **fresh** *constant, i.e., a constant which does not occur in T or any of the formulas $\phi_1(v), \dots, \phi_n(v)$; then*

$$\phi_1(v), \dots, \phi_n(v) \textit{ is a deduction from } T \iff \phi_1(c), \dots, \phi_n(c) \textit{ is a deduction from } T.$$

Lemma 1H.5 (The Propositional Deduction Theorem). *For every set of formulas T and all formulas χ, ϕ,*

$$T, \chi \vdash_{\text{prop}} \phi \iff T \vdash_{\text{prop}} \chi \to \phi,$$

where the subscript indicates that the given and resulting deductions are propositional.

Theorem 1H.6 (The Deduction Theorem). *For every theory T, every sentence χ and every formula ϕ,*

$$T, \chi \vdash \phi \iff T \vdash \chi \to \phi.$$

Theorem 1H.7 (The natural introduction rules). *If T is a set of sentences, the indicated substitutions are free and the additional restrictions hold:*

($\to$) *If $T, \chi \vdash \phi$, then $T \vdash \chi \to \phi$.*
Restriction: χ must be a sentence.
(&) $\phi, \psi \vdash \phi \;\&\; \psi$.
($\vee$) $\phi \vdash \phi \vee \psi$, $\psi \vdash \phi \vee \psi$.
($\neg$) *If $T, \chi \vdash \psi$ and $T, \chi \vdash \neg\psi$, then $T \vdash \neg\chi$.*
Restriction: χ must be a sentence.
($\forall$) $\phi \vdash \forall v' \phi\{v :\equiv v'\}$.
($\exists$) $\phi\{v :\equiv t\} \vdash \exists v \phi$.

Theorem 1H.8 (The natural elimination rules). *If T is a set of sentences, the indicated substitutions are free and the additional restrictions hold:*

($\to$) $\phi, \phi \to \psi \vdash \psi$.
(&) $\phi \;\&\; \psi \vdash \phi$, $\phi \;\&\; \psi \vdash \psi$.
($\vee$) *If $T, \phi \vdash \chi$ and $T, \psi \vdash \chi$, then $T, \phi \vee \psi \vdash \chi$.*
Restriction: ϕ, ψ must be sentences.
($\neg$) $\neg\neg\phi \vdash \phi$.
($\forall$) $\forall v \phi \vdash \phi\{v :\equiv t\}$.
($\exists$) *If $T, \phi \vdash \chi$, then $T, \exists v \phi \vdash \chi$.*
Restriction: v does not occur free in χ, $\exists v \phi$ is a sentence, and the given proof has no bound occurrence of v.

We end the section with the definitions of three basic, proof-theoretic notions about theories:

Definition 1H.9. Suppose T is a τ-theory:

(1) T is **consistent** if it does not prove a contradiction, i.e., if there is no χ such that $T \vdash \chi \;\&\; \neg\chi$.
(2) T is **complete** if for each τ-sentence θ, either $T \vdash \theta$ or $T \vdash \neg\theta$.

(3) A τ'-theory T' is a **conservative extension** of T if $\tau \subseteq \tau'$ and for every τ-sentence θ,

$$T \vdash \theta \iff T' \vdash \theta.$$

Lemma 1H.10. (1) *A theory T is consistent if and only if there is some sentence χ such that $T \nvdash \chi$.*

(2) *A theory T is consistent if and only if every finite subset $T_0 \subseteq T$ is consistent.*

(3) *For any theory T and any sentence χ,*

$$T \vdash \chi \iff T \cup \{\neg\chi\} \text{ is inconsistent.}$$

(4) *If T is consistent, then for every sentence χ, either $T \cup \{\chi\}$ is consistent, or $T \cup \{\neg\chi\}$ is consistent.*

(5) *If $\exists v\phi(v)$ is a sentence, $T \cup \{\exists v\phi(v)\}$ is consistent and c is a constant which does not occur in T or in $\exists v\phi(v)$, then $T \cup \{\phi(c)\}$ is consistent.*

1I. The Completeness Theorem

In this section we will prove the basic result of First Order Logic:

Theorem 1I.1 (Gödel's Completeness Theorem)**.** (1) *Every consistent, countable theory T has a countable model.*

(2) *For every countable τ-theory T and every τ-sentence χ,*

$$\text{if } T \models \chi, \text{ then } T \vdash \chi. \tag{20}$$

Proof of the second claim from the first. Suppose $T \models \chi$ but $T \not\vdash \chi$; then $T \cup \{\neg\chi\}$ is consistent, and so it has a model $\mathbf{A}$ which is a model of T such that $\mathbf{A} \not\models \chi$, contradicting the hypothesis. ⊣

Thus the basic result is (1), but (2) has the more obvious foundational significance since with the Soundness Theorem 1H.3 it identifies *logical consequence* with *provability*,

$$T \models \chi \iff T \vdash \chi;$$

in fact, it is common to refer to either (1) or (2) as "*Gödel's Completeness Theorem*".

The key notion for the prof of (1) in the Completeness Theorem is the following:

Definition 1I.2 (Henkin sets)**.** A τ-theory H is a **Henkin set** if it satisfies the following conditions:

(H1) H is consistent.

(H2) For each τ-sentence χ, either $\chi \in H$ or $\neg\chi \in H$, and in particular, H is complete.

(H3) If $\exists v\phi(v) \in H$, then there is some constant c such that $\phi(c) \in H$.

The constant c in the last condition is called a **Henkin witness** for the existential sentence $\exists v\phi(v)$, so (briefly) a Henkin set is a consistent, (strongly) complete theory which has Henkin witnesses.

Lemma 1I.3 (Properties of Henkin sets)**.** *Suppose H is a Henkin set.*

(1) *H is deductively closed, i.e., for every sentence χ,*

$$\text{if } H \vdash \chi, \text{ then } \chi \in H.$$

(2) *For all sentences $\phi, \psi, \exists v\phi(v)$:*

$$\begin{aligned}
\neg\phi \in H &\iff \phi \notin H\\
\phi \,\&\, \psi \in H &\iff \phi \in H \text{ and } \psi \in H\\
\phi \vee \psi \in H &\iff \phi \in H \text{ or } \psi \in H\\
\phi \rightarrow \psi \in H &\iff \phi \notin H \text{ or } \psi \in H\\
\exists v\phi(v) \in H &\iff \text{ there is some } c \text{ such that } \phi(c) \in H\\
\forall v\phi(v) \in H &\iff \text{ for all } c,\ \phi(c) \in H
\end{aligned}$$

Proof. (1) Suppose $H \vdash \chi$ but $\chi \notin H$; then $\neg\chi \in H$ by (H2), and so $H \vdash \neg\chi$, which makes H inconsistent contradicting property (H1).

(2) We consider just two of these equivalences.

If $\phi \,\&\, \psi \in H$, then $\phi, \psi \in H$ by the deductive completeness of H, since $\phi \,\&\, \psi \vdash \phi$ and $\phi \,\&\, \psi \vdash \psi$; and for the converse of this, we use the fact that $\phi, \psi \vdash \phi \,\&\, \psi$, so that if $\phi, \psi \in H$, then $H \vdash \phi \,\&\, \psi$ and so $\phi \,\&\, \psi \in H$.

If $\exists v\phi(v) \in H$, then $\phi(c) \in H$ for some c, by the key property (H3). The converse holds because $\phi(c) \vdash \exists v\phi(v)$ and H is deductively complete. ⊣

The lemma suggests that every Henkin set is $\mathrm{Th}(\mathbf{A})$ for some structure $\mathbf{A}$, and so to construct a model of some consistent theory T we should aim to construct a Henkin set which extends T; to do this, however, we will need to expand the signature of the language (to introduce enough constants which can serve as Henkin witnesses), and this expansion is the main trick needed for the proof of the Completeness Theorem.

Lemma 1I.4. *If τ is a countable signature, then every consistent τ-theory T is contained in a Henkin set $H \supseteq T$ of $\mathbb{FOL}(\overline{\tau})$, where the vocabulary $\overline{\tau}$ is an expansion of τ by an infinite sequence of fresh constants $(d_0, d_1, \dots)$, i.e.,*

(21) $\quad$ *if* $\tau = (\mathrm{Const}, \mathrm{Rel}, \mathrm{Funct}, \mathrm{arity})$,

$$\textit{then } \overline{\tau} = (\mathrm{Const} \cup \{d_0, d_1, \dots\}, \mathrm{Rel}, \mathrm{Funct}, \mathrm{arity}).$$

Proof. Fix an enumeration

$$S = \{=, s_1, \dots\}$$

of all the constants, relation and function symbols of τ, including the identity symbol (which we put first), and say that a symbol s has *order* n if it occurs in $\{s_0, \dots, s_n\}$; so $=$ is the only symbol of order 0.

Sublemma 1. There is an enumeration

$$\chi_0, \chi_1, \dots$$

of all $\mathbb{FOL}(\overline{\tau})$ *sentences, such that for each* n*, the constant* d_n *does not occur in any of the first* n *sentences* $\chi_0, \dots, \chi_{n-1}$.

Proof. For each $n = 0, 1, \dots$, let

$$\begin{aligned} S_n = {} & \text{the set of all sentences of } \mathbb{FOL}(\overline{\tau}) \text{ of length} \le 5 + n \\ & \text{whose variables are in } \{v_0, \dots, v_n\}, \text{ and in which} \\ & \text{only } \tau\text{-constants of order } n \text{ and only} \\ & d_0, \dots, d_{n-1} \text{ of the fresh constants may occur.} \end{aligned}$$

The choice of 5 in this definition insures that S_0 is not empty, since

$$\exists v_0 v_0 = v_0 \in S_0.$$

At the same time, easily:

1. Each S_n is finite.
2. $S_n \subseteq S_{n+1}$, for each n.
3. d_0 does not occur in any sentence in S_0, and for $n > 0$, d_n does not occur in any sentence of S_{n-1}.

We now enumerate in some standard way all these finite sets,

$$S_n = (\chi_0^n, \dots, \chi_{k_n}^n),$$

and conclude that the required enumeration of all the $\mathbb{FOL}(\overline{\tau})$- sentences is the "concatenation" of all these enumerations,

$$\chi_0^0, \dots, \chi_{k_0}^0, \chi_0^1, \dots, \chi_{k_1}^1, \dots . \qquad \dashv \text{ (Sublemma 1)}$$

Sublemma 2. There exists a sequence

$$\phi_0, \phi_1, \dots, \tag{22}$$

of $\mathbb{FOL}(\overline{\tau})$*-sentences with the following properties:*

1. *For each* n*,* $\phi_{2n} \equiv \chi_n$ *or* $\phi_{2n} \equiv \neg\chi_n$.
2. *For each* n*, if* $\phi_{2n} \equiv \exists v \psi(v)$ *for some variable* v *and full extended formula* $\psi(v)$*, then* $\phi_{2n+1} \equiv \psi(d_n)$*, otherwise* $\phi_{2n+1} \equiv \phi_{2n}$.
3. *For each* n*, the set* $T \cup \{\phi_0, \dots, \phi_{2n+1}\}$ *is consistent.*

Proof. The sentences ϕ_{2n}, ϕ_{2n+1} are defined by recursion on n, using Lemma 1H.10—and their definition is basically determined by the conditions they are required to satisfy. $\dashv$ (Sublemma 2)

It is now easy to verify that the range $H = \{\phi_0, \phi_1, \dots, \}$ of the sequence of sentences in (22) constructed in the proof of Sublemma 2 is a Henkin set.

To see that it includes T, suppose $\chi \in T$. Now $\chi \equiv \chi_n$ for some n, and so either $\phi_{2n} \equiv \chi$ or $\phi_{2n} \equiv \neg\chi$; but $T \cup \{\phi_0, \dots, \phi_{2n+1}\}$ is consistent, and so it cannot contain both χ and $\neg\chi$—so it must be that $\phi_{2n} \equiv \chi$. $\dashv$

Recall that a binary relation $\sim$ on a set C is an **equivalence relation**, if for all $x, y, z \in C$,

$$x \sim x, \quad x \sim y \Longrightarrow y \sim x, \quad [x \sim y \ \&\ y \sim z] \Longrightarrow x \sim z. \tag{23}$$

In the next, main lemma we will appeal to the basic characterization of equivalence relations in Problem x6.8.

Lemma 1I.5. *If $\overline{\tau} = (C, \mathrm{Rel}, \mathrm{Funct}, \mathrm{arity})$ is a countable signature and H is a Henkin set in the language $\mathbb{FOL}(\overline{\tau})$, then there exists a countable $\overline{\tau}$-structure $\overline{\mathbf{C}}$ such that for every $\overline{\tau}$-sentence χ,*

$$\overline{\mathbf{C}} \models \chi \iff \chi \in H. \tag{24}$$

Proof. Let C be the (countable) set of all the constants in the signature $\overline{\tau}$. Lemma 1I.3 suggests that we can construct a model $\mathbf{C}$ of H on the universe C by setting for $e_1, \dots, e_n, e \in C$,

$$R^{\mathbf{C}}(e_1, \dots, e_n) \iff R(e_1, \dots, e_n) \in H,$$
$$f^{\mathbf{C}}(e_1, \dots, e_n) = e \iff f(e_1, \dots, e_n) = e \in H,$$

and this almost works, except that it gives "multiple valued" interpretations of the constants: it may well be that $e = e' \in H$, while e and e' are distinct constants. To deal with this, we need to "identify" constants which H thinks that they are equal, as follows. We set:

$$a \sim b \iff (a = b) \in H \qquad (a, b \in C).$$

Sublemma 1. The relation $\sim$ is an equivalence relation on the set C of constants of $\overline{\tau}$.

Proof is immediate from (15) of the Axioms of Identity of the Hilbert system, which are satisfied by H, since it is deductively closed. For example, $(a = a) \in H$ for every constant a, because $\vdash a = a$. $\dashv$ (Sublemma 1)

We fix a quotient $\overline{C}$ and a determinism homomorphism $\rho : C \twoheadrightarrow \overline{C}$ of $\sim$, so that (with $\overline{a} = \rho(a)$, to simplify notation),

$$(a = b) \in H \iff \overline{a} = \overline{b} \qquad (a, b \in C). \tag{25}$$

Sublemma 2. For each n-ary relation symbol R, there is an n-ary relation $\overline{R}$ on $\overline{C}$ such that for all $a_1, \dots, a_n \in C$,

$$\overline{R}(\overline{a}_1, \dots, \overline{a}_n) \iff R(a_1, \dots, a_n) \in H. \tag{26}$$

Proof. By (16) of the Axioms of Identity, for any constants $a_1, \ldots, a_n$, $b_1, \ldots, b_n$,

$$\vdash [a_1 = b_1 \ \& \ \cdots \ \& \ a_n = b_n] \rightarrow \Big(R(a_1, \ldots, a_n) \leftrightarrow R(b_1, \ldots, b_n)\Big);$$

thus this sentence is in H, sine H is deductively closed, and then Lemma 1I.3 implies easily that

$$(\overline{a}_1 = \overline{b}_1, \ldots, \overline{a}_n = \overline{b}_n) \Longrightarrow \Big(R(a_1, \ldots, a_n) \in H \iff R(b_1, \ldots, b_n) \in H\Big).$$

We can thus insure (26) by setting

$$R(u_1, \ldots, u_n) \iff R(a_1, \ldots, a_n) \in H,$$

where $a_1, \ldots, a_n$ are any constants such that $\overline{a}_1 = u_1, \ldots, \overline{a}_n = u_n$—any other choice of $a_1, \ldots, a_n$ would give the same truth value to $R(u_1, \ldots, u_n)$. ⊣ (Sublemma 2)

Sublemma 3. For each closed term t, there is a constant c such that

$$(t = c) \in H;$$

and for any two constants c, d,

$$(t = c) \in H \iff (t = d) \in H.$$

Proof. For the first claim, notice that for every term t, $\vdash \exists v(t = v)$ by the proof

$$v = v,\ \forall v(v = v),\ \forall v(v = v) \rightarrow t = t,$$
$$t = t,\ t = t \rightarrow \exists v(t = v),\ \exists v(t = v)$$

where the next-to-the-last inference is by Rule (11), setting $\phi(v) \equiv t = v$. Thus $\exists v(t = v) \in H$ if t is closed, and the Henkin property supplies us with a witness c such that $(t = c) \in H$.

The second claim follows again by the deductive closure of H and Lemma 1I.3, because $\vdash (t = c \ \& \ t = d) \rightarrow c = d$. ⊣ (Sublemma 3)

Sublemma 4. For every n-ary function symbol f, there is an n-ary function $\overline{f} : \overline{C}^n \rightarrow \overline{C}$ such that for all constants $a_1, \ldots, a_n, c$,

$$\overline{f}(\overline{a}_1, \ldots, \overline{a}_n) = \overline{c} \iff (f(a_1, \ldots, a_n) = c) \in H. \tag{27}$$

Proof. By Sublemma 3, for any $a_1, \ldots, a_n$ there is some c such that $(f(a_1, \ldots, a_n) = c) \in H$; we then define $\overline{f}$ by

$$\overline{f}(u_1, \ldots, u_n) = \overline{c}$$

for any $a_1, \ldots, a_n$ such that $u_1 = \overline{a}_1, \ldots, u_n = \overline{a}_n$, and show (as in Sublemma 2) that all such choice of $a_1, \ldots, a_n$ and c give the same value for $\overline{f}(u_1, \ldots, u_n)$. ⊣ (Sublemma 4)

The structure we need is

$$\overline{\mathbf{C}} = (\overline{C}, \{\overline{c}\}_{c\in C}, \{\overline{R}\}_{R\in\mathrm{Rel}}, \{\overline{f}\}_{f\in\mathrm{Funct}}).$$

Sublemma 5. For every closed term t, there is a constant c such that

$$(t = c) \in H \text{ and } \mathrm{value}^{\overline{\mathbf{C}}}(t) = \overline{c}.$$

Proof is by structural induction on t, using (27). ⊣ (Sublemma 5)

Proof of (24) is by structural induction on the sentence χ, and it is enough to check the Basis (for prime formulas), since (24) for non-prime formulas then follows immediately by Lemma 1I.3.

If $\chi \equiv s = t$, then by Sublemma 5, there are constants a, b such that

$$(t = a) \in H, \quad \mathrm{value}^{\overline{\mathbf{C}}}(t) = \overline{a}, \quad (s = b) \in H, \quad \mathrm{value}^{\overline{\mathbf{C}}}(s) = \overline{b}.$$

Thus

$$\overline{\mathbf{C}} \models s = t \iff \overline{a} = \overline{b} \quad (\iff (a = b) \in H),$$

and the consistency and deductive closure of H imply that

$$(a = b) \in H \iff (s = t) \in H,$$

as required.
The argument is similar for the case $\chi \equiv R(t_1, \dots, t_n)$. ⊣

Proof of the Completeness Theorem 1I.1. Fix a consistent τ-theory T (with countable τ), let H be the Henkin set guaranteed by Lemma 1I.4 for the expanded signature $\overline{\tau}$ with constants

$$C = \mathrm{Const} \cup \{d_0, d_1, \dots, \};$$

and let

$$\overline{\mathbf{A}} = (\overline{A}, \{\overline{c}\}_{c\in\mathrm{Const}}, \{\overline{d}_0, \overline{d}_1, \dots, \}, \{\overline{R}\}_{R\in\mathrm{Rel}}, \{\overline{f}\}_{f\in\mathrm{Funct}})$$

be the $\overline{\tau}$-structure guaranteed by Lemma 1I.5 for this H; the τ-structure we need is the reduct

$$\mathbf{A} = (\overline{A}, \{\overline{c}\}_{c\in\mathrm{Const}}, \{\overline{R}\}_{R\in\mathrm{Rel}}, \{\overline{f}\}_{f\in\mathrm{Funct}})$$

which does not interpret the constants $d_0, d_1, \dots$. (Notice, however, that $\overline{d}_0, \overline{d}_1, \dots$ are elements of the universe $\overline{A}$ of the structure $\mathbf{A}$.) ⊣

The Completeness Theorem identifies *logical* (but possibly accidental) *truth* with *justified truth*, and its foundational significance can hardly be overestimated. It also has a large number of mathematical applications.

1J. The Compactness and Skolem-Löwenheim Theorems

We derive here two simple but rich in consequences corollaries of the Completeness Theorem which do not refer directly to *provability*.

Theorem 1J.1 (Compactness Theorem)**.** *If every finite subset of a countable theory T has a model, then T has a* (countable) *model.*

Proof. By the hypothesis, every finite subset of T is consistent; hence T is consistent, and it has a model by the Completeness Theorem. ⊣

We will consider many applications of the Compactness Theorem in the problems, but the following, basic fact gives an idea of how it can be applied:

Corollary 1J.2. *If a countable theory T has arbitrarily large finite models, then it has an infinite model.*

Proof. For each n, let

$$\theta_n = \exists v_0 \cdots \exists v_n \bigwedge\!\!\!\bigwedge_{i,j \leq n, i \neq j} [v_i \neq v_j]$$

be a sentence which asserts that there are at least $n+1$ objects, and set

$$T^* = T \cup \{\theta_0, \theta_1, \dots\};$$

now every finite subset of T^* has a model, by the hypothesis, and so by the Compactness Theorem, T^* has a model—which is an infinite model of T.⊣

Theorem 1J.3 (Weak Skolem-Löwenheim Theorem)**.** *If a countable theory T has a model, then it has a countable model.*

Proof. Again, the hypothesis gives us that T is consistent, and then the Completeness Theorem provides us with a countable model of T. ⊣

The Skolem-Löwenheim Theorem yields a spectacular consequence if we apply it to Zermelo-Fraenkel Set Theory ZFC, the formal version of the axioms for sets we described in Definition 1A.5: ZFC proves that *there exist uncountable sets*, but since it is (we hope!) consistent, it can be interpreted in a countable universe! There is no formal contradiction in this *Skolem Paradox* (think it through), but it sounds funny, and it has provoked tons of philosophical research—not all of it as useless as these dismissive remarks might imply.

Definition 1J.4. A **non-standard model of Peano arithmetic** is any model of PA which is not isomorphic with the standard model $\mathbf{N}$. A non-standard **model of true arithmetic** is any τ_a-structure $\mathbf{N}^*$ which is elementarily equivalent with the standard structure $\mathbf{N}$, but is not isomorphic with $\mathbf{N}$.

Every non-standard model of true arithmetic is a non-standard model of PA, but (as we will see) not vice versa.

Theorem 1J.5. *There exist non-standard models of true arithmetic.*

Proof. We define the function $n \mapsto \Delta(n)$ from natural numbers to terms of the language of arithmetic by the recursion,

$$\Delta(0) \equiv 0, \quad \Delta(n+1) \equiv S(\Delta(n)), \tag{28}$$

so that $\Delta(1) \equiv S(0)$, $\Delta(2) \equiv S(S(0))$, etc. These **numerals** are the standard (unary) names of numbers in the language of PA.

Let $\tau(c) = (0, c, S, +, \cdot)$ be the expansion of the vocabulary of Peano arithmetic by a new constant c, and let

$$T(c) = \mathrm{Th}(\mathbf{N}) \cup \{c \neq \Delta(0), c \neq \Delta(1), \dots\}. \tag{29}$$

Every finite subset T_0 of $T(c)$ contains only finitely many sentences of the form $c \neq \Delta(i)$, and so it has a model, namely the expansion $(\mathbf{N}, m)$ for any sufficiently large m; so $T(c)$ has a model

$$\mathbf{A} = (A, \overline{0}, \overline{c}, \overline{S}, \overline{+}, \overline{\cdot})$$

which satisfies all the sentences in the language of arithmetic which are true in $\mathbf{N}$ since $\mathrm{Th}(\mathbf{N}) \subseteq T(c)$, and so its reduct

$$\mathbf{N}^* = (A, \overline{0}, \overline{S}, \overline{+}, \overline{\cdot}) \tag{30}$$

also satisfies all the true sentences of arithmetic. But $\mathbf{N}^*$ is not isomorphic with $\mathbf{N}$: because if $\rho : \mathbb{N} \rightarrowtail\!\!\!\!\!\twoheadrightarrow A$ were an isomorphism, then (easily)

$$\rho(n) = \Delta(n)^{\mathbf{A}},$$

and the interpretations of the numerals do not exhaust the universe A, since $\mathbf{A} \models c \neq \Delta(n)$ for every n and so $\overline{c} \notin \rho[\mathbb{N}]$. $\dashv$

1J.6. Remark. The assumption that T is countable is not needed for the results of this section (other than Corollary 1J.3), but the proofs for arbitrary theories require some cardinal arithmetic, including (for some of them) the full Axiom of Choice).

1K. Some other languages

We end this introductory chapter by introducing some simple languages other than $\mathbb{FOL}$ which also carry a useful theory of syntax and semantics.

1K.1. The propositional calculus. We have an infinite list of *propositional variables* $\mathrm{p}_0, \mathrm{p}_1, \dots$ Formulas are defined recursively by: (1) Each variable p is a formula. (2) If ϕ, ψ are formulas, so are

$$\neg(\phi) \quad (\phi) \rightarrow (\psi) \quad (\phi)\ \&\ (\psi) \quad (\phi) \vee (\psi)$$

An *assignment* is a function π : variables $\rightarrow \{0, 1\}$ and it extends to a function value(ϕ, π) on the formulas as in the case of $\mathbb{FOL}$. a propositional formula is a **tautology** if it is assigned the value 1 by all assignments. The axiom schemata are (1)-(9) of the full system and the only rule of inference is Modus Ponens.

1K.2. Equational logic. If a signature τ has no relation symbols, we call it an *algebra vocabulary*, and we call the τ-structures *algebras*. The formulas of **equational logic** for an algebra signature are the simple identities

$$s = t$$

where s and t are terms. An algebra satisfies $s = t$ if it satisfies it as an *identity*, i.e., if it satisfies its universal closure. The rules of inference of equational logic are:

$$\Longrightarrow s = s, \quad s = t \Longrightarrow t = s, \quad s = s',\ s' = s'' \Longrightarrow s = s''$$
$$s_1 = t_1, \dots, s_n = t_n \Longrightarrow f(s_1, \dots, s_n) = f(t_1, \dots, t_n)$$
$$t_1(v) = t_2(v) \Longrightarrow t_1(s) = t_2(s)$$

where in the last rule, $t_1(v), t_2(v)$ are terms in which v (among other variables) may occur. (The first of these is really an **axiom scheme**: it declares that $s = s$ can be deduced from no hypotheses.)

An **equational theory** is a set of *identities* in some algebra vocabulary.

1K.3. Second order logic. The language $\mathbb{FOL}^2$ of second order logic is the extension of $\mathbb{FOL}$ that we get if we add for each n an infinite list of n-ary *relation variables*

$$\mathsf{X}_0^n, \mathsf{X}_1^n, \dots .$$

In the formation rules for terms and formulas we treat these new variables as if they were relation constants in the vocabulary, so that $\mathsf{X}_i^n(t_1, \dots, t_n)$ is well formed, and we also add to the formation rules for formulas the clauses

$$\phi \mapsto \forall X \phi \quad \phi \mapsto \exists X \phi$$

which introduce quantification over the relation variables. A formula is $\forall_1^1$ if it is of the form

$$\forall X_1 \forall X_2 \cdots \forall X_n \phi$$

where $X_1, \dots, X_n$ are relation variables (of any arity) and ϕ is **elementary**, i.e., it has no relation quantifiers; a formula is $\exists_1^1$ if it is of the corresponding form, with $\exists$'s rather than $\forall$'s.

The language $\mathbb{FOL}^2(\tau)$ is interpreted in the same τ-structures as $\mathbb{FOL}(\tau)$. An assignment into a structure $\mathbf{A}$ is a function π which assigns to each individual variable v a member of A and to each n-ary relation variable X

an n-ary relation over A. The satisfaction relation for $\mathbb{FOL}^2$ is the natural extension of its version for $\mathbb{FOL}$ with the clauses

$$\begin{aligned}\mathrm{value}(\forall X\phi,\pi) &= \min\{\mathrm{value}(\phi,\pi\{X := R\}) \mid R \subseteq A^n\},\\ \mathrm{value}(\exists X\phi,\pi) &= \max\{\mathrm{value}(\phi,\pi\{X := R\}) \mid R \subseteq A^n\},\end{aligned}$$

for the quantifiers over n-ary relations, and they lead to the obvious extensions of the Tarski conditions 1C.9:

$$\begin{aligned}\mathbf{A},\pi \models \forall X\phi &\iff \text{for all } R \subseteq A^n, \mathbf{A},\pi\{X := R\} \models \phi,\\ \mathbf{A},\pi \models \exists X\phi &\iff \text{for some } R \subseteq A^n, \mathbf{A},\pi\{X := R\} \models \phi.\end{aligned}$$

Extended and *full extended* formulas of $\mathbb{FOL}^2$ are defined as for $\mathbb{FOL}$, and a relation $P(x_1,\dots,x_n,P_1,\dots,P_m$ with individual and relation arguments is **second order definable** in a structure $\mathbf{A}$, if there is a full extended $\mathbb{FOL}^2$-formula $\chi(v_1,\dots,v_n,X_1,\dots,X_m)$ such that for all $x_1,\dots,x_n$ in A and all relations $R_1,\dots,R_m$ (of appropriate arities) on A,

$$\begin{aligned}P(\vec{x},\vec{R}) &\iff \mathbf{A} \models \chi[\vec{x},\vec{R}]\\ &\iff \text{for some (and so all) assignments } \pi,\\ &\qquad\qquad \mathbf{A},\pi\{\vec{v} := \vec{x}, \vec{X} := \vec{R}\} \models \chi;\end{aligned}$$

P is $\forall^1_1$ or $\exists^1_1$ if χ can be taken to be $\forall^1_1$ or $\exists^1_1$ respectively.

There is no useful proof theory for second order logic, but many natural, non-elementary relations on structures are second-order definable, and so $\mathbb{FOL}^2$ is a good tool in *definability theory.*

1L. Problems for Chapter 1

Problem x1.1. Prove Proposition 1B.4 (parsing for terms). Hint: Show first that no term is a proper initial segment of another term.

Problem x1.2. Prove Proposition 1B.5 (parsing for formulas).
Hint: Show first the number of left parentheses matches the number of right parentheses in a formula; that if ϕ is a formula and $\alpha \sqsubseteq \phi$, then the number of left parentheses in α is greater than or equal to the number of right parentheses in α; and that no formula is a proper, initial segment of another.

Problem x1.3. Fix a τ-structure $\mathbf{A}$.

(x1.3.1) Prove that if a term t is free for the variable v in an expression α, then for every assignment π to $\mathbf{A}$,

$$\mathrm{value}(\alpha\{v :\equiv t\},\pi) = \mathrm{value}(\alpha,\pi\{v := \mathrm{value}(t,\pi)\}).$$

(x1.3.2) Give an example of two formulas ϕ and ψ in the language of arithmetic, an assignment π into $\mathbf{N}$, and a closed term t, such that

$$\mathbf{N}, \pi \models (\phi \leftrightarrow \psi), \text{ but } \mathbf{N}, \pi \not\models \phi\{v :\equiv t\} \leftrightarrow \psi\{v :\equiv t\}.$$

(x1.3.3) Prove that

$$\text{if } \models (\phi \leftrightarrow \psi), \text{ then } \models \phi\{v :\equiv t\} \leftrightarrow \psi\{v :\equiv t\}.$$

(Logical equivalence is preserved by free substitutions.)

Problem x1.4. Prove Proposition 1C.3.

Problem x1.5. The structures $\mathbf{N}$ of arithmetic and $\mathbf{Q}$ of fractions are rigid.

Problem x1.6. The structure $(\mathbb{R}, \leq)$ is *homogeneous*, in the following sense: if $(a_1, \dots, a_n)$, $(b_1, \dots, b_n)$ are sequences of real numbers such that

$$a_i < a_j \iff b_i < b_j,$$

then there is an automorphism $\rho : (\mathbb{R}, \leq) \rightarrowtail\!\!\!\!\twoheadrightarrow (\mathbb{R}, \leq)$ such that for $i = 1, \dots, n$, $\rho(a_i) = b_i$. (Do it first for $n = 1$ to see what is going on.)

Show also that the structure $(\mathbb{Q}, \leq)$ is homogeneous.

Problem x1.7. Prove that if a binary relation $P(x, y)$ is elementary in a structure $\mathbf{A}$, then so is the converse relation

$$\breve{P}(x, y) \iff P(y, x).$$

Problem x1.8. Prove that if $f(\vec{x}), g(\vec{x})$ are elementary functions in a structure $\mathbf{A}$, then so is the relation

$$P(\vec{x}) \iff f(\vec{x}) = g(\vec{x}).$$

Problem x1.9. Show by examples that (4) does not necessarily hold for all $\mathbb{FOL}^-(\tau)$-sentences unless $\rho : \mathbf{A} \to \mathbf{B}$ is both strong and surjective; and it does not necessarily hold for all $\mathbb{FOL}(\tau)$-sentences unless $\rho : \mathbf{A} \to \mathbf{B}$ is an isomorphism.

Problem x1.10. Prove part (3) of Theorem 1D.2, i.e., that the collection of $\mathbf{A}$-elementary functions is closed under composition.

Problem x1.11. Prove the last claim of Theorem 1D.2, that $\mathcal{E}(\mathbf{A})$ is the smallest collection of functions and relations which satisfies (1) – (5) of the theorem.

In the next few problems you are asked to decide whether a given relation is elementary or not on a given structure, and to provide a full extended formula which defines it if your answer is "yes". You will not be able to prove all your negative answers, as we have not developed yet enough tools for proving non-elementarity—Proposition 1C.3 is the only result that you can appeal to; but you should try to guess the correct answers.

Problem x1.12. Determine whether the following relations are elementary on the structure $(\mathbb{R}, \leq)$.

1. $P_1(x) \iff x > 0$.
2. $P_1(x, y, z) \iff z = \max(x, y)$
3. $P_3(x, y, z) \iff x < y < z \;\&\; z - y = y - x$

Problem x1.13. Determine whether the following relations are elementary on a fixed, symmetric graph $\mathbf{G} = (G, E)$, and if your answer is positive, find a full extended formula which defines them.

1. $P(x, y) \iff d(x, y) \leq 2$.
2. $P(x, y) \iff d(x, y) = 2$.
3. $P(x, y, z) \iff d(x, y) \leq d(x, z)$
4. $P(x, y) \iff d(x, y) < \infty$.
5. $P(x) \iff$ every y can be joined to x.

Problem x1.14. Determine whether the following relations are arithmetical, and if your answer is positive, find a full extended formula which defines them.

1. $\mathrm{Prime}(x) \iff x$ is a prime number.
2. $\mathrm{TP}(x) \iff$ there are infinitely many twin primes y such that $x \leq y$.
3. $\mathrm{P}(n) \iff$ there exist infinitely many pairs of numbers (x, y) such that $Q(n, x, y)$, where $Q(n, x, y)$ is a given arithmetical relation.
4. $\mathrm{Quot}(x, y, w) \iff \mathrm{quot}(x, y) = w$
5. $\mathrm{Rem}(x, y, w) \iff \mathrm{rem}(x, y) = w$.
6. $x \perp y \iff x$ and y are coprime (i.e., no number other than 1 divides both x and y).

Problem x1.15. Prove that the following functions and relations on $\mathbb{N}$ are arithmetical.

1. $p(i) = p_i =$ the i'th prime number, so that $p_0 = 2, p_1 = 3, p_2 = 5$, etc.
2. $f_n(x_0, \dots, x_n) = p_0^{x_0+1} \cdot p_1^{x_1+1} \cdots p_{n-1}^{x_n+1}$. (This is a different function of $n+1$ arguments for each n.)
3. $R(u) \iff$ there exists some n and some $x_1, \dots, x_n$ such that $u = f_n(x_1, \dots, x_n)$.

Problem x1.16 (The Ackermann function)**.**
(x1.16.1) Prove that there is a function $A : \mathbb{N}^2 \to \mathbb{N}$ which satisfies the following identities:

$$A(0, x) = x + 1$$
$$A(n + 1, 0) = A(n, 1)$$
$$A(n + 1, x + 1) = A(n, A(n + 1, x))$$

(This is a definition by *double recursion*.)

(x1.16.2) Compute $A(1,2)$ and $A(2,1)$.

Problem x1.17*. Prove that the Ackermann function defined in Problem x1.16 is arithmetical.

Problem x1.18. Determine whether the (usual) ordering relation on real numbers is elementary on the field $\mathbf{R} = (\mathbb{R}, 0, 1, +, \cdot)$, and if your answer is positive, find a formula which defines them.

Problem x1.19. Prove that the ring of integers $\mathbf{Z} = (\mathbb{Z}, 0, 1, +, \cdot)$ admits tuple coding.

The difficulty in proving Julia Robinson's Theorem 1E.10 lies in showing that the set $\mathbb{N} \subseteq \mathbb{Q}$ is elementary in the structure $\mathbf{Q}$; if we make this part of the hypothesis, then the rest is quite routine:

Problem x1.20. Prove that the structure $(\mathbf{Q}, \mathbb{N}) = (\mathbb{Q}, 0, 1, \mathbb{N}, +, \cdot)$ admits tuple coding.

Problem x1.21. Suppose that the structure $\mathbf{A} = (A, \text{——})$ has a copy of $\mathbf{N}$ and call it $\mathbf{N} = (\mathbb{N}, 0, S, +, \cdot)$, for simplicity. Suppose $R \subseteq \mathbb{N}^n$ is an arithmetical relation, and let

$$R^{\mathbf{A}}(x_1, \ldots, x_n) \iff x_1, \ldots, x_n \in \mathbb{N} \;\&\; R(x_1, \ldots, x_n)$$

be its natural extension on A, set false when one of the arguments is not in $\mathbb{N}$. Prove that $R^{\mathbf{A}}$ is $\mathbf{A}$-elementary.

Consider the *structure of analysis*

$$(\mathbf{R}, \mathbb{Z}) = (\mathbb{R}, 0, 1, \mathbb{Z}, +, \cdot)$$

obtained by expanding the field of real numbers by the (unary) relation of being an integer. This structure has a copy of $\mathbf{N}$ (by Definition 1E.7), with

$$\mathbb{N} = \{x \in \mathbb{Z} \mid \exists y[y^2 = x]\}.$$

In the next three problems we outline a proof that it admits tuple coding—and considerably more.

Definition 1L.1 (Binary expansion)**.** Every real number can be expanded uniquely in the form

$$x = x^*.x_0x_1x_2\cdots = x^* + \sum_{i=1}^{\infty} \frac{x_i}{2^i}, \tag{31}$$

where $x^* \in \mathbb{Z}$, $x_i \in \{0,1\}$ for each $i \geq 1$, and $x_i \neq 1$ for infinitely many i. (The last condition chooses the representation

$$1.0000\cdots \text{ rather than } 0.1111\cdots$$

for the number 1 and insures the uniqueness. It also insures that for every $n \in \mathbb{N}$,

$$.x_n x_{n+1} \cdots < 1$$

since it cannot be that $x_{n+i} = 1$ for all i.)

Problem x1.22*. Prove that with the notation of Definition 1L.1, the function

$$\mathrm{bin}(x, i) = x_i$$

is elementary in $(\mathbf{R}, \mathbb{Z})$.

HINT: Show first that the functions

1. $\lfloor x \rfloor =$ the largest $y \in \mathbb{Z}$ such that $y \leq x$, so that $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$,
2. $f_n(x) = 2^n x$,

are elementary, and then check that for every real number $x \in [0, 1)$ and every $n \geq 0$,

$$2^n x = \lfloor 2^n x \rfloor + .x_n x_{n+1} \cdots ,$$

which gives $x_n = \lfloor 2^{n+1} x - 2\lfloor 2^n x \rfloor \rfloor$. (There are many other ways to do this, but remember that you do not know yet that you can give recursive definitions in $(\mathbf{R}, \mathbb{Z})$.)

Problem x1.23*. Prove that there is an $(\mathbf{R}, \mathbb{Z})$-elementary function $\gamma(w, i)$ such that for every infinite sequence $x_0, x_1, \ldots \in \mathbb{N}$, there is some $w \in \mathbb{R}$ such that

$$\gamma(w, 0) = x_0, \gamma(w, 1) = x_1, \ldots .$$

HINT: Use Problem x1.22* to code binary sequences by reals, and then code an arbitrary $x_0, x_1, \ldots \in \mathbb{N}$ by the binary sequence

$$(\underbrace{1, 1, \ldots, 1}_{x_0+1}, 0, \underbrace{1, 1, \ldots, 1}_{x_1+1}, 0, \ldots).$$

Problem x1.24*. Prove that there is a $(\mathbf{R}, \mathbb{Z})$-elementary function $\delta(w, i)$ such that for every infinite sequence $x_0, x_1, \ldots, \in \mathbb{R}$, there is some $w \in \mathbb{R}$ such that

$$\delta(w, 0) = x_0, \delta(w, 1) = x_1, \ldots .$$

Infer that $(\mathbf{R}, \mathbb{Z})$ admits tuple coding.

Problem x1.25. Find all n-ary elementary relations in the trivial structure $\mathbf{A} = (A)$, with A infinite.

Problem x1.26. Consider the structure $\mathbf{L} = (\mathbb{Q}, \leq)$ of the rational numbers with (only) their ordering.

1. Find all unary, elementary relations in $\mathbf{L}$.

2. Find all binary, elementary relations in $\mathbf{L}$.

Problem x1.27. (1) Let $\mathbf{L} = ([0, 0), 0, \leq)$, where $[0, 1)$ is the half-open interval of real numbers,

$$[0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$$

and 0 is a constant which names the number 0. Prove that $\mathbf{L}$ admits effective elimination of quantifiers. Infer that it is a decidable structure, i.e., there is an effective procedure which decides whether $\mathbf{L} \models \chi$, for an arbitrary sentence χ.

(2) Let $\mathbf{L}' = ([0, 1), \leq)$ be the same linear ordering as in (1), but in the language without a name for 0. Does $\mathbf{L}'$ admit elimination of quantifiers?

(3) Is the structure $\mathbf{L}'$ decidable?

Problem x1.28*. Prove that the structure $(\mathbb{N}, 0, S)$ admits effective quantifier elimination. Hint: For any term t of this language and any number k, define the term $s + k$ by the recursion

$$s + 0 \equiv s,\ s + (k + 1) \equiv S(s + k),$$

so that (for example) $x + 3 \equiv S(S(S(x)))$, and (with $s \equiv 0$), $3 \equiv 0 + 3 \equiv S(S(S(0)))$. Prove that every literal is equivalent on this structure with a formula in one of the following forms

$$T,\ F,\ x = k,\ x = y + k,\ x \neq k,\ x \neq y + k,$$

where x, y are distinct variables.

Problem x1.29. Show that the structure $(\mathbb{R}, 0, 1, \leq, f)$ with $f(x) = 2x$ admits effective quantifier elimination. Hint: Show first that (with the obvious notation) every term is equivalent in this structure to one of

$$0,\ 2^n,\ 2^n x$$

with a variable x.

Problem x1.30*. Prove that the structure $(\mathbb{R}, 0, 1, +, \leq)$ admits effective quantifier elimination, and so is decidable. Hint: Show first that (with the natural definitions) every term is equal in this structure to a linear expression

$$k_0 + k_1 x_1 + \cdots k_m x_m,$$

where $x_1, \ldots, x_m$ are distinct variables (if $m > 0$), and

$$kx \equiv \underbrace{x + \cdots + x}_{k}.$$

Problem x1.31. Prove that a structure $\mathbf{A}$ admits (effective) quantifier elimination if and only if its theory $\mathrm{Th}(\mathbf{A})$ admits (effective) quantifier elimination.

Problem x1.32. Construct a model of the Robinson system Q which is not isomorphic with the standard model $\mathbf{N}$. Hint: Take for universe $A = \mathbb{N} \cup \{\infty\}$ for some object $\infty \notin \mathbb{N}$.

Problem x1.33. Construct a model of the Robinson system Q in which addition is not commutative. *Hint.* Construct a model of Q whose universe is $\mathbb{N} \cup \{a, b\}$, where $a \neq b$, $Sa = b$ and $Sb = a$.

Problem x1.34. Give an example which shows that the restriction is necessary in Axiom Scheme (10) of $\mathbb{FOL}(\tau)$.

Problem x1.35. Give an example which shows that the restriction on the Exists Elimination Rule (14) of $\mathbb{FOL}(\tau)$ is necessary.

Problem x1.36. Show that if $T \vdash \forall v \phi(v, \vec{u})$ and x is any variable which is free for v in $\phi(v, \vec{u})$, then $T \vdash \forall x \phi(x, \vec{u})$.

Problem x1.37. Prove the Lemma 1H.4 (Constant Substitution), and explain why the restriction that c is a fresh constant is needed.

Problem x1.38. Show that for any two formulas ϕ, ψ,

$$\vdash (\phi \to \psi) \leftrightarrow (\neg\psi \to \neg\phi).$$

Problem x1.39 (Peirce's Law)**.** Show that for any two formulas ϕ, ψ,

$$\vdash ((\phi \to \psi) \to \phi) \to \phi$$

Problem x1.40. Prove that for any set of formulas T and formulas ϕ, ψ, χ, if $T \vdash_{\text{prop}} \phi$ and $T, \psi \vdash_{\text{prop}} \chi$, then $T, \phi \to \psi \vdash_{\text{prop}} \chi$. In symbols:

$$\frac{T \vdash_{\text{prop}} \phi \qquad T, \psi \vdash_{\text{prop}} \chi}{T, \phi \to \psi \vdash_{\text{prop}} \chi}$$

What restrictions are needed to prove this rule with $\vdash$ instead of $\vdash_{\text{prop}}$?

Problem x1.41. Show that for any full extended formula $\phi(x, y)$,

$$\vdash \exists x \forall y \phi(x, y) \to \forall y \exists x \phi(x, y).$$

Does this hold for arbitrary extended formulas $\phi(x, y)$, which may have free variables other than x and y?

Problem x1.42 (The system with just $\neg, \to, \exists$)**.** For every formula ϕ we can construct another formula ϕ^* which is proof-theoretically equivalent with ϕ, and such that $=, \neg, \to, \exists$ are the only logical symbols which (possibly) occur in ϕ^*.

Problem x1.43. Prove that if a sentence χ in $\mathbb{FOL}(\tau)$ is true in all countable models of a countable τ-theory T, then χ is true in all models of T.

Problem x1.44. Suppose χ is a sentence in the language in the language $\mathbb{FOL}(E)$ of graphs. For each of the following claims, determine whether it is true or false and prove your answer.

(1) If χ is true in some infinite graph, then it is true in all finite graphs.
(2) If χ is true in some infinite graph, then it is true in all sufficiently large, finite graphs (i.e., in all finite graphs with more than m nodes, for some m).
(3) If χ is true in some infinite graph, then it is true in infinitely many finite graphs.
(4) If χ is true in some infinite graph, then it is true in at least one finite graph.

Problem x1.45. For each of the following classes of graphs, determine whether it is basic elementary, elementary or neither, and prove your answer:

(1) The class of finite graphs.
(2) The class of infinite graphs.

Problem x1.46*. For each of the following classes of graphs, determine whether it is basic elementary, elementary or neither, and prove your answer:

(1) The class of connected graphs.
(2) The class of disconnected graphs.

Problem x1.47*. For each of the following classes or linear orderings, determine whether it is basic elementary, elementary or neither and prove your answer:

(1) The class $\mathcal{W}$ of wellorderings.
(2) The class $\mathcal{W}^c$ of linear orderings which are not wellorderings.

HINT: You will need the characterization in Problem x6.9,

$$(A, \leq) \text{ is a wellordering} \iff \text{there is no infinite, descending chain } x_0 > x_1 > \cdots .$$

Problem x1.48. Prove that if a sentence χ in the language of fields $\mathbb{FOL}(0, 1, +, \cdot)$ is true in all fields of finite characteristic > 0, then it is also true in some field of characteristic 0.

Problem x1.49*. A graph $\mathbf{G} = (G, E)$ is 3-*colorable* if we can split its universe into three disjoint sets

$$G = A \cup B \cup C, \quad (A \cap B = A \cap C = B \cap C = \emptyset)$$

such that no two adjacent vertices belong to the same part of the partition. Prove that a countable graph $\mathbf{G}$ is 3-colorable if and only if every finite subgraph of $\mathbf{G}$ is 3-colorable.

Hint: You need to apply the Compactness Theorem, in an expansion of the signature which has names for all the members of $\mathbf{G}$ and for the three parts of the required partition.

Problem x1.50. Suppose $\mathbf{N}^* = (\mathbb{N}^*, 0^*, S^*, +^*, \cdot^*)$ is a countable, non-standard model of Peano Arithmetic, and let $\overline{\mathbb{N}}$ be its *standard part*, the image of the function $f : \mathbb{N} \to \mathbb{N}^*$ defined by the recursion

$$f(0) = 0^*, \quad f(n+1) = S^*(f(n)).$$

Prove that $\overline{\mathbb{N}}$ is not an elementary subset of $\mathbf{N}^*$.

Problem x1.51. Give an example of a structure $\mathbf{A} = (A, \text{—})$ (in some signature) and an $\mathbf{A}$-elementary binary relation $Q(x, y)$ on A, such that the relation

$$P(x) \iff (\text{for infinitely many } y) Q(x, y)$$

is not $\mathbf{A}$-elementary.

Problem x1.52*. Suppose $\mathbf{N}^* = (\mathbb{N}^*, 0, S, +, \cdot)$ is a countable, non-standard model of Peano Arithmetic—where we have not bothered to star its primitives—and let $\mathbb{N}$ be its standard part. Set

$$x \sim y \iff |x - y| \in \mathbb{N} \quad (x, y \in \mathbb{N}^*).$$

(1) Prove that $\sim$ is an equivalence relation on $\mathbb{N}^*$, which is not $\mathbb{N}^*$-elementary.

Let Q be a quotient of $\sim$, i.e., a set such that for some surjection $\rho : \mathbb{N}^* \twoheadrightarrow Q$ (and setting $\rho(x) = \overline{x}$ to simplify notation),

$$x \sim y \iff \overline{x} = \overline{y} \quad (x, y \in \mathbb{N}^*);$$

and define on Q the binary relation

$$u \leq v \iff \text{for some } x, y \in \mathbb{N}, u = \overline{x}, v = \overline{y} \text{ and } x \leq^* y,$$

where $x \leq^* y$ is the natural ordering on $\mathbf{N}^*$.

(2) Prove that $\leq$ is a total ordering on Q.

(3) Prove that the ordering $(Q, \leq)$ has a least element but no greatest element, and it is dense in itself, i.e.,

$$u < v \Longrightarrow (\exists w)[u < w \ \& \ w < v] \quad (u, v \in Q).$$

CHAPTER 2

SOME RESULTS FROM MODEL THEORY

Our (very limited) aim in this chapter is to introduce a few, basic notions of classical model theory, and to establish some of their simple properties.

2A. More consequences of Completeness and Compactness

The results in this section are more-or-less straight-forward consequences of the Completeness and the Compactness Theorems.

Definition 2A.1. Suppose $\mathbf{A}, \mathbf{B}$ are τ-structures. A one-to-one function $\pi : A \rightarrowtail B$ is an **embedding** if the following conditions hold:

1. For each constant symbol c of τ, $c^{\mathbf{B}} = \pi(c^{\mathbf{A}})$.
2. For each n-ary relation symbol R and all $x_1 \ldots , x_n \in A$,
$$R^{\mathbf{A}}(x_1 \ldots , x_n) \iff R^{\mathbf{B}}(\pi(x_1) \ldots , \pi(x_n)).$$
3. For each n-ary function symbol f and all $x_1 \ldots , x_n \in A$,
$$f^{\mathbf{B}}(\pi(x_1) \ldots , \pi(x_n)) = \pi(f^{\mathbf{A}}(x_1 \ldots , x_n)).$$

It is an **elementary embedding** if in addition, for every full extended formula $\chi(v_1, \ldots , v_n)$ and all $x_1, \ldots , x_n \in A$,
$$\mathbf{A} \models \chi[x_1, \ldots , x_n] \iff \mathbf{B} \models \chi[\pi(x_1), \ldots , \pi(x_n)].$$

If $A \subseteq B$, then clearly, the identity $\mathrm{id} : A \rightarrowtail B$ is an imbedding exactly when $\mathbf{A}$ is a substructure of $\mathbf{B}$, i.e., $\mathbf{A} \subseteq \mathbf{B}$. We set
$$\mathbf{A} \preceq \mathbf{B} \iff \mathrm{id} : A \rightarrowtail B \text{ is an elementary embedding,}$$
and when this holds, we say that $\mathbf{A}$ is an **elementary substructure** of $\mathbf{B}$ and $\mathbf{B}$ is an **elementary extension** of $\mathbf{A}$.

Isomorphisms are obviously elementary embeddings, and the composition of elementary embeddings is an elementary embedding. It is also clear that if $\mathbf{A} \preceq \mathbf{B}$, then the two structures are elementarily equivalent, but the converse does not hold in general: for example, if
$$\mathbf{A} = (\{1, 2, \ldots\}, \leq), \quad \mathbf{B} = (\{0, 1, \ldots\}, \leq)$$

with $\leq$ the usual ordering in both cases, then $\mathbf{A} \subseteq \mathbf{B}$, the mapping $x \mapsto x-1$ is an isomorphism of $\mathbf{A}$ with $\mathbf{B}$ (and so $\mathbf{A} \equiv \mathbf{B}$), but $\mathbf{A}$ is not an elementary substructure of $\mathbf{B}$ because

$$\mathbf{A} \models \forall x(v \leq x)[1] \text{ while } \mathbf{B} \models \neg\forall x(v \leq x)[1].$$

Lemma 2A.2. *Suppose* $\mathbf{A}$ *and* $\mathbf{B}$ *are* τ*-structures.*

(1) *If* $\pi : \mathbf{A} \rightarrowtail \mathbf{B}$ *is an embedding, then* π *is an isomorphism of* $\mathbf{A}$ *with* $\mathbf{A}' = \pi[\mathbf{A}] \subseteq \mathbf{B}$*, and there is an extension* $\mathbf{B}' \supseteq \mathbf{A}$ *and an isomorphism* $\rho : \mathbf{B} \rightarrowtail\!\!\!\!\rightarrow \mathbf{B}'$ *such that for every* $x \in A$*,* $\rho(\pi(x)) = x$*.*

(2) *If* $\pi : \mathbf{A} \rightarrowtail \mathbf{B}$ *is an elementary embedding, then* π *is an isomorphism of* $\mathbf{A}$ *with* $\mathbf{A}' = \pi[\mathbf{A}] \preceq \mathbf{B}$*, and there is an elementary extension* $\mathbf{B}' \succeq \mathbf{A}$ *and an isomorphism* $\rho : \mathbf{B} \rightarrowtail\!\!\!\!\rightarrow \mathbf{B}'$ *such that for every* $x \in A$*,* $\rho(\pi(x)) = x$*.*

PROOF of the second claim of (2). We may assume that $A \cap B = \emptyset$, by replacing $\mathbf{B}$ (if necessary) by an isomorphic structure, we let

$$B' = A \cup (B \setminus \pi[A]),$$

we define $\sigma : B' \rightarrowtail\!\!\!\!\rightarrow B$ by

$$\sigma(x) = \begin{cases} \pi(x), & \text{if } x \in A, \\ x, & \text{otherwise} \end{cases}$$

and we interpret the constant, relation and function symbols of the signature in B' by copying them from $\mathbf{B}$ using the bijection σ:

$$\begin{aligned} c^{\mathbf{B}'} &= \sigma(c^{\mathbf{A}}) = \pi(c^{\mathbf{A}}) = c^{\mathbf{B}}, \\ R^{\mathbf{B}'}(x_1, \dots, x_n) &\iff R^{\mathbf{B}}(\sigma(x_1), \dots, \sigma(x_n)), \\ f^{\mathbf{B}'}(x_1, \dots, x_n) &= \sigma^{-1}(f^{\mathbf{B}}(\sigma(x_1), \dots, \sigma(x_n)). \end{aligned}$$

Now $\sigma : \mathbf{B}' \rightarrowtail\!\!\!\!\rightarrow \mathbf{B}$ is an isomorphism by definition, and $\mathbf{A} \preceq \mathbf{B}'$ directly by the definitions: for any $\chi(\vec{v})$ and any $\vec{x} \in A^n$ and using that π is an imbedding and the definition of σ,

$$\begin{aligned} \mathbf{A} \models \chi[\vec{x}] &\iff \mathbf{B} \models \chi[\pi(\vec{x})] \\ &\iff \mathbf{B} \models \chi[\sigma(\vec{x})] \\ &\iff \mathbf{B}' \models \chi[\vec{x}]. \end{aligned}$$

The required isomorphism $\rho : \mathbf{B} \rightarrowtail\!\!\!\!\rightarrow \mathbf{B}'$ is the inverse $\rho = \sigma^{-1}$, and proofs of the other claims are similar. ⊣

There is an alternative way of formulating this lemma in terms of sets of sentences in the expanded vocabulary

(32) $$\overline{\tau}^{\mathbf{A}} = (\tau, \{c_a \mid a \in A\})$$

associated with each (countable) structure $\mathbf{A}$ and constructed by adding a distinct, fresh constant c_a for each $a \in A$. The **diagram** of $\mathbf{A}$ is the set of $\overline{\tau}^{\mathbf{A}}$-sentences

$$\begin{aligned}\mathrm{Diagram}(\mathbf{A}) = \{\theta(c_{a_1}, \dots, a_{c_n}) \mid \\ \theta(v_1, \dots, v_n) \text{ is a full extended } \tau\text{-literal and } \mathbf{A} \models \theta[a_1, \dots, a_n]\},\end{aligned}$$

where by 1F.2, a literal is a prime formula or the negation of a prime formula. Similarly, the **elementary diagram** of $\mathbf{A}$ is the set

$$\begin{aligned}\mathrm{EDiagram}(\mathbf{A}) = \{\theta(c_{a_1}, \dots, a_{c_n}) \mid \\ \theta(v_1, \dots, v_n) \text{ is a full extended } \tau\text{-formula and } \mathbf{A} \models \theta[a_1, \dots, a_n]\}.\end{aligned}$$

Lemma 2A.3. *Suppose* $\mathbf{A}$ *is a* τ*-structure and* $\mathbf{B}$ *is a* $\overline{\tau}^{\mathbf{A}}$*-structures, where* $\overline{\tau}^{\mathbf{A}}$ *is the expanded signature of* $\mathbf{A}$, *and let* $\mathbf{B} \restriction \tau$ *be the reduct of* $\mathbf{B}$ *to* τ.

(1) *If* $\mathbf{B} \models \mathrm{Diagram}(\mathbf{A})$, *then there is a* τ*-structure* $\mathbf{B}' \supseteq \mathbf{A}$ *and an isomorphism* $\rho : \mathbf{B}' \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbf{B} \restriction \tau$ *for which* $\rho(a) = c_a^{\mathbf{B}}$.

(2) *If* $\mathbf{B} \models \mathrm{EDiagram}(\mathbf{A})$, *then there is a* τ*-structure* $\mathbf{B}' \succeq \mathbf{A}$ *and an isomorphism* $\rho : \mathbf{B}' \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbf{B} \restriction \tau$ *for which* $\rho(a) = c_a^{\mathbf{B}}$.

Proof. The hypothesis of (1) implies easily that the map $\pi : A \to B$ defined by

$$\pi(a) = c_a^{\mathbf{B}}$$

is an imbedding of $\mathbf{A}$ into $\mathbf{B}$, and then (1) of Lemma 2A.2 gives the required conclusion. (2) is proved similarly, using (2) of Lemma 2A.2. $\dashv$

Theorem 2A.4. *Every infinite countable structure has a proper, countable elementary extension.*

Proof. Given $\mathbf{A}$, let

$$T = \mathrm{EDiagram}(\mathbf{A}) \cup \{d \neq c_a \mid a \in A\}$$

in the vocabulary $\overline{\tau}^{\mathbf{A}}$ expanded further by a fresh constant d. Every finite subset T_0 of T has a model, namely the expansion of $\mathbf{A}$ which interprets each c_a by a and d by some member of A which does not occur in T_0. By the Compactness Theorem, T has a model $\mathbf{B}$, and $\mathbf{B} \models \mathrm{EDiagram}(\mathbf{A})$. Now Lemma 2A.3 gives us a $\mathbf{B}' \succeq \mathbf{A}$ and an isomorphism $\rho : \mathbf{B}' \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbf{B}$ for which $\rho(a) = c_a^{\mathbf{B}}$—which means that $\mathbf{B}'$ is a proper extension of $\mathbf{A}$, since there must be some $d' \notin A$ for which $\rho(d') = d^{\mathbf{B}}$. $\dashv$

Note that the construction in this theorem is a generalization of the proof of Theorem 1J.5, so that the non-standard model $\mathbf{N}^*$ constructed in 1J.5 is, in fact, an elementary extension of the standard model of arithmetic, $\mathbf{N} \preceq \mathbf{N}^*$.

Definition 2A.5. A formula ϕ is **existential** if

$$\phi \equiv \exists v_1 \exists v_2 \cdots \exists v_n \psi \quad \text{where } \psi \text{ is quantifier free,}$$

and, similarly, ϕ is **universal** if

$$\phi \equiv \forall v_1 \forall v_2 \cdots \forall v_n \psi \quad \text{where } \psi \text{ is quantifier free.}$$

Theorem 2A.6. *The following are equivalent for a τ-theory T and a τ-sentence χ:*

(1) *If $\mathbf{A} \subseteq \mathbf{B}$ and both are models of T, then $\mathbf{B} \models \chi \Longrightarrow \mathbf{A} \models \chi$.*
(2) *There is a universal sentence χ^* such that $T \vdash \chi \leftrightarrow \chi^*$.*

Similarly, the following are equivalent:

(3) *If $\mathbf{A} \subseteq \mathbf{B}$ and both are models of T, then $\mathbf{A} \models \chi \Longrightarrow \mathbf{B} \models \chi$.*
(4) *There is an existential sentence χ^* such that $T \vdash \chi \leftrightarrow \chi^*$.*

Proof. The second claim in the theorem follows from the first (applied to $\neg\chi$), and the implication (2) $\Longrightarrow$ (1) is simple, so it is enough to prove that (1) $\Longrightarrow$ (2).

Fix a sentence χ which satisfies (1), and let

$$S_\chi = \{\theta \mid \theta \text{ is a universal sentence and } T, \chi \vdash \theta\}.$$

Lemma. If $T \cup S_\chi \cup \{\neg\chi\}$ is inconsistent, then (2) holds.

Proof. The hypothesis implies that

$$T, S_\chi \vdash \chi,$$

and so there is a finite sequence $\theta_1, \dots, \theta_n \in S_\chi$ such that

$$T, \theta_1, \dots, \theta_n \vdash \chi.$$

Notice that since $\theta_1, \dots, \theta_n \in S_\chi$, we also have

$$T, \chi \vdash \theta_1 \;\&\; \cdots \;\&\; \theta_n.$$

Now, easily, there is a universal sentence χ^* such that

$$\vdash \chi^* \leftrightarrow \theta_1 \;\&\; \cdots \;\&\; \theta_n,$$

so that

$$T, \chi^* \vdash \chi \text{ and } T, \chi \vdash \chi^*$$

which give the required $T \vdash \chi \leftrightarrow \chi^*$. ⊣ (Sublemma)

So it is enough to derive a contradiction from the assumption that the theory $T \cup S_\chi \cup \{\neg\chi\}$ is consistent, or, equivalently that $T \cup S_\chi \cup \{\neg\chi\}$ *has a countable model* $\mathbf{A}$. Notice that

there is no model of T, $\mathbf{B} \supseteq \mathbf{A}$ such that $\mathbf{B} \models \chi$;

this is because if such a $\mathbf{B}$ existed, then $\mathbf{A} \models \chi$ by the hypothesis on χ, which contradicts the assumption $\mathbf{A} \models \neg\chi$. It follows by Lemma 2A.3 that the set

$$S = T \cup \mathrm{Diagram}(\mathbf{A}) \cup \{\chi\}$$

(in the vocabulary $\tau^{\mathbf{A}}$) is inconsistent, so that

$$T, \theta_1(c_{a_1}, \dots, c_{a_n}), \dots, \theta_k(c_{a_1}, \dots, c_{a_n}) \vdash \neg\chi,$$

for some sequence $\theta_1(\vec{v}), \dots, \theta_k(\vec{v})$ of full, extended τ-literals and suitable $a_1, \dots, a_n \in A$. Since none of the fresh constants $c_{a_1}, \dots, c_{a_n}$ occur in χ, we have by $\exists$-elimination,

$$T, \exists v_1 \exists v_1 \cdots \exists v_n (\theta_1 \;\&\; \cdots \;\&\; \theta_k) \vdash \neg\chi,$$

so that

$$T, \chi \vdash \theta \text{ with } \theta \equiv \forall v_1 \forall v_1 \cdots \forall v_n \neg(\theta_1 \;\&\; \cdots \;\&\; \theta_k)$$

and hence $\theta \in S_\chi$, so that $\mathbf{A} \models \theta$; but immediately from its definition, we also have $\mathbf{A} \models \neg\theta$, which is absurd. ⊣

2B. The downward Skolem-Löwenheim Theorem

In this section we will prove the following substantial extension of Theorem 1J.3:

Theorem 2B.1 (Countable, downward Skolem-Löwenheim Theorem). *If $X \subseteq B$ is a countable subset of the universe of a structure $\mathbf{B}$, then there exists a countable, elementary substructure $\mathbf{A} \preceq \mathbf{B}$ such that $X \subseteq A$.*

This is one of the fundamental results of model theory with important mathematical and foundational applications. For example, if we apply it to the universe of sets $\mathbf{V} = (V, \in)$ with $X = \{\kappa\}$, the singleton of an uncountable set κ, it yields a countable $\mathbf{A} \preceq \mathbf{V}$ with $\kappa \in A$: in particular, the universe A of $\mathbf{A}$ is a collection of *sets*, $\in^{\mathbf{A}}$ is the standard membership relation, and $\mathbf{A}$ "believes" that κ uncountable, although it is clearly countable, as a subset of the countable set A. This application can only be established in a rather strong set theory (because the universe V of sets is not a set), but it poses "the Skolem paradox" in a very striking manner.

The proof of Theorem 2B.1 will use the following three, simple lemmas.

Lemma 2B.2. *Suppose $\mathbf{B}$ is a τ-structure and $A \subseteq B$; then A is the universe of a substructure $\mathbf{A} \subseteq \mathbf{B}$ if and only if A contains the interpretation $c^{\mathbf{B}}$ in $\mathbf{B}$ of every constant in τ and it is closed under the interpretation $f^{\mathbf{B}}$ of every function symbol of τ,*

$$x_1, \dots, x_n \in A \Longrightarrow f^{\mathbf{B}}(x_1, \dots, x_n) \in A.$$

PROOF. For the direction of the claim which is not immediate, just set $c^{\mathbf{A}} = c^{\mathbf{B}}$, $f^{\mathbf{A}} = f^{\mathbf{B}} \upharpoonright A$, and

$$R^{\mathbf{A}}(x_1, \dots, x_n) \iff R^{\mathbf{B}}(x_1, \dots, x_n) \quad (x_1, \dots, x_n \in A). \qquad \dashv$$

Lemma 2B.3. *Suppose* $\mathbf{A} \subseteq \mathbf{B}$*; then* $\mathbf{A} \preceq \mathbf{B}$ *if and only if for each full extended formula* $\phi(v_1, \dots, v_n, u)$ *and any* $x_1, \dots, x_n \in A$*,*

(33) if there exists some $y \in B$ such that $\mathbf{B} \models \phi[x_1, \dots, x_n, y]$,
then there exists some $z \in A$ such that $\mathbf{B} \models \phi[x_1, \dots, x_n, z]$.

PROOF. Assume first that $\mathbf{A} \preceq \mathbf{B}$. If the hypothesis of (33) holds with some $x_1, \dots, x_n \in A$, then

$$\mathbf{B} \models \exists u \phi[x_1, \dots, x_n],$$

and so by the hypothesis $\mathbf{A} \preceq \mathbf{B}$, we have

$$\mathbf{A} \models \exists u \phi[x_1, \dots, x_n],$$

which implies that for some $z \in A$, $\mathbf{A} \models \phi[x_1, \dots, x_n, z]$; now $\mathbf{A} \preceq \mathbf{B}$ again implies the conclusion of (33).

For the converse, assume that $\mathbf{A} \subseteq \mathbf{B}$ and (33) holds for every $\phi(v_1, \dots, v_n, u)$. We need to prove that for every $\chi(v_1, \dots, v_n)$ and all $x_1, \dots, x_n \in A$,

$$\mathbf{A} \models \chi[x_1, \dots, x_n] \iff \mathbf{B} \models \chi[x_1, \dots, x_n],$$

and we do this by structural induction on χ. The argument is trivial in the basis case, for prime χ, because $\mathbf{A} \subseteq \mathbf{B}$, and it is very easy when χ is a propositional combination of smaller formulas. If $\chi \equiv \exists u \phi(v_1, \dots, v_n, u)$, then

$$\begin{aligned}
\mathbf{A} \models \chi[x_1, \dots, x_n] &\iff \text{for some } z \in A, \mathbf{A} \models \phi[x_1, \dots, x_n, z] \\
&\iff \text{for some } z \in A, \mathbf{B} \models \phi[x_1, \dots, x_n, z] \text{ (ind. hyp.)} \\
&\iff \text{for some } y \in B, \mathbf{B} \models \phi[x_1, \dots, x_n, y] \text{ (assumption)} \\
&\iff \mathbf{B} \models \chi[x_1, \dots, x_n].
\end{aligned}$$

Finally, if $\chi \equiv \forall u \phi(v_1, \dots, v_n, u)$ we use the same argument together with the equivalence

$$\models \chi \leftrightarrow \neg \exists u \neg \phi(v_1, \dots, v_n, u) \qquad \dashv$$

Definition 2B.4 (Absoluteness and Skolem sets). Suppose $\mathbf{B}$ is a τ-structure and ϕ is a formula. A set of functions $\mathcal{S}$ (of all arities) on the universe B is a *Skolem set for* ϕ *in* $\mathbf{B}$, if for every substructure $\mathbf{A} \subseteq \mathbf{B}$, if A is closed under (all the functions in) $\mathcal{S}$, then ϕ *is absolute between* $\mathbf{A}$ *and* $\mathbf{B}$, i.e., if all the free variables of ϕ are in and list $v_1, \dots, v_n$ and $x_1, \dots, x_n \in A$, then

$$\mathbf{A} \models \phi[x_1, \dots, x_n] \iff \mathbf{B} \models \phi[x_1, \dots, x_n]. \tag{34}$$

Notice that (directly from the definition), if $\mathcal{S}$ is a Skolem set for ϕ and $\mathcal{S} \subseteq \mathcal{S}'$, then $\mathcal{S}'$ is also a Skolem set for ϕ.

In the proof of the next lemma we will appeal to the Axiom of Choice, in the following (so-called) logical form: if $R \subseteq X \times Y$ is a binary relation, then

$$(\forall x \in X)(\exists y \in Y)R(x,y) \Longrightarrow (\exists f : X \to Y)(\forall x \in X)R(x, f(x)). \tag{35}$$

Lemma 2B.5. *In every τ-structure $\mathbf{B}$, every formula ϕ has a finite Skolem set.*

Proof is by structural induction on ϕ, and it is trivial at the base: if ϕ is prime, we simply take $\mathcal{S}_\phi = \emptyset$. Proceeding inductively, set

$$\mathcal{S}_{\neg\phi} = \mathcal{S}_\phi, \quad \mathcal{S}_{\phi\ \&\ \psi} = \mathcal{S}_{\phi\vee\psi} = \mathcal{S}_{\phi\to\psi} = \mathcal{S}_\phi \cup \mathcal{S}_\psi,$$

and check easily that the induction hypothesis implies the required property for the result. In the interesting case when

$$\phi(v_1, \dots, v_n) \equiv \exists u \psi(v_1, \dots, v_n, u),$$

fix some $y_0 \in B$ and set

$$\begin{aligned} R(x_1, \dots, x_n, y) \iff & \mathbf{B} \models \psi[x_1, \dots, x_n, y] \\ & \text{or } \big(\text{for all } y \in B, \mathbf{B} \not\models \psi[x_1, \dots, x_n, y] \text{ and } y = y_0\big) \end{aligned}$$

so that, obviously, for all $\vec{x} \in B^n$ there is some $y \in B$ such that $R(\vec{x}, y)$. The Axiom of Choice gives us a function $f : B^n \to B$ such that $R(\vec{x}, f(\vec{x}))$ for all $\vec{x} \in B^n$, and we set

$$\mathcal{S}_{\exists u\psi} = \mathcal{S}_\psi \cup \{f\}.$$

For the non-trivial direction of (34), we assume that $\mathbf{A} \subseteq \mathbf{B}$, A is closed under all the functions in $\mathcal{S}_{\exists u\psi}$ (including f) and $x_1, \dots, x_n \in A$. Compute, using the induction hypothesis:

$$\begin{aligned} \mathbf{B} \models \exists u\psi[x_1, \dots, x_n] & \Longrightarrow \text{for some } y \in B, \mathbf{B} \models \psi[x_1, \dots, x_n, y] \\ & \Longrightarrow \mathbf{B} \models \psi[x_1, \dots, x_n, f(x_1, \dots, x_n)] \\ & \Longrightarrow \mathbf{A} \models \psi[x_1, \dots, x_n, f(x_1, \dots, x_n)] \\ & \Longrightarrow \mathbf{A} \models \exists u\psi[x_1, \dots, x_n]. \end{aligned}$$

Finally, when $\phi \equiv \forall u\psi$ we set $\mathcal{S}_{\forall u\psi} = \mathcal{S}_{\exists u\psi}$ and verify (34) directly. ⊣

Proof of Theorem 2B.1. Given $\mathbf{B}$ and a countable $X \subseteq B$, fix some $y_0 \in B$, let

$$Y = X \cup \{y_0\} \cup \{c^{\mathbf{B}} \mid c \text{ a constant symbol}\},$$

so that Y is countable and not empty (even if $X = \emptyset$ and there are no constants). Let $\mathcal{S}_\phi$ be a finite Skolem set for each formula ϕ, by Lemma 2B.5, set

$$\mathcal{F} = \{f^{\mathbf{B}} \mid f \text{ is a function symbol}\} \cup \bigcup_\phi \mathcal{S}_\phi,$$

and let A be the closure of Y under $\mathcal{F}$ by appealing to Problem x6.3. Now A is countable by Problem x6.6 (because Y and $\mathcal{F}$ are countable), and it is the universe of some $\mathbf{A} \subseteq \mathbf{B}$ by Lemma 2B.2. Moreover, for each ϕ, A is closed under a Skolem set for ϕ, and so (34) holds, which means precisely that $\mathbf{A} \preceq \mathbf{B}$. ⊣

2C. Types

Actually, there are at least two (related) kinds of types, the types of a theory T and those of a structure $\mathbf{A}$, and there are important results about both of them. In this section we will prove just one, basic fact for each of these two kinds; the proofs are elaborations of he proof of the Completeness Theorem.

Definition 2C.1. A **partial** n**-type** of a τ-theory T is any set $\Phi(\vec{v})$ of τ-formulas all of whose free variables are in the given list $\vec{v} \equiv v_1, \dots, v_n$, and such that (with fresh constants $c_1, \dots, c_n$), the theory

$$T \cup \{\phi(c_1, \dots, c_n) \mid \phi \in \Phi\}$$

is consistent; Φ is a **complete type** of T if, in addition, for each full, extended formula $\phi(v_1, \dots, v_n)$, either $\phi \in \Phi$ or $\neg\phi \in \Phi$.

A partial n-type $\Phi(\vec{v})$ of T is **realized** in a model $\mathbf{A}$ of T if

$$\phi(v_1, \dots, v_n) \in \Phi \Longrightarrow \mathbf{A} \models \phi[x_1, \dots, x_n]$$

for some n-tuple $x_1, \dots, x_n \in A$; and it is **omitted** in $\mathbf{A}$ if it is not realized in $\mathbf{A}$. Note that if $\Phi(\vec{x})$ is complete, then it is realized in $\mathbf{A}$ exactly when for some $\vec{x} \in A^n$,

$$\Phi = \{\phi(\vec{v}) \mid \mathbf{A} \models \phi[\vec{x}]\}.$$

A partial n-type $\Phi(\vec{v})$ of T is **principal** if there is a full extended formula $\chi(v_1, \dots, v_n)$ so that the following hold:

(1) $T \vdash \exists\vec{v}\chi(\vec{v})$.

(2) For every $\phi(\vec{v}) \in \Phi$, $T \vdash \forall\vec{v}[\chi(\vec{v}) \to \phi(\vec{v})]$.

When (1) and (2) hold, we say that $\chi(\vec{v})$ **supports** the type $\Phi(\vec{v})$ in T.

Remark. We have defined *partial, complete* and *principal* types of T, but we have avoided defining the plain "types" of T because the terminology about types is not completely standard: in some books what we call "partial types" are just called "types", while in others "types" are what we call here "complete types". It is usually very easy to check what the authors are talking about, and in these notes we will stick to the precise terms of this definition.

Notice that every principal partial type of T is realized in every model $\mathbf{A}$ of T: because, by (1) of the definition, there exists a tuple $x_1, \dots, x_n \in A$ such that $\mathbf{A} \models \chi[x_1, \dots, x_n]$, and every such $\vec{x}$ satisfies every formula in Φ. The next result is the converse of this fact for complete theories:

Theorem 2C.2 (The Omitting Types Theorem). *If T is a complete, consistent theory and Φ is a non-principal, partial n-type of T, then Φ is omitted in some countable model of T.*

Proof. Fix a consistent, complete theory T and a non-principal partial 1-type $\Phi(v)$ of T—the argument for n-types being only notationally more complicated. We will construct a model of T which omits $\Phi(v)$ by an elaboration of the proof of the Completeness Theorem, so we start by adding to the vocabulary τ a sequence of fresh constants

$$d_0, d_1, \dots$$

and constructing an enumeration of all the sentences in the extended signature $(\tau, \{d_0, d_1, \dots\})$

$$\chi_0, \chi_1, \dots .$$

(We will not bother this time to keep track of where the fresh constants occur in the sentences χ_i.)

Lemma. There is a sequence

$$\psi_0, \psi_1, \dots ,$$

of $(\tau, \{d_0, d_1, \dots\})$-sentences so that the following hold:

(1) *For each k, the theory $T \cup \{\psi_0, \dots, \psi_k\}$ is consistent.*
(2) *For each n, either $\psi_{3n} \equiv \chi_n$ or $\psi_{3n} \equiv \neg\chi_n$.*
(3) *For each n, if $\psi_{3n} \equiv \exists u\sigma(u)$, then $\psi_{3n+1} \equiv \sigma(d_i)$, for some i such that the fresh constant d_i does not occur in $\psi_0, \dots, \psi_{3n}$; otherwise $\psi_{3n+1} \equiv \psi_{3n}$.*
(4) *For each n, if there exists some formula $\phi(v) \in \Phi$ such that the set*

$$T \cup \{\psi, \dots, \psi_{3n+1}, \neg\phi(d_n)\}$$

is consistent, then $\phi_{3n+1} \equiv \neg\phi(d_n)$ for one such $\phi(v)$; otherwise, $\psi_{3n+2} \equiv \psi_{3n+1}$.

Proof of the Lemma. We construct the required sequence $\psi_0, \psi_1, \dots$ by recursion (keeping the initial segments consistent with T) exactly as we did in the proof of the Completeness Theorem in the stages $3n$ and $3n+1$. The additional case $3n+2$ is trivial. ⊣ (Lemma)

We now check that the set $H = T \cup \{\psi_0, \psi_1, \dots\}$ is a Henkin set and we construct a structure $\overline{\mathbf{A}}$ in the expanded signature $(\tau, \{d_0, d_1, \dots\})$ such that for every sentence θ,

$$\overline{\mathbf{A}} \models \theta \iff \theta \in H, \tag{36}$$

exactly as in the proof of the Completeness Theorem; the universe of $\overline{\mathbf{A}}$ is

$$\overline{A} = \{\overline{d}_0, \overline{d}_1, \dots\} \text{ with } \overline{d}_i = d_i^{\overline{\mathbf{A}}},$$

and $\overline{\mathbf{A}} \models T$. It follows that the reduct $\mathbf{A} = \overline{\mathbf{A}} \restriction \tau$ is also a model of T, and so it is enough to prove that $\mathbf{A}$ does not realize the type $\Phi(v)$. Note that the universe of $\mathbf{A}$ is the same as that of $\overline{\mathbf{A}}$, i.e., the set $\{\overline{d}_0, \overline{d}_1, \dots\}$.

Suppose, towards a contradiction that there is some $\overline{d}_n \in \overline{A}$ which realizes $\Phi(v)$ so that

$$\overline{\mathbf{A}} \models \phi(d_n), \text{ for every } \phi(v) \in \Phi,$$

and by (36),

$$\phi(d_n) \in H, \text{ for every } \phi(v) \in \Phi.$$

This means that at stage $3n+2$ in the construction in the Lemma we could not add $\neg\phi(d_n)$ to H, for any $\phi(v) \in \Phi$, and so the set

$$T \cup \{\psi_0, \dots, \psi_{3n+1}, \neg\phi(d_n)\}$$

is inconsistent, i.e.,

$$\text{for every } \phi(v) \in \Phi,\ T, \psi_0, \dots, \psi_{3n+1} \vdash \phi(d_n).$$

Keeping in mind that the constant d_n may have already been used in the construction at stage $3n+2$, suppose that the fresh constants which occur in the sentences $\psi_0, \dots, \psi_{3n+1}$ are in the list

$$\vec{d}, d_n \equiv d_{i_1}, \dots, d_{i_k}, d_n,$$

so that

$$\text{for every } \phi(v) \in \Phi,\ T, \psi(\vec{d}, d_n) \vdash \phi(d_n),$$

where $\psi(\vec{d}, d_n) \equiv \psi_0 \,\&\, \cdots \,\&\, \psi_{3n+1}$, and let $\psi(u_1, \dots, u_k, u)$ be the τ-formula obtained by replacing the constants $\vec{d}, d_n$ with fresh variables. Since none of the constants in the list $\vec{d}$ occurs in $\phi(d_n)$, we can apply $\exists$-elimination to deduce that

$$\text{for every } \phi(v) \in \Phi,\ T, \exists u_1, \exists u_2 \cdots \exists u_k \psi(\vec{u}, d_n) \vdash \phi(d_n),$$

and then by the Deduction Theorem,

$$\text{for every } \phi(v) \in \Phi,\ T \vdash \theta^*(d_n) \to \phi(d_n),$$

where $\theta^*(d_n) \equiv \exists u_1, \exists u_2 \cdots \exists u_k \psi(\vec{u}, d_n)$. By the Constant Substitution Lemma 1H.4,

$$\text{for every } \phi(v) \in \Phi,\ T \vdash \theta^*(w) \to \phi(w),$$

with a fresh variable w, and then by generalization we finally get

$$\text{for every } \phi(v) \in \Phi,\ T \vdash \forall v[\theta^*(v) \to \phi(v)]. \tag{37}$$

We also claim that

$$T \vdash \exists v \theta^*(v); \tag{38}$$

because otherwise we would have that $T \vdash \neg\exists v\theta^*(v)$, since T is complete, and this is absurd since $\mathbf{A} \models \exists v\theta^*(v)$ by the construction, and $\mathbf{A}$ is a model of T.

Now (37) and (38) together imply that $\Phi(v)$ is principal over T. ⊣

Corollary 2C.3 (to the proof of 2C.2). *If T is a consistent theory and $\Phi(\vec{v})$ is a partial n-type of T, then there exists a formula $\chi(\vec{v})$ and a countable model $\mathbf{A}$ of T so that the following hold:*

(1) $\mathbf{A} \models \exists\vec{v}\chi(\vec{v})$.
(2) *For every* $\phi(\vec{v}) \in \Phi$, $T \vdash (\forall\vec{v})[\chi(\vec{v}) \to \phi(\vec{v})]$.

(In fact this Corollary is what we showed, and it easily implies Theorem 2C.2 with the additional hypothesis that T is complete.)

Theorem 2C.4 (Omitting countably many types). *Suppose T is a complete, consistent theory and for each $i = 0, 1, \ldots$, Φ_i is a non-principal, partial n_i-type of T; then then there is a countable model of T which omits every Φ_i.*

Proof is by a minor modification of the proof of Theorem 2C.2, where we modify the construction which insures that every Φ_i is omitted in the model $\mathbf{A}$. ⊣

(The missing details can be seen in the proof Theorem 2C.7 below, which is quite similar and which we have included in full.)

We now turn to results about *realizing* rather than omitting types in a structure, and it is best to adjust the definitions somewhat.

Definition 2C.5. Let $\mathbf{A}$ be a τ-structure and $X \subseteq A$, let

$$\tau_X = (\tau, \{c_a \mid a \in X\})$$

be the expansion of τ with (fresh) constants for the members of X, and let

$$\mathbf{A}_X = (\mathbf{A}, \{a \mid a \in X\})$$

be the τ_X-structure which is the expansion of $\mathbf{A}$ in which each c_a $(a \in X)$ is interpreted by a.

A **partial n-type of A over** X is any set $\Phi(v_1, \dots, v_n)$ of τ_X-formulas whose free variables are among $v_1, \dots, v_n$ and which is *finitely satisfiable* in $\mathbf{A}$, i.e., such that for every finite $\Phi_0 \subseteq \Phi$, there exists a tuple $x_1, \dots, x_n$ such that for every $\phi \in \Phi_0$,

$$\mathbf{A}_X \models \phi[x_1, \dots, x_n]; \tag{39}$$

$\Phi(v_1, \dots, v_n)$ is **realized** in $\mathbf{A}$ if there is a tuple $x_1, \dots, x_n$ such that (39) holds for every $\phi \in \Phi$.

A structure $\mathbf{A}$ is **countably saturated** if for every finite $X \subseteq A$ and every n, every partial n-type $\Phi(v_1, \dots, v_n)$ of $\mathbf{A}$ over X which is finitely satisfiable is realized.

If $\mathbf{A}$ is infinite, then, in general, there are uncountably many partial n-types of $\mathbf{A}$ over a finite X, and we cannot hope to extend $\mathbf{A}$ so that it realizes all of them: in fact countably saturated structures are few and very special. Our aim here is to construct elementary extensions of an arbitrary, countably infinite $\mathbf{A}$ which realize as many types as possible.

Definition 2C.6. A τ-partial m-n-**pretype** is a set of τ-formulas

$$\Omega(u_1, \dots, u_m; v_1, \dots, v_n) = \{\omega_0(\vec{u}; \vec{v}), \omega_1(\vec{u}; \vec{v}), \dots\}$$

with the indicated two sequences of distinct free variables. On each τ-structure $\mathbf{A}$ and for each m-tuple

$$\vec{a} = (a_1, \dots, a_m) \in A^m$$

of members of A, the pretype Ω determines the set of $\tau_{\{a_1, \dots, a_m\}}$-formulas

$$\Omega^{\vec{a}}(\vec{v}) = \{\omega_0(\vec{a}; \vec{v}), \omega_1(\vec{a}; \vec{v}), \dots\},$$

which is a partial n-type of $\mathbf{A}$ over $\{a_1, \dots, a_m\}$ if it is finitely satisfiable in $\mathbf{A}$.

A τ-structure $\mathbf{A}$ is Ω-**saturated** if for every $\vec{a} = a_1, \dots, a_m \in A$, if $\Omega^{\vec{a}}(\vec{v})$ is finitely satisfiable in $\mathbf{A}$, then it is realized in $\mathbf{A}$.

It is not hard to show that for every countable structure $\mathbf{A}$ and every partial pretype Ω, there is a Ω-saturated, elementary extension $\mathbf{B} \succeq \mathbf{A}$. We will show directly the messier but more useful generalization to infinitely many pretypes, as an additional example of this kind of construction.

Theorem 2C.7. *Suppose that for each $i = 0, 1, \dots,$*

$$\begin{aligned}\Omega_i(u_1, \dots, u_{m_i}; v_1, \dots, v_{n_i}) \\ = \{\omega_{i,s}(u_1, \dots, u_{m_i}; v_1, \dots, v_{n_i}) \mid s = 0, 1, \dots\}\end{aligned}$$

is a τ-partial m_i-n_i-pretype, and $\mathbf{A}$ *is a countable, infinite τ-structure; then* $\mathbf{A}$ *has an elementary extension $\mathbf{B} \succeq \mathbf{A}$ which is Ω_i-saturated for every i.*

Proof. Recall the vocabulary $\overline{\tau}^{\mathbf{A}}$ which has a distinct constant c_a for each $a \in A$ and define the vocabulary τ^* by adding to $\overline{\tau}^{\mathbf{A}}$ distinct, fresh constants

$$d_0, d_1, \dots .$$

Fix an enumeration

$$\chi_0, \chi_1, \cdots$$

of all the τ^*-sentences. We also fix a doubly-indexed enumeration

$$\vec{d}^{\,i,0}, \vec{d}^{\,i,1}, \dots , \quad (i = 0, 1, \dots)$$

of all finite sequences (of distinct elements) from $\{d_0, d_1, \dots\}$, such that the length of each $\vec{d}^{\,i,j}$ is m_i, the "parameter length" of the pretype Ω_i.

Lemma. There is a sequence

$$S_0, S_1, \dots$$

of sets of τ^*-sentences so that the following hold:

(1) $S_0 = \mathrm{EDiagram}(\mathbf{A})$*, and for each k, $S_k \subseteq S_{k+1}$.*
(2) *For each k, only finitely many of the fresh constants $d_0, d_1, \dots$ occur in the sentences of S_k.*
(3) *For each k, the theory S_k is consistent.*
(4) *For each n, either $S_{3n} = S_{3n-1} \cup \{\chi_n\}$ or $S_{3n} = S_{3n-1} \cup \{\neg\chi_n\}$ (with $S_{-1} = \emptyset$ at the basis).*
(5) *For each n, if $S_{3n} \setminus S_{3n-1} = \{\exists u \sigma(u)\}$, then $S_{3n+1} = S_{3n} \cup \{\sigma(d_i)\}$ for some i such that the fresh constant d_i does not occur in S_{3n}; otherwise $S_{3n+1} = S_{3n}$.*
(6) *For each n not of the form $2^i 3^j$, $S_{3n+2} = S_{3n+1}$.*

   If $n = 2^i 3^j$ for some (uniquely determined) i, j, let $d_{\ell_1}, \dots , d_{\ell_{n_i}}$ be a sequence of distinct fresh constants which do not occur in any of the sentences in S_{3n+1} and set

$$S' = S_{3n+1} \cup \{\omega_{i,s}(\vec{d}^{\,i,j}, d_{\ell_1}, \dots , d_{\ell_{n_i}}) \mid s = 0, 1, \dots \}.$$

   If S' is consistent, then $S_{3n+2} = S'$, otherwise $S_{3n+2} = S_{3n+1}$.

Proof of the Lemma is quite routine by the methods we have been using and we will omit the details. (The only thing that needs to be verified is that at each stage of the construction, we only add finitely many fresh constants to S_k, and we keep it consistent.) ⊣ (Lemma)

With familiar arguments, we can also verify that that the set

$$H = \bigcup_k S_k$$

is a Henkin set, and that there is a structure **B** with universe

$$B = \{\overline{d}_0, \overline{d}_1, \dots\}$$

all of whose members are named by the fresh constants we added and such that

$$\mathbf{B} \models \chi \iff \chi \in H.$$

Moreover, $\mathbf{B} \models \text{EDiagram}(\mathbf{A})$, so we may assume that it is an elementary extension of **A** by Lemma 2A.3. It remains to check that it realizes every

$$\Omega_i^{\vec{d}^{i,j}}(v_1, \dots, v_{n_i}) = \{\omega_{i,0}(\vec{d}^{i,j}; \vec{v}), \omega_{i,1}(\vec{d}^{i,j}; \vec{v}), \dots\}$$

which is finitely satisfiable. To check this, suppose that $\Omega_i^{\vec{d}^{i,j}}(v_1, \dots, v_{n_i})$ is finitely satisfiable and consider the set S' defined in stage $n = 3(2^i 3^j)$ of the construction. If S' is not consistent, then

$$S_{3n+1} \vdash \neg \bigwedge\!\!\!\bigwedge_{s \leq N} \omega_s(\vec{d}^{i,j}, d_{\ell_1}, \dots, d_{\ell_{n_i}}),$$

and since the constants $d_{\ell_1}, \dots, d_{\ell_{n_i}}$ do not occur in S_{3n+1}, we have

$$S_{3n+1} \vdash (\forall \vec{v}) \neg \bigwedge\!\!\!\bigwedge_{s \leq N} \omega_s(\vec{d}^{i,j}, \vec{v});$$

but then

$$\mathbf{B} \models (\forall \vec{v}) \neg \bigwedge\!\!\!\bigwedge_{s \leq N} \omega_s(\vec{d}^{i,j}, \vec{v})$$

which means that $\Omega_i^{\vec{d}^{i,j}}(v_1, \dots, v_{n_i})$ is not finitely satisfiable, contrary to hypothesis. We conclude that S' is consistent, so $H \supseteq S_{3n+2} = S'$, hence $\mathbf{B} \models S'$—and this says precisely that the tuple $d_{\ell_1}, \dots, d_{\ell_{n_i}}$ realizes $\Omega_i^{\vec{d}^{i,j}}(v_1, \dots, v_{n_i})$ in **B**. ⊣

2D. Back-and-forth games

In this section we will consider only **finite, relational** vocabularies, i.e., finite τ's with no function symbols—but notice that we allow constants and, in fact, much of what we will do will involve adding to and removing constants from the vocabulary. To simplify the statements of results, we will also admit (as in 1F.2) the **propositional constants** T, F standing for *truth* and *falsity*, so that there will always be *quantifier free τ-sentences* (T and F), even if τ has no constants.

Notice that if τ is relational and $\mathbf{A}$ is a τ-structure, then the substructure $\langle X\rangle_{\mathbf{A}}$ generated by $X \subseteq A$ (as in Problem x2.6) has universe the set $X \cup \{c^{\mathbf{A}} \mid c \in \text{Const}\}$ and, in particular, it is finite if X is finite. An isomorphism

$$\pi : \langle X\rangle_{\mathbf{A}} \to \langle Y\rangle_{\mathbf{B}}$$

is completely determined by the values $x \mapsto \pi(x)$ for $x \in X$, since it must satisfy $\pi(c^{\mathbf{A}}) = c^{\mathbf{B}}$ for every constant— and so we will be specifying such isomorphisms by giving only the values $\pi(x)$ for $x \in X$.

Definition 2D.1. Given two τ-structures $\mathbf{A}, \mathbf{B}$ and a number $k \in \mathbb{N}$, the **Ehrenfeucht-Fraïsse game** $G_k(\mathbf{A}, \mathbf{B})$ is played by two players called $\forall$ (Abelard, or the first player I) and $\exists$ (Eloise, or the second player II).

If $k = 0$, then there are no moves and $\exists$ wins if the map $c^{\mathbf{A}} \mapsto c^{\mathbf{B}}$ is an isomorphism of the (finite) substructures of $\mathbf{A}$ and $\mathbf{B}$ determined by the constants, which simply means that for any two constants c_1, c_2,

$$c_1^{\mathbf{A}} = c_2^{\mathbf{A}} \iff c_1^{\mathbf{B}} = c_2^{\mathbf{B}}, \tag{40}$$

and for each n-ary relation symbol R and any n (not necessarily distinct) constants $c_1, \dots, c_n$,

$$R^{\mathbf{A}}(c_1^{\mathbf{A}}, \dots, c_n^{\mathbf{A}}) \iff R^{\mathbf{B}}(c_1^{\mathbf{B}}, \dots, c_n^{\mathbf{B}}); \tag{41}$$

if there are no constants in τ, then $\exists$ wins (by default). In either case, the game $G_0(\mathbf{A}, \mathbf{B})$ does not involve any moves—it ends before it even gets started.

If $k > 0$, then the game $G_k(\mathbf{A}, \mathbf{B})$ has k *rounds*, and each of these rounds has two *moves*, one by each of the players. The player $\forall$ moves first in each round i (for $i = 1, \dots, k$) and chooses one of the two structures and a point x in that structure; then $\exists$ responds by choosing a point y in the other structure, so that the two moves together determine points $a_i \in A$ and $b_i \in B$. In more detail, the two possibilities are that $\forall$ chooses $(\mathbf{A}, a_i)$ with $a_i \in A$ and $\exists$ responds with some $b_i \in B$, *or* $\forall$ chooses $(\mathbf{B}, b_i)$ with $b_i \in B$ and $\exists$ responds with some $a_i \in A$. At the end of the k-th round, the players have together determined two finite sequences

$$\vec{a} = (a_1, \dots, a_k) \text{ and } \vec{b} = (b_1, \dots, b_k);$$

now $\exists$ wins if the map $a_i \mapsto b_i$ is an isomorphism of $\langle a_1, \dots, a_k\rangle_{\mathbf{A}}$ with $\langle b_1, \dots, b_k\rangle_{\mathbf{B}}$, otherwise $\forall$ wins.

Notice. This is a *game of perfect information*, i.e., each player can see all the choices (by both players) in previous moves; this will be used heavily in the proofs below.

A **strategy for** $\forall$ in $G_k(\mathbf{A}, \mathbf{B})$ is a function defined on pairs

$$(a_1, \dots, a_{i-1}; b_1, \dots, b_{i-1})$$

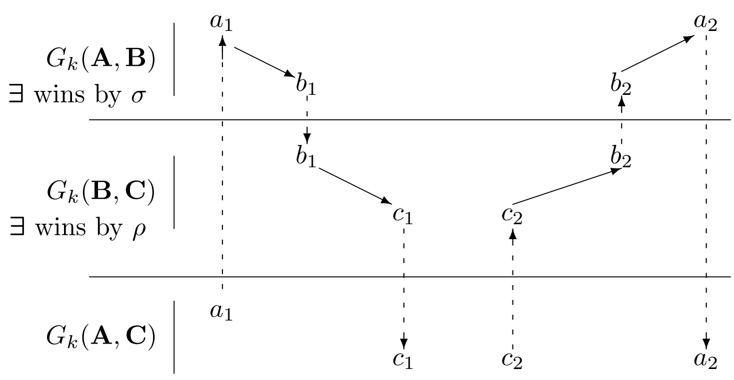


Figure 1. The first two moves in Case (3a)

of finite sequences of length $i < k$ (including $i = 0$) which instructs $\forall$ how to make his i'th move, i.e., which structure and which x in that structure to choose; and a **strategy for** $\exists$ is a function defined on sequences of the form

$$(a_1, \dots, a_{i-1}; b_1, \dots, b_{i-1}; (\mathbf{A}, x)) \qquad \text{and } (a_1, \dots, a_{i-1}; b_1, \dots, b_{i-1}; (\mathbf{B}, y))$$

which instructs $\exists$ how to make her i'th move, i.e., which element of the "the other" structure to choose. A strategy for either player is **winning** if that player wins when he plays by it, against all possible plays by the opponent.

Finally, we set

$$\mathbf{A} \sim_k \mathbf{B} \iff \exists \text{ has a winning strategy in } G_k(\mathbf{A}, \mathbf{B}). \tag{42}$$

Proposition 2D.2. *For all τ-structures and all k:*

(1) $\mathbf{A} \sim_k \mathbf{A}$.
(2) *If* $\mathbf{A} \sim_k \mathbf{B}$*, then* $\mathbf{B} \sim_k \mathbf{A}$.
(3) *If* $\mathbf{A} \sim_k \mathbf{B}$ *and* $\mathbf{B} \sim_k \mathbf{C}$*, then* $\mathbf{A} \sim_k \mathbf{C}$.

Proof. (1) $\exists$ wins $G_k(\mathbf{A}, \mathbf{A})$ by *copying* $\forall$'s moves, i.e., responding to $\forall$'s $(\mathbf{A}, x)$ by x. At the end of the game we have the identity function $a_i \mapsto a_i$, which is certainly an isomorphism of $\langle \vec{a} \rangle_{\mathbf{A}}$ with $\langle \vec{a} \rangle_{\mathbf{A}}$.

(2) If $\exists$ wins $G_k(\mathbf{A},\mathbf{B})$ using a strategy σ, then she also wins $G_k(\mathbf{B},\mathbf{A})$ using exactly the same σ—this is because these games are completely symmetric, both in the types of moves that they allow and in the conditions for winning.

(3) If $\exists$ wins $G_k(\mathbf{A},\mathbf{B})$ using a strategy σ and also wins $G_k(\mathbf{B},\mathbf{C})$ using ρ, then she can win $G_k(\mathbf{A},\mathbf{C})$ by combining the two strategies as follows, in each round i:

> (3a) If $\forall$ moves $(\mathbf{A}, a_i)$ in $G_k(\mathbf{A},\mathbf{C})$, then $\exists$ pretends that $\forall$ made this move in $G_k(\mathbf{A},\mathbf{B})$, and her strategy σ gives her a move $b_i \in B$; she then pretends that $\exists$ played $(\mathbf{B}, b_i)$ in $G_k(\mathbf{B},\mathbf{C})$, and her strategy ρ gives her a move $c_i \in C$; so she responds to $(\mathbf{A}, a_i)$ in $G_k(\mathbf{A},\mathbf{C})$ by this c_i.
>
> (3b) Symmetrically, if $\forall$ moves $(\mathbf{C}, c_i)$ in $G_k(\mathbf{A},\mathbf{C})$, then $\exists$ pretends that $\forall$ made this move in $G_k(\mathbf{B},\mathbf{C})$, and her strategy ρ gives her a move $b_i i \in B$; she then pretends that $\exists$ played $(\mathbf{B}, b_i)$ in $G_k(\mathbf{A},\mathbf{B})$, and her strategy σ gives her a move $a_i \in A$; so she responds to $(\mathbf{C}, c_i)$ in $G_k(\mathbf{A},\mathbf{C})$ by this a_i.

Figure 1 illustrates how the first two moves of $\exists$ in $G_k(\mathbf{A},\mathbf{C})$ are computed using the given winning strategies in $G_k(\mathbf{A},\mathbf{B})$ and $G_k(\mathbf{B},\mathbf{C})$, and assuming that $\forall$ moved $(\mathbf{A}, a_1)$ (Case (3a)) in the first round and then $(\mathbf{C}, c_2)$ (Case (3b)) in round 2. We use dashed arrows to indicate copying and solid arrows to indicate responses by the relevant winning strategy.

At the end of the k rounds, three sequences of elements are determined,

$$a_1, \dots, a_k \in A; \quad b_1, \dots, b_k; \text{ and } c_1, \dots, c_k,$$

and since $\exists$ wins both *simulated games* $G_k(\mathbf{A},\mathbf{B})$ and $G_k(\mathbf{B},\mathbf{C})$ (since she is playing in these with winning strategies), we have that

$$a_i \mapsto b_i \text{ is an isomorphism of } \langle \vec{a} \rangle_{\mathbf{A}} \text{ with } \langle \vec{b} \rangle_{\mathbf{B}}$$
$$\text{and } b_i \mapsto c_i \text{ is an isomorphism of } \langle \vec{b} \rangle_{\mathbf{B}} \text{ with } \langle \vec{c} \rangle_{\mathbf{C}},$$

whence $a_i \mapsto c_i$ is an isomorphism of $\langle \vec{a} \rangle_{\mathbf{A}}$ with $\langle \vec{c} \rangle_{\mathbf{C}}$. $\dashv$

Thus $\sim_k$ is an equivalence relation on the class of all τ-structures. The next (basic) property of this equivalence relation involves changing the vocabulary by adding a constant, and it is useful to introduce (temporarily) a notation which makes clear the vocabulary in which we are working:

$$\mathbf{A} \sim_{k,\tau} \mathbf{B} \iff \mathbf{A},\mathbf{B} \text{ are } \tau\text{-structures and } \mathbf{A} \sim_k \mathbf{B}.$$

Recall that we indicate by (τ, c) the expansion of τ by a fresh constant c, and by $(\mathbf{A}, x)$ the expansion of the τ-structure $\mathbf{A}$ to the (τ, c)-structure in which the new constant c is interpreted by x.

Proposition 2D.3. *For any two τ-structures $\mathbf{A}, \mathbf{B}$ and any k,*

$$(43)\quad \mathbf{A} \sim_{k+1,\tau} \mathbf{B} \iff (\forall x \in A)(\exists y \in B)[(\mathbf{A}, x) \sim_{k,(\tau,c)} (\mathbf{B}, y)] \\ \text{and } (\forall y \in B)(\exists x \in A)[(\mathbf{A}, x) \sim_{k,(\tau,c)} (\mathbf{B}, y)].$$

Proof is almost immediate from the definition of the game, with the two conjuncts on the right corresponding to the two kinds of first moves that $\forall$ can make. We will omit the details. ⊣

(In quoting this Proposition we will often skip the embellishments which specify the expansion in the vocabulary, as it is determined by the reference to the expanded structures $(\mathbf{A}, x)$ and $(\mathbf{B}, y)$.)

For our first application of Ehrenfeucht-Fraïsse games, we need to define "quantifier depth".

Definition 2D.4. The **quantifier depth** $\mathrm{qd}(\phi)$ of each formula ϕ is defined by the structural recursion

$$\mathrm{qd}(T) = \mathrm{qd}(F) = \mathrm{qd}(\text{prime formula}) = 0,\ \mathrm{qd}(\neg\phi) = \mathrm{qd}(\phi),$$
$$\mathrm{qd}(\phi \ \&\ \psi) = \mathrm{qd}(\phi \vee \psi) = \mathrm{qd}(\phi \rightarrow \psi) = \max(\mathrm{qd}(\phi), \mathrm{qd}(\psi)),$$
$$\mathrm{qd}(\exists v\phi) = \mathrm{qd}(\forall v\phi) = \mathrm{qd}(\phi) + 1.$$

Theorem 2D.5. *If $\mathbf{A}, \mathbf{B}$ are two τ-structures and $\mathbf{A} \sim_k \mathbf{B}$, then for every sentence θ with $\mathrm{qd}(\theta) \leq k$,*

$$\mathbf{A} \models \theta \iff \mathbf{B} \models \theta.$$

Proof is by induction on k, simultaneously for all (finite, relational) vocabularies τ.

Basis, $k = 0$, in which case the sentences with quantifier depth 0 are exactly the quantifier-free sentences in which only the constants occur. If $\mathbf{A} \sim_0 \mathbf{B}$, then the map

$$\{c^{\mathbf{A}} \mapsto c^{\mathbf{B}} \mid c \text{ a constant of } \tau\}$$

is an isomorphism of the substructures determined by (the interpretations of) the constants, and this says exactly that quantifier-free sentences have the same truth value in both structures. (This is the empty map if τ has no constants, but then θ is one of T or F, so the conclusion is trivial.)

Induction step. We assume the result for k and also that $\mathbf{A} \sim_{k+1} \mathbf{B}$, so that the right-hand-side of (43) holds. Suppose (first) that

$$\theta \equiv \exists v\phi(v)$$

with $\mathrm{qd}(\phi(v)) = k$ and compute, with a fresh constant c:

$$\begin{aligned}
\mathbf{A} \models \theta &\Longrightarrow \mathbf{A} \models \exists v\phi(v)\\
&\Longrightarrow \text{ there exists some } x \in A \text{ such that } (\mathbf{A}, x) \models \phi(c)\\
&\Longrightarrow \text{ there exists some } y \in B \text{ such that } (\mathbf{B}, y) \models \phi(c)\\
&\Longrightarrow \mathbf{B} \models \exists v\phi(v).
\end{aligned}$$

In the crucial step of this computation (changing from $(\mathbf{A}, x)$ to $(\mathbf{B}, y)$), we appealed to the right-hand-side of (2D.3) which gives us a y such that

$$(\mathbf{A}, x) \sim_k (\mathbf{B}, y)$$

and then to the induction hypothesis. The same argument (using the other half of the right-hand-side of (43)) shows that

$$\mathbf{B} \models \exists v\phi(v) \Longrightarrow \mathbf{A} \models \exists v\phi(v),$$

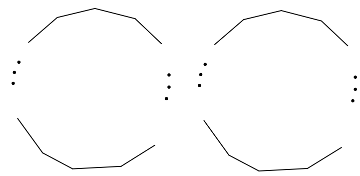
and then the argument is completed trivially for propositional combinations of sentences of quantifier depth $k + 1$ and sentences $\forall v\phi(v)$, which are equivalent to $\neg\exists v\neg\phi$. ⊣

The converse of this Proposition is also true, but it is worth deriving first an important

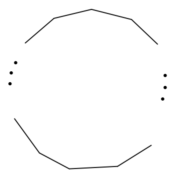
Corollary 2D.6. *There is no sentence χ in the vocabulary $\mathbb{FOL}(E)$ of graphs, such that for every finite, symmetric graph $\mathbf{G} = (G, E)$,*

$$\mathbf{G} \textit{ is connected } \iff \mathbf{G} \models \chi.$$

Outline of proof. It is enough to construct for each $k \geq 1$, two finite graphs $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A} \sim_k \mathbf{B}$ but $\mathbf{B}$ is connected while $\mathbf{A}$ is not, and here they are:



A: two cycles with 2^{2k} nodes each.



B: one cycle with 2^{2k} nodes.

1. **B** is a simple cycle with 2^{2k} nodes.
2. **A** comprises two simple cycles, each with 2^{2k} nodes.

By the *interval* $[x, y]$ *from* x *to* y in one of these graphs we will mean the set of nodes in the shorter of the two paths joining x to y (assuming that one such shorter path exists), without any implication that “x is less than y” in some sense or other.

To prove that $\mathbf{A} \sim_k \mathbf{B}$, suppose first that

$$a_1, \ldots, a_m \in A, \quad b_1, \ldots, b_m \in B$$

with $m, \ell \leq k$. We say that the pair of sequences

$$(\vec{a}; \vec{b}) = (a_1, \ldots, a_m; b_1, \ldots, b_m)$$

is *ℓ-good* if the following conditions are satisfied:

(1) The map $a_i \mapsto b_i$ is an isomorphism of $\langle \vec{a} \rangle_{\mathbf{A}}$ with $\langle \vec{b} \rangle_{\mathbf{B}}$.
(2) If $d(a_i, a_j) \leq 2^\ell$, then $d(b_i, b_j) = d(a_i, a_j)$.
(3) If $d(b_i, b_j) \leq 2^\ell$, then $d(a_i, a_j) = d(b_i, b_j)$.

Notice that $(\vec{a}; \vec{b})$ is 0-good exactly when (1) holds, since (2) and (3) say exactly the same thing as (1) when $\ell = 0$ (and $2^\ell = 1$).

Lemma. If $m < k, 0 < \ell \leq k$ and $(\vec{a}; \vec{b})$ is ℓ-good, then:

(a) *For each $x \in A$, there is a $y \in B$, such that $(\vec{a}, x; \vec{b}, y)$ is $\ell - 1$-good.*
(b) *For each $y \in B$, there is an $x \in A$, such that $(\vec{a}, x; \vec{b}, y)$ is $\ell - 1$-good.*

Proof. We assume the hypothesis and prove (a), the proof of (b) being the same.

Let

$$S_A = \{x \in A \mid \text{for some } j, d(x, a_j) \leq 2^{\ell-1}\},$$
$$S_B = \{y \in B \mid \text{for some } j, d(y, b_j) \leq 2^{\ell-1}\}$$

and consider the following possibilities for any given $x \in A$.

Case 1: $x \in S_A$, and there exist a_i, a_j such that

$$d(a_i, a_j) \leq 2^\ell,$$

x is on the shortest path from a_i to a_j and there is no other a_s on this path.

Now by ℓ-goodness, $d(b_i, b_j) = d(a_i, a_j)$ and there is a one-to-one correspondence between the intervals $[a_i, a_j]$ in $\mathbf{A}$ and $[b_i, b_j]$ in $\mathbf{B}$. This specifies a unique y in $[b_i, b_j]$ which we can associate with x, which is what we do, and it is easy to verify that the pair $(\vec{a}, x; \vec{b}, y)$ is $\ell - 1$-good.

Case 2: $x \in S_A$ but Case 1 does not hold. This means that if a_i is closest to x, then $d(a_i, x) \leq 2^{\ell-1}$ and there is no a_j such that x is in the interval $[a_i, a_j]$ and $d(a_i, a_j) \leq 2^\ell$.

The hypothesis now implies that in one direction starting from b_i, there is no b_j such that $d(b_i, b_j) \leq 2^\ell$; because if we had $d(b_i, b_j) \leq 2^\ell$ and also $d(b_i, b_s) \leq 2^\ell$, then there is a one-to-one correspondence between the intervals $[a_i, a_j]$ and $[b_i, b_j]$ and also between the intervals $[a_i, a_s]$ and $[b_i, b_s]$ and so the picture is like this:

$$a_j \cdots a_i \cdots a_s \text{ with } d(a_j, a_i), d(a_i, a_s) \leq 2^\ell;$$

moreover, x must lie in one of the intervals $[a_j, a_i]$, $[a_i, a_s]$ (because if it were outside both then either a_j or a_s would be closer to it than a_i), and this contradicts the Case Hypothesis. So we now associate with x the unique t at a distance $d(a_i, x)$ from b_i, in the direction which is free of b_j's for more than 2^ℓ nodes, and we can verify that the pair $(\vec{a}, x; \vec{b}, y)$ is $\ell - 1$-good.

Case 3: $x \notin S_A$. In this case it is enough to prove that there is some $y \notin S_B$, since it is easily verified that for any such y, the pair $(\vec{a}, x; \vec{b}, y)$ is $\ell - 1$-good. To see this, notice that

$$S_B = \bigcup_{j=1}^m \{y \mid d(y, b_j) \leq 2^{\ell-1}\},$$

and since the number of nodes in each $\{y \mid d(y, b_j) \leq 2^{\ell-1}\}$ is no more that 2^ℓ, the number of members of S_B is no more than $m \cdot 2^\ell < k2^k \leq 2^{2k}$. It follows that S_B cannot exhaust B which has 2^{2k} elements, which completes the proof of (a). ⊣ (Lemma)

To prove the theorem, we start with the trivial fact that

$$(\emptyset; \emptyset) \text{ is } k\text{-good},$$

and we use the Lemma to define a strategy for $\exists$ in $G_k(\mathbf{A}, \mathbf{B})$—i.e., $\exists$ moves in every round the $y \in B$ given by (a) if $\forall$ moves some $x \in A$, and the $x \in A$ given by (b) if $\forall$ moves some $y \in B$. We have successively that

$$(a_1; b_1) \text{ is } k-1\text{-good}, \ (a_1, a_2; b_1, b_2) \text{ is } k-2\text{-good}, \\ \dots, (a_1, \dots, a_k; b_1, \dots, b_k) \text{ is } 0\text{-good},$$

and so $\exists$ wins, since 0-goodness insures that the map $a_i \mapsto b_i$ is an isomorphism. ⊣

The proof of this result is the archetype of many arguments in **Finite Model Theory**, which is burgeoning, partly because of its relevance to theoretical computer science.

We now turn to the proof of the converse of Theorem 2D.5, for which we need two lemmas:

Lemma 2D.7. *For each* (finite, relational) *vocabulary τ and each k, there are only finitely many equivalence classes of the relation $\sim_{k,\tau}$.*

Proof. If τ has s constants $c_1, \dots, c_s$ and t relation symbols $R_1, \dots, R_t$ of respective arities $n_1, \dots, n_t$, then the $\sim_{0,\tau}$ equivalence class of a τ-structure $\mathbf{A}$ is determined by the set

$$(44) \quad G(\mathbf{A} = \{(i,j) \mid 1 \leq i, j \leq m \text{ and } c_i^{\mathbf{A}} = c_j^{\mathbf{A}}\} \\ \cup \bigcup_{i=1}^t \{(c_{m_1}, \dots, c_{m_{n_i}}) \mid R^{\mathbf{A}}(c_{m_1}^{\mathbf{A}}, \dots, c_{m_{n_i}}^{\mathbf{A}})\}$$

which has no more than

$$\text{efn}(0, \tau) = 2^s \cdot s^{n_1} \cdots s^{n_t}$$

members; thus there are no more than $\text{efn}(0,\tau)$ equivalence classes of structures for the relation $\sim_{0,\tau}$.

Proceeding inductively, suppose there are $m \le \text{efn}(k,(\tau,c))$ equivalence classes for $\sim_{k,(\tau,c)}$, call them

$$E_1, \ldots, E_m,$$

and for each τ-structure $\mathbf{A}$, let

$$F(\mathbf{A}) = \{i \mid 1 \le i \le m \text{ and for some } x, (\mathbf{A}, x) \in E_i\}.$$

It is enough to prove that

$$F(\mathbf{A}) = F(\mathbf{B}) \iff \mathbf{A} \sim_{k+1,\tau} \mathbf{B}, \tag{45}$$

since that implies that there are no more than

$$2^m \le 2^{\text{efn}(k,(\tau,c)} = \text{efn}(k+1,\tau)$$

equivalence classes for $\sim_{k+1,\tau}$. But the direction $\Rightarrow$ of (45) is almost immediately a consequence of (43); because if $F(\mathbf{A}) = F(\mathbf{B})$, then for each $x \in A$, there is an $i \in F(\mathbf{A})$ such that the equivalence class of $(\mathbf{A}, x)$ is E_i; so that for some $y \in B$, the equivalence class of $(\mathbf{B}, y)$ is also E_i, in other words,

$$F(\mathbf{A}) = F(\mathbf{B}) \Longrightarrow (\forall x \in A)(\exists y \in B)[(\mathbf{A}, x) \sim_{k,(\tau,c)} (\mathbf{B}, y)],$$

which is half of the right-hand-side of (43), and the proof of the other half is basically the same.

The converse direction $\Leftarrow$ is also easy, by a similar appeal to (43). $\dashv$

The next Lemma is really a corollary of the proof of this one:

Lemma 2D.8. *For each τ and each k, there is a finite set*

$$\chi_1^{k,\tau}, \ldots, \chi_m^{k,\tau} \quad (m \le \text{efn}(k,\tau))$$

of τ-sentences of quantifier depth $\le k$, such that for each τ-structure $\mathbf{A}$, there is exactly one i such that with $\chi \equiv \chi_i^{k,\tau}$, the following hold:

(1) $\mathbf{A} \models \chi$.
(2) *For every τ-structure $\mathbf{B}$,*

$$\mathbf{B} \sim_{k,\tau} \mathbf{A} \iff \mathbf{B} \models \chi.$$

Proof is by induction on k, simultaneously for all signatures τ.

In general, we will construct the sentences $\chi_i^{k,\tau}$, such that for some enumeration $E_1, \ldots, E_m$ of the equivalence classes of $\sim_{k,\tau}$ as in the previous lemma,

$$\mathbf{A} \in E_i \iff \mathbf{A} \models \chi_i^{k,\tau}.$$

Basis, $k = 0$. Consider the finite set $G(\mathbf{A})$ associated with $\mathbf{A}$ in (44), which determines the $\sim_{0,\tau}$ equivalence class E_i of $\mathbf{A}$; for each of these sets, we simply write down a quantifier free sentence χ_i such that

$$\mathbf{A} \in E_i \iff \mathbf{A} \models \chi_i.$$

(If there are no constants, then there is only one $\sim_{0,\tau}$ equivalence class, since $\exists$ always wins, and we just set $\chi_1 \equiv T$).

Assume we have done this for k and the vocabulary (τ, c), and for each $S \subseteq \{1, \dots, m\}$ let

$$\chi_S \equiv \bigwedge\!\!\!\bigwedge_{i \in S} \exists v \chi_i^{k,(\tau,c)}(v) \ \&\ \forall v \bigvee\!\!\!\bigvee_{i \in S} \chi_i^{k,(\tau,c)}(v), \tag{46}$$

where $\chi_i^{k,(\tau,c)}(v)$ is the result of replacing the constant c in $\chi_i^{k,(\tau,c)}$ by the fresh variable v. These sentences all have quantifier depth $k+1$. There are only finitely many such χ_S (2^n of them) and we can enumerate them in some way to get the required result if we verify that for each $S \subseteq \{1, \dots, m\}$,

$$\mathbf{A} \models \chi_S \iff F(\mathbf{A}) = S \quad (S \subseteq \{1, \dots, m\}).$$

Proof of $\mathbf{A} \models \chi_S \Longrightarrow F(\mathbf{A}) = S$. Assume the hypothesis $\mathbf{A} \models \chi_S$ and let $1 \le i \le m$. If $i \in F(\mathbf{A})$, then by the definition there is some $x \in A$ such that $(\mathbf{A}, x) \in E_i$, and from the second conjunct of χ_S applied to this x we get a $j \in S$ such that $(\mathbf{A}, x) \models \chi_j^{k,(\tau,c)}$ and so $(\mathbf{A}, x) \in E_j$; but $(\mathbf{A}, x)$ can only belong to one equivalence class, and so $i = j \in S$. Conversely, if $i \in S$, then the first conjunct of χ_S gives us an x such that $(\mathbf{A}, x) \models \chi_i^{k,(\tau,c)}$, so that $(\mathbf{A}, x) \in E_i$ and $i \in F(\mathbf{A})$ by the definition.

The converse implication $F(\mathbf{A}) = S \Longrightarrow \mathbf{A} \models \chi_S$ is proved similarly and we leave it for an exercise. ⊣

As an immediate corollary of these two lemmas, we have:

Theorem 2D.9. *For any two τ-structures $\mathbf{A}, \mathbf{B}$,*

$$\mathbf{A} \sim_k \mathbf{B}$$
$$\iff \text{for every sentence } \theta \text{ with } \mathrm{qd}(\theta) \le k,\ [\mathbf{A} \models \theta \iff \mathbf{B} \models \theta].$$

In particular,

$$\mathbf{A} \equiv \mathbf{B} \iff \text{for every } k,\ \mathbf{A} \sim_k \mathbf{B}.$$

Next we consider the obvious, infinite version of Ehrenfeucht-Fraïsse games:

Definition 2D.10. Foe any two structures $\mathbf{A}, \mathbf{B}$ of the same (finite, relational) vocabulary τ, the **back-and-forth** game $G_\omega(\mathbf{A}, \mathbf{B})$ is played by the two players $\forall$ and $\exists$ exactly like the game $G_k(\mathbf{A}, \mathbf{B})$, except that it goes on forever. In each round $i = 1, \dots$, player $\forall$ moves first either $(\mathbf{A}, x)$

with $x \in A$ or $(\mathbf{B}, y)$ with $y \in B$ and $\exists$ responds with some $y \in B$ in the first case or with some $x \in A$ in the second; we set

$$a_i := x, \quad b_i := y,$$

and the game proceeds to the next round. At the end of time the two players together have determined an infinite sequence of pairs

$$(a_1, b_1), (a_2, b_2), \dots ,$$

and $\exists$ *wins if the mapping* $a_i \mapsto b_i$ *is an isomorphism of*

$$\langle \{a_i \mid i = 1, 2, \dots\} \rangle_{\mathbf{A}} \text{ with } \langle \{b_i, \mid i = 1, 2, \dots\} \rangle_{\mathbf{B}}.$$

We set

$$\mathbf{A} \sim_\omega \mathbf{B} \iff \exists \text{ has a winning strategy in } G_\omega(\mathbf{A}, \mathbf{B}),$$

and if $\mathbf{A} \sim_\omega \mathbf{B}$, we say that $\mathbf{A}$ and $\mathbf{B}$ are **back-and-forth equivalent**.

The basic properties of back-and-forth equivalence are very similar to the corresponding properties of $\sim_k$:

Proposition 2D.11. *For all τ-structures:*

(1) $\mathbf{A} \sim_\omega \mathbf{A}$.
(2) *If* $\mathbf{A} \sim_\omega \mathbf{B}$, *then* $\mathbf{B} \sim_\omega \mathbf{A}$.
(3) *If* $\mathbf{A} \sim_\omega \mathbf{B}$ *and* $\mathbf{B} \sim_\omega \mathbf{C}$, *then* $\mathbf{A} \sim_\omega \mathbf{C}$.
(4) *If* $\mathbf{A} \sim_\omega \mathbf{B}$, *then* $\mathbf{A} \sim_k \mathbf{B}$ *for every* k, *and hence* $\mathbf{A} \equiv \mathbf{B}$.
(5) *If* $\mathbf{A} \simeq \mathbf{B}$, *then* $\mathbf{A} \sim_\omega \mathbf{B}$.

Proof. (1) – (3) are proved exactly like the corresponding properties of the finite games in Proposition 2D.2, and (4) is obvious—$\exists$'s winning strategy in $G_\omega(\mathbf{A}, \mathbf{B})$ will also win every $G_k(\mathbf{A}, \mathbf{B})$ when we restrict it to the first k rounds. (5) is also trivial: $\exists$ uses the given isomorphism $\rho : \mathbf{A} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbf{B}$ and responds by $\rho(x)$ or $\rho^{-1}(y)$ in each round, depending on whether $\forall$'s move was in $\mathbf{A}$ or in $\mathbf{B}$. $\dashv$

Parts (4) and (5) of the proposition give us the implications

$$\mathbf{A} \simeq \mathbf{B} \Longrightarrow \mathbf{A} \sim_\omega \mathbf{B} \Longrightarrow \mathbf{A} \equiv \mathbf{B}. \tag{47}$$

The first of these is not reversible in general, because for infinite structures $(A), (B)$ with no primitives (trivially) $(A) \sim_\omega (B)$ while $(A) \not\simeq (B)$ if A is countable and B is uncountable. It is perhaps surprising that the converse holds for countable structures:

Theorem 2D.12. *For countable structures* $\mathbf{A}, \mathbf{B}$ *of the same finite, relational vocabulary,*

$$\mathbf{A} \sim_\omega \mathbf{B} \iff \mathbf{A} \simeq \mathbf{B}.$$

PROOF. For the $\Rightarrow$ direction that we have not yet proved, fix enumerations

$$A = \{x_0, x_1, \dots\}, \quad B = \{y_0, y_1, \dots\}$$

of the two structures, perhaps with repetitions (which cannot be avoided if one of them is finite), and consider a run of $G_\omega(\mathbf{A}, \mathbf{B})$ in which $\exists$ plays by her winning strategy and $\forall$ plays

$$a_{2j+1} = x_j, \quad b_{2j+2} = y_j \qquad (j = 0, 1, \dots);$$

the resulting play gives an isomorphism $a_i \mapsto b_i$ of the substructures $\langle A' \rangle_{\mathbf{A}}$ and $\langle B' \rangle_{\mathbf{B}}$ with

$$A' = \{a_1, a_2, \dots, \}, \quad B' = \{b_1, b_2, \dots\},$$

since $\exists$ wins; but $A' = A$ and $B' = B$, since $\forall$ moves x_j in round $2j+1$ and y_j in round $2j+2$. $\dashv$

2E. $\exists^1_1$ on countable structures

Recall the language $\mathbb{FOL}^2$ of second order logic defined in Section 1K.3. Our aim in this section is to establish an interesting *game representation* for $\exists^1_1$ formulas and relations on countable structures, which becomes especially useful when the structure is sufficiently saturated. We restrict ourselves again to relational signatures (with no function symbols).

Proposition 2E.1 ($\exists^1_1$ Normal Form). *Every $\exists^1_1$, τ-formula ϕ is logically equivalent with a $\exists^1_1$-formula*

$$\phi^* \equiv \exists X_1 \exists X_2 \cdots \exists X_n \forall \vec{u}\, \exists \vec{v}\, \psi(\vec{u}, \vec{v}, X_1, \dots, X_n) \tag{48}$$

in which $\psi(\vec{u}, \vec{v}, X_1, \dots, X_n)$ is quantifier free.

PROOF. Notice first that for any relation $R(\vec{x}, \vec{y})$ on a set A,

$$\begin{aligned} &(\forall \vec{u})(\exists \vec{v}) R(\vec{x}, \vec{u}, \vec{v}) \\ &\quad \Longleftrightarrow (\exists X)\Big((\forall \vec{u})(\exists \vec{v}) X(\vec{u}, \vec{v}) \ \&\ (\forall \vec{u})(\forall \vec{v})[X(\vec{u}, \vec{v}) \Longrightarrow R(\vec{x}, \vec{u}, \vec{v})]\Big); \end{aligned} \tag{49}$$

this is immediate in the direction ($\Longleftarrow$), and direction ($\Longrightarrow$) follows by setting

$$X = \{(\vec{u}, \vec{v}) \mid R(\vec{x}, \vec{u}, \vec{v})\}.$$

This simple "poor man's Axiom of Choice" is often useful, and it is the key equivalence that we need here.

To prove the Proposition, it is clearly enough to find the appropriate ϕ^* when ϕ is elementary (with no relation quantifiers), since the full result follows then by adding a quantifier prefix $\exists X_1 \exists X_2 \cdots \exists X_n$ to both sides. Moreover, by bringing ϕ to prenex normal form and adding vacuous quantifiers (if necessary), we may assume that

$$\phi \equiv \forall \vec{u}_1 \, \exists \vec{v}_1 \, \forall \vec{u}_2 \, \exists \vec{v}_2 \cdots \forall \vec{u}_n \, \exists \vec{v}_n \psi(\vec{u}_1, \dots, \vec{v}_n) \tag{50}$$

where $\psi(\vec{u}_1, \dots, \vec{v}_n)$ is quantifier free. We will prove the result by induction on the number n of *quantifier alternations*, noticing that it is trivial when $n \leq 1$; so assume (50) and the Proposition for elementary formulas with no more than $n - 1 \geq 1$ quantifier alternations in prenex normal form, and apply (the formal version of) (49) to get

$$\begin{aligned} \phi \asymp \exists X \Big(& \forall \vec{u}_1 \, \exists \vec{v}_1 X(\vec{u}_1, \vec{v}_1) \\ & \& \; \forall \vec{u}_1 \, \forall \vec{v}_1 [X(\vec{u}_1, \vec{v}_1) \to \forall \vec{u}_2 \, \exists \vec{v}_2 \cdots \forall \vec{u}_n \, \exists \vec{v}_n \psi(\vec{u}_1, \dots, \vec{v}_n)] \Big). \end{aligned}$$

Now the formula on the second line of this equivalence can be put in prenex normal form by pulling the string of quantifiers $\forall \vec{u}_2 \, \exists \vec{v}_2 \cdots \forall \vec{u}_n \, \exists \vec{v}_n$ to the front, and then it has only $n - 1$ quantifier alternations; so the induction hypothesis supplies us an equivalence

$$\phi \asymp \exists X \Big(\forall \vec{u}_1 \, \exists \vec{v}_1 X(\vec{u}_1, \vec{v}_1) \; \& \; \exists X_1 \exists X_2 \cdots \exists X_m \forall \vec{z} \, \exists \vec{w} \psi^{**} \Big)$$

with ψ^{**} quantifier free, and we can finish the construction by pulling judicially the quantifiers up front in this:

$$\phi \asymp \exists X \exists X_1 \exists X_2 \cdots \exists X_m \forall \vec{u}_1 \, \forall \vec{z} \, \exists \vec{v}_1 \, \exists \vec{w} \psi^{**}. \qquad \dashv$$

Suppose

$$\theta \equiv \exists X_1 \exists X_2 \cdots \exists X_n \forall \vec{u} \, \exists \vec{v} \, \psi(\vec{u}, \vec{v}, X_1, \dots, X_n) \tag{51}$$

is an $\exists^1_1$ τ-sentence in normal form, where

$$\vec{u} \equiv u_1, \dots, u_k, \quad \vec{v} \equiv v_1, \dots, v_l$$

are tuples of variables of respective lengths k and l. With θ and each τ-structure $\mathbf{A}$ we associate an infinite, two-person game of perfect information, in which the two players $\exists$ and $\forall$ alternate moves as follows:

$$G(\mathbf{A}, \theta) : \quad \begin{array}{c|ccccccccc} \forall & x_0 & & x_1 & & \cdots & & x_i & & \cdots \\ & & & & & & & & & \\ \exists & & \mathbf{B}_0 & & \mathbf{B}_1 & & \cdots & & \mathbf{B}_i & & \cdots \end{array}$$

The rules for the game are:

(1) In each round i, $\forall$ moves first an arbitrary point $x_i \in A$ (and he may repeat the same move as often as he pleases).

(2) In each round i, $\exists$ responds by a finite structure

$$\mathbf{B}_i = (\mathbf{A}_i, X^i_1, \dots, X^i_n),$$

such that $\mathbf{A}_i \subseteq \mathbf{A}$, $x_i \in A_i$, and the arities of the extra relations $X^i_1, \dots, X^i_n$ match the arities of the relation variables $X_1, \dots, X_n$.

(3) For each $i+1$, $\exists$ must play so that $\mathbf{B}_i \subseteq \mathbf{B}_{i+1}$ and

$$\text{for all } \vec{u} \in A^k_i, \text{ there exists } \vec{v} \in A^l_{i+1} \text{ such that} \quad \mathbf{B}_{i+1} \models \psi[\vec{u}, \vec{v}, X^{i+1}_1, \dots X^{i+1}_n];$$

if this condition does not hold, then the game ends and $\forall$ is declared the winner.

If the game goes on forever without $\exists$ violating any of the rules, then she is declared the winner.

The rules of the game do not specify the size of the finite structures $\mathbf{B}_i$ that $\exists$ may play, but we can compute sufficiently large upper bounds for the size of these structure with which $\exists$ can win, if she can win at all. If K is the number of constants in the (relational) signature τ, set recursively:

$$\text{sb}_1 = K+2, \quad \text{sb}_{i+1} = \text{sb}_i + l\text{sb}^k_i. \tag{52}$$

(The proof of the next theorem requires only that $\text{sb}_1 \geq 1$, but insuring that $\text{sb}_1 \geq 2$ will be useful in a later computation.)

Theorem 2E.2. *Suppose* $\mathbf{A}$ *is a* τ*-structure and*

$$\theta \equiv \exists X_1 \exists X_2 \cdots \exists X_n \forall \vec{u}\, \exists \vec{v}\, \psi(\vec{u}, \vec{v}, X_1, \dots, X_n)$$

is an $\exists^1_1$ τ*-sentence in normal form.*

(1) *If* $\mathbf{A}$ *is infinite and* $\mathbf{A} \models \theta$*, then* $\exists$ *has a winning strategy in* $G(\mathbf{A}, \theta)$ *in which she plays so that for each* i*,* $|A_i| = \text{sb}_i$*.*

(2) *If* $\mathbf{A}$ *is countable and* $\exists$ *has a winning strategy in* $G(\mathbf{A}, \theta)$*, then* $\mathbf{A} \models \theta$*.*

Proof. (1) The hypothesis gives us relations $X_1, \dots, X_n$ so that

$$\mathbf{A} \models \forall \vec{u}\, \exists \vec{v}\, \psi(\vec{u}, \vec{v}, X_1, \dots, X_n),$$

and we will use these to define recursively a winning strategy for $\exists$.

In the first round, $\exists$ sets first

$$\mathbf{A}_1 = \mathbf{A} \restriction \{x_1, \bar{c}_1, \dots, \bar{c}_K, y_1, \dots, y_s\},$$

where $\bar{c}_1, \dots, \bar{c}_K$ are the interpretations of the τ-constants in $\mathbf{A}$ and $y_1, \dots, y_s$ are arbitrarily chosen, distinct members of A so that

$$|A_1| = |\{x_1, \bar{c}_1, \dots, \bar{c}_K, y_1, \dots, y_s\}| = K + 2 = \text{sb}_1;$$

she then completes her move by setting

$$X^1_j = X_j \restriction A_1 \quad (j = 1, \dots, n),$$

i.e., if X_j is m-ary,

$$X^1_j(t_1, \dots, t_m) \iff t_1, \dots, t_m \in A_1 \ \&\ X_j(t_1, \dots, t_m).$$

In the $(i+1)$'st round, $\exists$ has already played $\mathbf{B}_i$ with universe $B_i = A_i$, and the induction hypothesis guarantees that $|B_i| = \mathrm{sb}_i$, so that the number of k-tuples in B_i is sb_i^k. The hypothesis also gives us for each $\vec{u} \in B_i^k$ an l-tuple $\vec{v}_{\vec{u}} \in A^l$ such that

$$\mathbf{A} \models \psi[\vec{u}, \vec{v}_{\vec{u}}, X_1, \dots, X_n];$$

we set

$$A_{i+1} = A_i \cup \{\vec{v}_{\vec{u}} \mid \vec{u} \in A_i^k\} \cup \{z_1, \dots z_t\},$$

where $z_1, \dots z_t$ are (if needed) arbitrarily chosen, distinct members of A so that $|A_{i+1}| = \mathrm{sb}_i + l\mathrm{sb}_i^k = \mathrm{sb}_{i+1}$. Finally, we set

$$\mathbf{A}_{i+1} = \mathbf{A} \upharpoonright A_{i+1}, \quad X_j^{i+1} = X_j \upharpoonright A_{i+1} \quad (j = 1, \dots, n)$$

and we verify easily that this is a successful move by $\exists$. (Notice the use of the Axiom of Choice in this argument.)

(2) Assume now that $\mathbf{A}$ is countable and $\exists$ has a winning strategy in $G(\mathbf{A}, \theta)$, and consider the run of the game in which $\forall$ enumerates the universe

$$A = \{x_1, x_2, \dots\}$$

(perhaps with repetitions) and $\exists$ plays by her winning strategy. At the end we have a sequence of finite structures

$$(\mathbf{A}_1, X_1^1, \dots, X_n^1) \subseteq (\mathbf{A}_2, X_1^2, \dots, X_n^2) \subseteq \cdots,$$

and since $x_i \in A_i$, clearly $A_1 \cup A_2 \cup \cdots = A$. The "limit structure"

$$(\mathbf{A}, X_1, \dots, X_n) = \cup_{i=1}^{\infty} (\mathbf{A}_i, X_1^i, \dots, X_n^i)$$

determines relations

$$X_1 = \cup_{i=1}^{\infty} X_1^i, \dots, X_n = \cup_{i=1}^{\infty} X_n^i$$

such that $X_j^i = X_j \upharpoonright A_i$, for $i = 1, \dots, n$; and since $\exists$ wins the run,

$$\text{for all } \vec{u} \in A_i^k, \text{ there exists } \vec{v} \in A_{i+1}^l \text{ such that}$$
$$\mathbf{B}_{i+1} \models \psi[\vec{u}, \vec{v}, X_1^{i+1}, \dots X_n^{i+1}];$$

which implies immediately that

$$(\mathbf{A}, X_1, \dots, X_n) \models \forall \vec{u}\, \exists \vec{v}\, \psi(\vec{u}, \vec{v}, X_1, \dots, X_n)$$

and completes the proof. $\dashv$

Corollary 2E.3 (Game representation for $\exists_1^1$, I)**.** *If θ is an $\exists_1^1$ τ-sentence (with relational τ) and $\mathbf{A}$ is a countably infinite τ-structure, then*

$$\mathbf{A} \models \theta \iff \exists \textit{ has a winning strategy in } G(\mathbf{A}, \theta).$$

The satisfaction relation for $\exists_1^1$ sentences takes a very simple form on sufficiently saturated structures, and to prove this we need to code finite structures of the form $(\mathbf{A}_i, X_1^1, \dots, X_n^i)$ by tuples from A of specified length. The idea is simple but a bit messy, so it is best to illustrate it first in a simple case.

Suppose B is a finite subset of A with $m \geq 2$ members which contains all the denotations of the constants in $\mathbf{A}$, and suppose $Y \subseteq B^2$ is a binary relation on B. A **code** of the structure $(\mathbf{A} \upharpoonright B, Y)$ is any sequence

$$\beta = (b_1, \dots, b_m, s_1, t_1, s_1', s_2, t_2, s_2', \dots, s_{m^2}, t_{m^2}, s_{m^2}')$$

such that

(1) $B = \{b_1, \dots, b_m\}$, i.e., the first m terms of β enumerate B.
(2) $B^2 = \{(s_1, t_1), (s_2, t_2), \dots, (s_{m^2}, t_{m^2})\}$, i.e., $(s_1, t_1), \dots, (s_{m^2}, t_{m^2})$ is an enumeration of all the (ordered) pairs from B.
(3) For every pair (s_j, t_j),
$$Y(s_j, t_j) \iff s_j = s_j'.$$

It is clear that any code β of $(\mathbf{A} \upharpoonright B, Y)$ determines $(\mathbf{A} \upharpoonright B, Y)$, and that every finite structure of the form $(\mathbf{A} \upharpoonright B, Y)$ of size at least 2 has a code—we need at least two members to make sure that if $\neg Y(s_i, t_i)$, then we can find some $s_i' \neq s_i$ to code this fact by putting s_i, t_i, s_i' in β.

It is also clear that we can define in a similar (messier) way codes

$$\vec{z} = (z_1, z_2, \dots, z_o)$$

of arbitrary structures of the form $(\mathbf{A} \upharpoonright B, X_1, \dots, X_n)$ with $B \subseteq A$ any set of size $m \geq 2$ which includes the values of the constants, and $X_1, \dots, X_n$ any relations on B of arbitrary arities $m_1, \dots, m_n$; the length o of $\vec{z}$ is determined by the numbers $m, n, m_1, \dots, m_n$,

$$o = h(m, n, m_1, \dots, m_n), \tag{53}$$

e.g., in the simple example of one, binary extra relation treated in detail above, $o = h(m, 1, 2) = m + 3m^2$.

The idea is that we can express many properties of the structures $\mathbf{B}_{\vec{z}}$ by τ-formulas. To begin with:

(54) $(z_1, \dots, z_o)$ codes a finite structure $(\mathbf{A} \upharpoonright B, Y)$ with Y binary
$$\iff \bigvee\!\!\!\!\bigvee_{m<o}[1 < m < o \;\&\; o = h(m,1,2) \;\&\; \bigwedge\!\!\!\!\bigwedge_{c \in \mathrm{Const}} \bigvee\!\!\!\!\bigvee_{1<i\leq m}[c = z_i]$$
$$\& \; \bigwedge\!\!\!\!\bigwedge_{1 \leq i,j \leq m} \bigvee\!\!\!\!\bigvee_{s<3m^2}[z_i = z_{m+3s} \;\&\; z_j = z_{m+3s+1}]]$$

The general case is messier, but, in fact, the relation

$$\vec{z} \text{ codes a finite structure } \mathbf{B} = (\mathbf{A} \upharpoonright B, X_1, \dots, X_n) \tag{55}$$

is definable by a quantifier free τ-formula. So is the satisfaction relation for quantifier free formulas in these finite structures:

Lemma 2E.4. *Suppose τ is a relational signature and $\phi(\mathsf{w}_1, \dots, \mathsf{w}_k)$ is a quantifier free, full extended formula in the signature $(\tau, X_1, \dots, X_n)$ with n additional relation symbols of respective arities $m_1, \dots, m_n$. There is a full extended, quantifier free τ-formula $\phi^*(\vec{\mathsf{z}}, \vec{\mathsf{w}})$, such that for every infinite τ-structure $\mathbf{A}$ and $\vec{z}, \vec{w} \in A$,*

$$\vec{z} \text{ codes a finite structure } \mathbf{B}_{\vec{z}} = (\mathbf{A} \upharpoonright B, X_1, \dots, X_n) \text{ and } \mathbf{B}_{\vec{z}} \models \phi[\vec{w}] \iff \mathbf{A} \models \phi^*[\vec{z}, \vec{w}].$$

Proof. The required formula is a conjunction

$$\phi^*(\vec{\mathsf{z}}, \vec{\mathsf{w}}) \equiv \chi_1(\vec{\mathsf{z}}) \;\&\; \chi_2(\vec{\mathsf{z}}, \vec{\mathsf{w}}) \;\&\; \phi^{**}(\vec{\mathsf{z}}, \vec{\mathsf{w}}),$$

where:

(1) $\chi_1(\vec{\mathsf{z}})$ defines the relation "$\vec{z}$ codes a finite structure $\mathbf{B}_{\vec{z}}$", as in (55);
(2) $\chi_2(\vec{\mathsf{z}}, \vec{\mathsf{w}})$ defines the relation "$w_1, \dots, w_k$ are in the universe of $\mathbf{B}_{\vec{z}}$"; and
(3) $\phi^{**}(\vec{\mathsf{z}}, \vec{\mathsf{w}})$ is defined by structural recursion on the given $\phi(\vec{\mathsf{w}})$,

assuming, in the last case, that $\vec{z}$ codes a structure whose universe includes $w_1, \dots, w_k$. We will give the construction of $\phi^{**}(\vec{\mathsf{z}}, \vec{\mathsf{w}})$ only for the simple case of the example above, where $|B| = m,\ n = 1,\ m_1 = 2$, for which (by renaming variables) we may assume that

$$\vec{z} = (b_1, \dots, b_m, s_1, t_1, s_1', s_2, t_2, s_2', \dots, s_{m^2}, t_{m^2}, s_{m^2}').$$

The definition is trivial in all cases which do not involve the coding of the relation Y, e.g.,

$$R(\vec{\mathsf{w}})^{**} :\equiv R(\vec{\mathsf{w}}), \quad \Big(\neg\phi\Big)^{**} :\equiv \neg\phi^{**}, \quad \Big(\phi_1 \;\&\; \phi_2\Big)^{**} :\equiv \phi_1^{**} \;\&\; \phi_2^{**},$$

etc. In the interesting case,

$$Y(w_1, w_2)^{**} :\equiv \bigvee\!\!\!\bigvee_{1 \le i < m^2} [w_1 = s_i \;\&\; w_2 = t_i \;\&\; s_i = s_i']. \qquad \dashv$$

The game $G^s(\mathbf{A}, \theta)$ (^{s} for "sequential") associated with a τ-structure $\mathbf{A}$ and an $\exists^1_1$ τ-sentence θ is the obvious modification of $G(\mathbf{A}, \theta)$ in which $\exists$ moves *codes of finite structures* rather than actual finite structures. A run of it looks like

$$G^s(\mathbf{A}, \theta) : \quad \begin{array}{c|cccccccccc} \forall & x_0 & & x_1 & & \cdots & & x_i & & \cdots & \\ & & & & & & & & & & \\ \exists & & \vec{z}_0 & & \vec{z}_1 & & \cdots & & \vec{z}_i & & \cdots \end{array}$$

and the rules for the game are as follows:

(1) In each round i, $\forall$ moves first an arbitrary point $x_i \in A$ (and he may repeat the same move as often as he pleases).

(2) In each round i, $\exists$ responds by a finite sequence

$$\vec{z}_i = (z_1, \dots , z_{h(\mathrm{sb}_i, n, m_1, \dots , m_n)})$$

where h is the function in (53) above; now $\vec{z}$ codes a (unique) structure $\mathbf{B}_i = (\mathbf{A}_i, X^i_1, \dots , X^i_n)$ with $|A_i| = \mathrm{sb}_i$, and this must satisfy (2) in the rules for $G(\mathbf{A}, \theta)$.

(3) is the same as in the rules for $G(\mathbf{A}, \theta)$.

Directly from Corollary 2E.3, we get

Corollary 2E.5 (Game representation for $\exists^1_1$, II)**.** *If θ is an $\exists^1_1$ τ-sentence (with relational τ) and $\mathbf{A}$ is a countably infinite τ-structure, then*

$$\mathbf{A} \models \theta \iff \exists \text{ has a winning strategy in } G^s(\mathbf{A}, \theta).$$

The advantage of the "sequential" game $G^s(\mathbf{A}, \theta)$ is that its payoff can be (uniformly) defined in $\mathbb{FOL}(\tau)$, because its moves are sequences of elements:

Lemma 2E.6. *Suppose*

$$\theta \equiv \exists X_1 \exists X_2 \cdots \exists X_n \forall \vec{u}\, \exists \vec{v}\, \psi(\vec{u}, \vec{v}, X_1, \dots , X_n)$$

is a $\exists^1_1$ τ-sentence in normal form, with $\mathrm{arity}(X_j) = m_j$*. For each $i \geq 1$, there is a quantifier free, full extended τ-formula*

$$\theta_i(\mathsf{x}_1, \vec{\mathsf{z}}_1, \mathsf{x}_2, \vec{\mathsf{z}}_2, \dots , \mathsf{x}_i, \vec{\mathsf{z}}_i) \tag{56}$$

such that each $\vec{\mathsf{z}}_j$ is a tuple of variables of length $h(\mathrm{sb}_j, n, m_1, \dots , m_n)$, and for each τ-structure $\mathbf{A}$ and any $x_1, \vec{z}_1, x_2, \vec{z}_2, \dots , x_i, \vec{z}_i \in A$,

$$\begin{aligned} &\exists \text{ has followed the rules in the initial run}\\ &\qquad (x_1, \vec{z}_1, x_2, \vec{z}_2, \dots , x_i, \vec{z}_i) \text{ of } G^s(\mathbf{A}, \theta)\\ &\qquad\qquad \iff \mathbf{A} \models \theta_i[x_1, \vec{z}_1, x_2, \vec{z}_2, \dots , x_i, \vec{z}_i]. \end{aligned}$$

Proof is by appealing to and using the method of proof of Lemma 2E.4, and we will skip it. ⊣

For each $i \geq 1$, set

$$\omega_{0,i} :\equiv \forall \mathsf{x}_1 \exists \vec{\mathsf{z}}_1 \cdots \forall \mathsf{x}_i \exists \vec{\mathsf{z}}_i \theta_i(\mathsf{x}_1, \vec{\mathsf{z}}_1, \mathsf{x}_2, \vec{\mathsf{z}}_2, \dots , \mathsf{x}_i, \vec{\mathsf{z}}_i) \tag{57}$$

so that

$$\mathbf{A} \models \omega_{0,i} \iff \exists \text{ can follow the rules of } G^s(\mathbf{A}, \theta) \text{ for } i \text{ rounds.}$$

For each $n \geq 1$ and $i \geq n$, set also

$$\begin{aligned} &\omega_{n,i}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \dots , \mathsf{x}_{n-1}, \vec{\mathsf{z}}_{n-1}, \mathsf{x}_n; \vec{\mathsf{z}}_n)\\ &\qquad :\equiv \forall \mathsf{x}_{n+1} \exists \vec{\mathsf{z}}_{n+1} \cdots \forall \mathsf{x}_i \exists \vec{\mathsf{z}}_i \theta_i(\mathsf{x}_1, \vec{\mathsf{z}}_1, \mathsf{x}_2, \vec{\mathsf{z}}_2, \dots , \mathsf{x}_i, \vec{\mathsf{z}}_i), \end{aligned} \tag{58}$$

reading this so that when $i = n \geq 1$ it renames θ_n,

$$\omega_{n,n}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \dots , \mathsf{x}_{n-1}, \vec{\mathsf{z}}_{n-1}, \mathsf{x}_n; \vec{\mathsf{z}}_n) \equiv \theta_n(\mathsf{x}_1, \vec{\mathsf{z}}_1, \mathsf{x}_2, \vec{\mathsf{z}}_2, \dots , \mathsf{x}_n, \vec{\mathsf{z}}_n);$$

it follows that if $1 \leq n \leq i$, then

$$\begin{aligned}&\mathbf{A} \models \omega_{n,i}[x_1, \vec{z}_1, \ldots, x_{n-1}, \vec{z}_{n-1}, x_n; \vec{z}_n]\\ \iff &\exists \text{ has followed the rules in the first } n \text{ rounds of } G^s(\mathbf{A}, \theta)\\ &\qquad \text{and can continue playing following the rules up to round } i.\end{aligned}$$

Immediately from the definitions, we get

$$(59) \quad \models \omega_{n,i+1}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \ldots, \mathsf{x}_{n-1}, \vec{\mathsf{z}}_{n-1}, \mathsf{x}_n; \vec{\mathsf{z}}_n) \\ \rightarrow \omega_{n,i}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \ldots, \mathsf{x}_{n-1}, \vec{\mathsf{z}}_{n-1}, \mathsf{x}_n; \vec{\mathsf{z}}_n),$$

for $i \geq n \geq 1$, and for $i \geq n+1 \geq 1$,

$$(60) \quad \omega_{n,i}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \ldots, \mathsf{x}_n; \vec{\mathsf{z}}_n) \\ \equiv \forall \mathsf{x}_{n+1} \exists \vec{\mathsf{z}}_{n+1} \omega_{n+1,i}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \ldots, \mathsf{x}_n, \vec{\mathsf{z}}_n, \mathsf{x}_{n+1}; \vec{\mathsf{z}}_{n+1}).$$

Finally, we set

$$\Omega_0 = \{\omega_{0,1}, \omega_{0,2}, \ldots, \},$$

and for each $n \geq 1$,

$$(61) \quad \Omega_n(\mathsf{x}_1, \vec{\mathsf{z}}_1, \cdots, \mathsf{x}_n; \vec{\mathsf{z}}_n) \\ = \{\omega_{n,n}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \cdots, \mathsf{x}_n; \vec{\mathsf{z}}_n), \omega_{n,n+1}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \cdots, \mathsf{x}_n; \vec{\mathsf{z}}_n), \\ \omega_{n,n+2}(\mathsf{x}_1, \vec{\mathsf{z}}_1, \cdots, \mathsf{x}_n; \vec{\mathsf{z}}_n), \ldots \quad \}.$$

Note that Ω_0 is a theory, and we can think of it as a 0-0 partial pretype, while for $n \geq 1$, Ω_n is an m_1-m_2-partial pretype with m_1, m_2 determined by the given $\exists^1_1$ sentence θ.

Theorem 2E.7. *Suppose*

$$\theta \equiv \exists X_1 \exists X_2 \cdots \exists X_n \forall \vec{u} \exists \vec{v}\, \psi(\vec{u}, \vec{v}, X_1, \ldots, X_n)$$

is a $\exists^1_1$ τ-sentence in normal form, $\Omega_0, \Omega_1, \ldots$ are the partial pretypes associated with it, and $\mathbf{A}$ is a countably infinite τ-structure. Then

$$\mathbf{A} \models \theta \Longrightarrow \mathbf{A} \models \textstyle\bigwedge\!\!\!\bigwedge_i \omega_{0,i},$$

and if $\mathbf{A}$ is Ω_n-saturated for every n, then

$$\mathbf{A} \models \theta \iff \textstyle\bigwedge\!\!\!\bigwedge_i \omega_{0,i}.$$

Proof. Suppose first that $\mathbf{A} \models \theta$. It follows by Lemma 2E.5 that $\exists$ wins the game $G^s(\mathbf{A}, \theta)$, and so $\exists$ can follow the rules without losing for the entire game—in particular for the first i rounds; but this is exactly what $\mathbf{A} \models \omega_{0,i}$ says, and i was arbitrary.

For the converse implication under the additional hypothesis, we assume that $\mathbf{A}$ is Ω_n-saturated for every n and satisfies every $\omega_{1,i}$, and we describe a winning strategy for $\exists$ in $G^s)\mathbf{A}, \theta)$.

Suppose $\forall$ moves x_1 in round 1, and consider the partial type

$$\Omega_1^{x_1}(\vec{\mathsf{z}}_1) = \{\omega_{1,1}(x_1;\vec{\mathsf{z}}_1), \omega_{1,2}(x_1;\vec{\mathsf{z}}_1), \dots\}$$

of the structure $\mathbf{A}$. By (60) and the hypothesis $\mathbf{A} \models \omega_{0,i}$, we get that

$$\mathbf{A} \models \forall \mathsf{x}_1 \exists \vec{\mathsf{z}}_1 \omega_{1,i}(\mathsf{x}_1, \vec{\mathsf{z}}_1);$$

and when we apply this to the x_1 moved by $\forall$, we get some $\vec{z}_1^{\,i}$ such that

$$\mathbf{A} \models \omega_{1,i}[x_1, \vec{z}_1^{\,i}],$$

which by (59) implies that

$$\text{for every } j \leq i, \mathbf{A} \models \omega_{1,j}[x_1, \vec{z}_1^{\,i}].$$

Thus $\Omega_1^{x_1}$ is finitely satisfiable, hence realized by the hypothesis, and we have a single $\vec{z}_1$ such that

(62) $$\mathbf{A} \models \omega_{1,i}[x_1, \vec{z}_1] \qquad (1 \leq i);$$

in particular, $\mathbf{A} \models \theta_1[x_1, \vec{z}_1]$, and so $\exists$ can move z_1 and not lose on the first round.

We now proceed recursively to show how, for each n, $\exists$ can respond to $\forall$'s first n moves following the rules, and so that if $\forall$ moves some x_{n+1}, then the partial type

(63) $$\begin{aligned}\Omega_{n+1}^{x_1,\mathsf{z}_1,\dots,x_n,\mathsf{z}_n,x_{n+1}}&(\vec{\mathsf{z}}_{n+1})\\ = \{&\omega_{n+1,n+1}(\mathsf{x}_1,\vec{\mathsf{z}}_1,\cdots,\mathsf{x}_n,\vec{\mathsf{z}}_n,\mathsf{x}_{n+1};\vec{\mathsf{z}}_{n+1}),\\ &\omega_{n+1,n+2}(\mathsf{x}_1,\vec{\mathsf{z}}_1,\cdots,\mathsf{x}_n,\vec{\mathsf{z}}_n,\mathsf{x}_{n+1};\vec{\mathsf{z}}_{n+1}),\\ &\omega_{n,n+2}(\mathsf{x}_1,\vec{\mathsf{z}}_1,\cdots,\mathsf{x}_n,\vec{\mathsf{z}}_n,\mathsf{x}_{n+1};\vec{\mathsf{z}}_{n+1})\dots\quad\}\end{aligned}$$

is finitely satisfiable, hence realized; $\exists$ can then move some $\vec{z}_{n+1}$ which realizes it, and go on indefinitely without losing—hence, in the end, winning. $\dashv$

Recall from Section 1K.3 that a relation $P \subseteq A^k$ is $\exists_1^1$ in a τ-structure $\mathbf{A}$, if there is a full extended $\exists_1^1$ formula $\theta(\vec{\mathsf{y}})$ such that

(64) $$P(\vec{y}) \iff \mathbf{A} \models \theta[\vec{y}] \qquad (\vec{y} \in A^k).$$

Choose fresh constants $\vec{d} \equiv (d_1, \dots, d_k)$, and for each $\vec{x} \in A^k$, let $(\mathbf{A}, \vec{y})$ be the $(\tau, \vec{d})$ structure in which $\vec{d} := \vec{y}$, so that

(65) $$P(\vec{y}) \iff \mathbf{A} \models \theta[\vec{y}] \iff (\mathbf{A}, \vec{y}) \models \theta(\vec{d}).$$

Theorem 2E.8. *Suppose $\mathbf{A}$ is a countably infinite τ-structure and suppose $P \subseteq A^n$ is a $\exists_1^1$ relation on A, defined by* (64)*; it follows that*

$$\begin{aligned}P(\vec{x}) &\iff \exists \textit{ has a winning strategy in } G((\mathbf{A},\vec{x}),\theta(\vec{d}))\\ &\iff \exists \textit{ has a winning strategy in } G^s((\mathbf{A},\vec{x}),\theta(\vec{d})).\end{aligned}$$

Theorem 2E.7 has a similar interpretation for $\exists^1_1$ relations on sufficiently saturated structures:

Theorem 2E.9. *Suppose τ is a relational signature and $\theta(\vec{\mathsf{y}})$ is a full extended $\exists^1_1$ τ-formula; then there is a sequence*

$$\Omega^\theta_n(\vec{\mathsf{y}}, \mathsf{x}_1, \vec{\mathsf{z}}_1, \cdots, \mathsf{x}_n; \vec{\mathsf{z}}_n) \quad (n \geq 0)$$

of partial pretypes, such that if $\mathbf{A}$ is a countably infinite structure which is Ω^θ_n-saturated for every n, then

$$\mathbf{A} \models \theta[\vec{y}] \iff \mathbf{A} \models \bigwedge\!\!\!\bigwedge \Omega^\theta[\vec{y}].$$

It follows that if $\mathbf{A}$ is Ω^θ_n-saturated for every $\exists^1_1$ formula $\theta(\vec{\mathsf{y}})$ and every n, then every $\exists^1_1$ relation on A is a conjunction of a sequence of $\mathbf{A}$-elementary relations.

2F. Craig interpolation and Beth definability (via games)

We use here Theorem 2E.9 to prove the following, basic result:

Theorem 2F.1 (The Craig Interpolation Theorem). *Suppose τ is a relational signature, T is a τ-theory which has no finite models, and*

$$T \vdash \phi(\vec{Y}) \rightarrow \psi(\vec{X}), \tag{66}$$

where the sentences

$$\phi(\vec{Y}) \equiv \phi(Y_1, \ldots, Y_m) \text{ and } \psi(\vec{X}) \equiv \psi(X_1, \ldots, X_n)$$

may have symbols from τ in addition to the (fresh, distinct) relation symbols exhibited. There is then a τ-sentence χ, such that

$$T \vdash \phi(\vec{Y}) \rightarrow \chi \text{ and } T \vdash \chi \rightarrow \psi(\vec{X}).$$

One of the (many) important consequences of this result is the following:

Theorem 2F.2 (The Beth Definability Theorem). *Suppose $\phi(X)$ is a sentence in $\mathbb{FOL}(\tau \cup \{X\})$, where the n-ary relation symbol X is not in the (relational) signature τ, T is a τ-theory with no finite models, and*

$$T \vdash \phi(X) \ \&\ \phi(Y) \rightarrow (\forall \vec{x})[X(\vec{x}) \leftrightarrow Y(\vec{x})];$$

there is then a full extended τ-formula $\chi(\vec{x})$ such that

$$T \vdash \phi(X) \rightarrow (\forall \vec{x})[X(\vec{x}) \leftrightarrow \chi(\vec{x})].$$

Somewhat loosely (and skipping the conditions on T, which can be removed), *if at most one relation X satisfies $\phi(X)$ in every model of T, then some τ-formula $\chi(\vec{x})$ defines this X in every model of T in which it exists.*

Proof of 2F.2 from 2F.1. Choose distinct, fresh constants $\vec{d} \equiv d_1, \dots, d_n$ and check (easily) that the hypothesis implies

$$T \vdash \Big(\phi(X) \mathbin{\&} X(\vec{d})\Big) \to \Big(\phi(Y) \to Y(\vec{d})\Big).$$

By Theorem 2F.1 then, there is a $(\tau, \vec{d})$-sentence $\chi(\vec{d})$ such that

$$T \vdash \Big(\phi(X) \mathbin{\&} X(\vec{d})\Big) \to \chi(\vec{d}), \text{ and } T \vdash \chi(\vec{d}) \to \Big(\phi(Y) \to Y(\vec{d})\Big),$$

from which we get (with a bit of logic)

$$T \vdash \Big(\phi(X) \mathbin{\&} X(\vec{x})\Big) \to \chi(\vec{x}), \text{ and } T \vdash \Big(\chi(\vec{x}) \mathbin{\&} \phi(X)\Big) \to X(\vec{x}),$$

which (with a bit of logic, again) yields the required result. ⊣

The proof of Theorem 2F.1 will be based on the following version of Theorem 2E.7, for $\forall^1_1$-sentences:

Theorem 2F.3. *Suppose τ is a relational signature and η is a $\forall^1_1$ τ-sentence. There exists a sequence $\Omega_0, \Omega_1, \dots$ of partial pretypes and a sequence of τ-sentences $\eta_0, \eta_1, \dots$, such that*

$$\models \eta_i \to \eta_{i+1} \quad (i = 0, 1, \dots);$$

for every countably infinite τ-structure $\mathbf{A}$ and every i,

$$\mathbf{A} \models \eta_i \to \eta;$$

and if $\mathbf{A}$ is Ω_n-saturated for every n, then

$$\mathbf{A} \models \eta \iff \mathbf{A} \models \bigvee\!\!\!\bigvee_i \eta_i.$$

Proof. Apply Theorem 2E.7 to the $\exists^1_1$ τ-sentence θ which is logically equivalent to $\neg\eta$, use the partial pretypes Ω_n constructed for the proof of that result, and set

$$\eta_i \equiv \neg\omega_{0,i}.$$

Now

$$\models \eta_i \to \eta_{i+1}$$

by (the contrapositive of) (59), with $n = 0$;

$$\mathbf{A} \models \eta_i \to \eta$$

for every countably infinite $\mathbf{A}$ by the (contrapositive of) the first part of Theorem 2E.7; and if $\mathbf{A}$ is Ω_n-saturated for every n, then

$$\begin{aligned} \mathbf{A} \models \eta \iff \text{not } \mathbf{A} \models \theta &\iff \text{not } \mathbf{A} \models \bigwedge\!\!\!\bigwedge_i \omega_{0,i} \\ &\iff \mathbf{A} \models \bigvee\!\!\!\bigvee_i \neg\omega_{0,i} \iff \mathbf{A} \models \bigvee\!\!\!\bigvee_i \eta_i. \end{aligned}$$

⊣

Proof of Theorem 2F.1. The hypothesis implies immediately that

$$T \models \exists \vec{Y} \phi(\vec{Y}) \to \forall \vec{X} \psi(\vec{X}),$$

so apply Theorem 2F.3 to $\eta \equiv \forall \vec{X} \psi(\vec{X})$ to get $\Omega_0, \Omega_1, \ldots$ and $\eta_0, \eta_1, \ldots$, with the properties enumerated in that result. One of them is that, for every i and every countable, infinite τ-structure $\mathbf{A}$,

$$\mathbf{A} \models \eta_i \to \eta;$$

so to complete the proof, it is enough to show that

Claim: *There is some i, such that if $\mathbf{A}'$ is any countably infinite model of T, then*

$$\mathbf{A}' \models \exists \vec{Y} \phi(\vec{Y}) \to \eta_i.$$

Proof of the Claim. If not, then the theory

$$T = \{\phi(Y), \neg\eta_0, \neg\eta_1, \neg\eta_2, \ldots\}$$

is consistent (appealing to $\models \eta_i \to \eta_{i+1}$), and so it has a countably infinite model $(\mathbf{A}', \vec{Y}')$. By the basic Theorem 2C.7 (which is the key to this proof), $(\mathbf{A}', \vec{Y}')$ has an elementary extension $(\mathbf{A}, \vec{Y}'')$ which is Ω_n-saturated for every Ω_n associated with η in Theorem 2F.3; in particular, $\mathbf{A} \models T$, and $(\mathbf{A}, \vec{Y}'') \models \phi(\vec{Y})$, which means that $\mathbf{A} \models \exists \vec{Y} \phi(\vec{Y})$. The hypothesis of the theorem now implies that $\mathbf{A} \models \forall \vec{X} \psi(\vec{X})$, which by the saturation gives $\mathbf{A} \models \bigvee\!\!\!\bigvee_i \eta_i$, contradicting our assumption. $\dashv$

2G. Problems for Chapter 2

Problem x2.1 (Courtesy of Alex Ustvyanov). Consider the following proposition about symmetric graphs:

> "There is no edge from any node to itself; and there is a node x which has just one neighbor, and such that every node other than x has exactly two neighbors".

Argue that it can be expressed by a sentence χ of $\mathbb{FOL}(E)$, and show that χ is true in some infinite, symmetric graph but it is not true in any finite symmetric graph.

Note. This shows that all four propositions in Problem x1.44 fail for symmetric graphs too.

Problem x2.2. Prove that every consistent τ-theory T has a consistent, complete extension T^*.

Note. Derive this (in one line) from the Completeness Theorem; but give also an independent proof, pretending that you were assigned the problem before we proved the Completeness Theorem—this ia an easy argument, a small part of the proof of the Completeness Theorem.

Problem x2.3. Prove (2) of Lemma 2A.3.

Problem x2.4. Suppose $\mathbf{A}_0, \mathbf{A}_1, \dots$ is an **elementary sequence** of τ-structures, i.e.,

$$\mathbf{A}_0 \preceq \mathbf{A}_1 \preceq \mathbf{A}_2 \preceq \cdots .$$

Give an appropriate definition of the **limit structure** $\mathbf{A} = \bigcup_{i=0}^{\infty} \mathbf{A}_i$ (with $A = \bigcup_{i=0}^{\infty} A_i$) and prove that for every $i = 0, 1, \dots$,

$$\mathbf{A}_i \preceq \mathbf{A}.$$

Problem x2.5. Prove the second part of Theorem 2A.6 for formulas (rather than just sentences): i.e., show that for a τ-theory T and a full extended τ-formula $\chi(v_1, \dots, v_n)$ the following two conditions are equivalent:

(3) If $\mathbf{A} \subseteq \mathbf{B}$ and both are models of T, then for all $x_1, \dots, x_n$

$$\mathbf{A} \models \chi[x_1, \dots, x_n] \Longrightarrow \mathbf{B} \models \chi[x_1, \dots, x_n].$$

(4) There is a full extended existential τ-formula $\chi^*(v_1, \dots, v_n)$ such that $T \vdash \forall \vec{v}[\chi(\vec{v}) \leftrightarrow \chi^*(\vec{v})$.

Note: Do not reprove Theorem 2A.6—use it.

Problem x2.6. Suppose $\mathbf{B}$ is a structure (not necessarily countable) and $X \subseteq B$; prove that there exists a smallest substructure $\mathbf{A} \subseteq \mathbf{B}$ such that $X \subseteq A$; i.e.,

$$\mathbf{A} \subseteq B, X \subseteq A, \text{ and for every } \mathbf{A}' \subseteq \mathbf{B}, \text{ if } X \subseteq A', \text{ then } \mathbf{A} \subseteq \mathbf{A}'.$$

Show also that if X is countable, then $\mathbf{A}$ is also countable.

Note. This $\mathbf{A}$ is called **the substructure of B generated by** X and is usually denoted by $\langle X \rangle_{\mathbf{B}}$.

Problem x2.7. Consider the following set of formulas with just v free in the language of orderings:

$$\Phi(v) = \{\exists u_1(u_1 < v),\ \exists u_1 \exists u_2(u_1 < u_2 < v),\ \dots, \exists u_1 \exists u_2 \cdots \exists u_n(u_1 < u_2 < \cdots < u_n < v), \dots\}.$$

Let T be the theory of dense linear orderings with a minimum element and no maximum. Prove that $\Phi(v)$ is a partial type of T_1, and determine (with proofs) whether each of the following claims is true or false:

(a) $\Phi(v)$ is complete.
(b) $\Phi(v)$ is principal.
(c) $\Phi(v)$ is realized in some model of T.
(d) $\Phi(v)$ is realized in every model of T.

Problem x2.8. Solve the preceding problem x2.7 for the theory $T = \mathrm{Th}(\mathbb{N}, \leq)$ of the natural numbers with their usual ordering.

A relation $R(x_1, \dots , x_n)$ is **elementary** (first-order-definable) **with parameters** in a structure $\mathbf{A}$ if there is a full extended formula

$$\chi(u_1, \dots , u_m, v_1, \dots , v_n)$$

and an m-tuple $a_1, \dots , a_m \in A$ such that for all $x_1, \dots , x_n \in A$,

$$R(x_1, \dots , x_n) \iff \chi[a_1, \dots , a_m, x_1, \dots , x_n].$$

For example, the relation $x > \pi$ is (obviously) elementary with parameters in $(\mathbb{R}, \leq)$, although it is not elementary in $(\mathbb{R}, \leq)$ (because it is not preserved by the automorphism $x \mapsto x - 1$).

Problem x2.9*. Consider the following relation of *accessibility* (or *transitive closure* on a symmetric graph $\mathbf{G} = (G, E)$:

$$\mathrm{TC}(x, y) \iff \text{there is a path from } x \text{ to } y,$$

where a path from x to y is a finite sequence of nodes

$$x = z_1 \ E \ z_2 \ \cdots \ E \ z_n = y.$$

Prove that there exists a symmetric graph $\mathbf{G} = (G, E)$ in which TC is not elementary with parameters.

Problem x2.10. Prove that the class of $\exists^1_1$ relations $P(\vec{x}, \vec{R})$ on a τ-structure $\mathbf{A}$ is closed under substitution of $\mathbf{A}$-elementary functions, as well as the *positive* operations

$$\& \ , \ \vee \ , \ \exists v, \ \forall v, \ \exists X;$$

similarly, the class of $\forall^1_1$ relations on $\mathbf{A}$ is closed under substitution of $\mathbf{A}$-elementary functions and the operations

$$\& \ , \ \vee \ , \ \exists v, \ \forall v, \ \forall X.$$

HINT: You will need some fairly simple logical equivalences, including

$$(\forall u)(\exists X)P(u, X) \iff (\exists Y)(\forall u)P(u, \{\vec{v} \mid Y(u, \vec{v})\}) \tag{67}$$

where X ranges over n-ary and Y ranges over $(n+1)$-ary relations. To use this in the formal language, you will need to associate with each extended $\mathbb{FOL}^2$-formula $\phi(X)$ and each variable u (which does not occur in $\phi(X)$), an extended formula

$$\phi^*(Y) \equiv \phi(\{\vec{v} \mid Y(u, \vec{v})\}),$$

in which X does not occur, Y is fresh, and for all structures $\mathbf{A}$ and all assignments π,

$$\mathbf{A}, \pi\{u := x, X := R\} \models \phi \iff \mathbf{A}, \pi\{u := x, Y := \{(x, \vec{y}) \mid \vec{x} \in X\} \models \phi^*.$$

(The construction of $\phi^*$is by structural recursion on ϕ.)

CHAPTER 3

INTRODUCTION TO THE THEORY OF PROOFS

In order to study *proofs* as mathematical objects, it is necessary to introduce deductive systems which are richer and model better the intuitive proofs we give in mathematics than the Hilbert system of Part A. Our (limited) aim in this Part is to formulate and establish in outline a central result of Gentzen, which in addition to its foundational significance also has a large number of applications.

3A. The Gentzen Systems

The main difference between the Hilbert proof system and the Gentzen systems **G** and **GI** is in the *proofs*, which Gentzen endows with a rich, combinatorial structure that facilitates their mathematical study. It will also be convenient, however, to enlarge the language $\mathbb{FOL}(\tau)$ with a sequence of **propositional variables**

$$\mathsf{p}_1, \mathsf{p}_1, \dots ,$$

so that the Propositional Calculus is naturally embedded in $\mathbb{FOL}(\tau)$, for any signature τ. So the formulas of $\mathbb{FOL}(\tau)$ are now defined by the recursion

$$\chi :\equiv p \mid s = t \mid R(t_1, \dots , t_n) \quad \text{(the } \textit{prime formulas}\text{)}$$
$$\mid \neg(\phi) \mid (\phi) \rightarrow (\psi) \mid (\phi) \mathbin{\&} (\psi) \mid (\phi) \vee (\psi) \mid \forall v \phi \mid \exists v \phi$$

where p is any propositional variable; and in the semantics of the system, we admit assignments which in addition to their values on individual variables also assign a truth value $\pi(p)$ (either 1 or 0) to every propositional variable p.

We should also note that the identity symbol is treated like any other relation constant by the Gentzen systems, i.e., we do not postulate the Axioms for Identity and we will need to include them among the hypotheses when they are relevant.

Definition 3A.1. A **sequent** (in a fixed signature τ) is an expression

$$\phi_1, \dots, \phi_n \Rightarrow \psi_1, \dots, \psi_m$$

where $\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m$ are τ-formulas. We view the formulas on the left and the right as comprising **multisets**, i.e., we identify sequences which differ only in the order in which they list their terms. The empty multisets are allowed, so that the simplest sequent is just $\Rightarrow$. The next simplest ones are of the form $\Rightarrow \phi$ and $\phi \Rightarrow$.

Definition 3A.2. The axioms and rules of inference of the **classical Gentzen system G** and the **intuitionistic system GI** are listed in Table 1; the only difference between the two systems is that in **GI** we only allow sequents which have at most one formula on the right, they look like

$$A \Rightarrow \phi \text{ or } A \Rightarrow$$

There is one axiom (scheme), the sequent $\phi \Rightarrow \phi$, for each formula ϕ; one **introduction rule** (on the left) and one **elimination rule** (on the right) for each logical construct; a similar pair of **thinning** (T) and **contraction** (C) introduction and elimination rules; and the **Cut Rule** at the end—which may be viewed as an elimination rule but plays a very special role. In all rules where an extended formula $\phi(v)$ and a substitution instance $\phi(t)$ or $\phi(x)$ of that formula occur, we assume that the term t or the variable x is free for v in $\phi(v)$, and there is an additional **Restriction** in the $\forall$-introduction and $\exists$-elimination rules which is listed in the Table.

3A.3. Terminology. We classify the rules of **G** and **GI** into three categories, as follows:

1. The **structural rules** T (Thinning) and C (Contraction).
2. The **Cut**.
3. The **logical rules**, two for each logical construct, which are again subdivided into **propositional** and **quantifier** rules in the obvious way.

Each rule has one or two **premises**, the sequents above the line, and a **conclusion**, the sequent below the line; a single sequent axiom is its own conclusion and has no premises.

The formulas in A, B are the **side formulas** of a rule. The remaining zero, one or two formulas in the premises are the **principal formulas** of the rule, and the remaining formulas in the conclusion are the **new formulas** of the rule. Notice that an axiom has no side formulas, no principal formulas and two new (identical) formulas; a Cut has two principal formulas and no new formulas; and every other rule has exactly one new formula.

Each new formula in a rule is associated with zero, one or two formulas in the premises, which are its **parents**; the new formula is an "orphan" in an axiom and in the thinning rule T. We also associate each side formula in the conclusion of a rule with exactly one parent in one of the premises, from which is was copied.

The Gentzen Systems **G**, **GI**

Axiom Scheme $\phi \Rightarrow \phi$

$\rightarrow$	$\dfrac{A,\, \phi \Rightarrow B,\, \psi}{A \Rightarrow B,\, \phi \rightarrow \psi}$	$\dfrac{A_1 \Rightarrow B_1,\, \phi \qquad A_2,\, \psi \Rightarrow B_2}{A_1,\, A_2,\, \phi \rightarrow \psi \Rightarrow B_1,\, B_2}$
&	$\dfrac{A \Rightarrow B,\, \phi \qquad A \Rightarrow B,\, \psi}{A \Rightarrow B,\, \phi \,\&\, \psi}$	$\dfrac{\phi,\, A \Rightarrow B}{\phi \,\&\, \psi,\, A \Rightarrow B} \qquad \dfrac{\psi,\, A \Rightarrow B}{\phi \,\&\, \psi,\, A \Rightarrow B}$
$\vee$	$\dfrac{A \Rightarrow B,\, \phi}{A \Rightarrow B,\, \phi \vee \psi} \qquad \dfrac{A \Rightarrow B,\, \psi}{A \Rightarrow B,\, \phi \vee \psi}$	$\dfrac{A,\, \phi \Rightarrow B \quad A,\, \psi \Rightarrow B}{A,\, \phi \vee \psi \Rightarrow B}$
$\neg$	$\dfrac{A,\, \phi \Rightarrow B}{A,\, \Rightarrow B,\, \neg\phi}$	$\dfrac{A \Rightarrow B,\, \phi}{A,\, \neg\phi \Rightarrow B}$
$\forall$	$\dfrac{A \Rightarrow B,\, \phi(v)}{A \Rightarrow B,\, \forall x \phi(x)}$ (**Restr**)	$\dfrac{A,\, \phi(t) \Rightarrow B}{A,\, \forall x \phi(x) \Rightarrow B}$
$\exists$	$\dfrac{A \Rightarrow B,\, \phi(t)}{A \Rightarrow B,\, \exists x \phi(x)}$	$\dfrac{A,\, \phi(v) \Rightarrow B}{A,\, \exists x \phi(x) \Rightarrow B}$ (**Restr**)
T	$\dfrac{A \Rightarrow B}{A \Rightarrow B,\, \phi}$	$\dfrac{A \Rightarrow B}{A,\, \phi \Rightarrow B}$
C	$\dfrac{A \Rightarrow B,\, \phi,\, \phi}{A \Rightarrow B,\, \phi}$	$\dfrac{A,\, \phi,\, \phi \Rightarrow B}{A,\, \phi \Rightarrow B}$

Cut $\qquad \dfrac{A_1 \Rightarrow B_1,\, \chi, \qquad \chi,\, A_2 \Rightarrow B_2}{A_1,\, A_2 \Rightarrow B_1,\, B_2}$

(1) A, B are multisets of formulas in $\mathbb{FOL}(\tau)$.
(2) For the Intuitionistic system **GI**, at most one formula is allowed on the right.
(3) **Restr** : the **active variable** v is not free in A, B.
(4) The formulas in A, B are the *side formulas* of an inference.
(5) The formulas ϕ, ψ above the line are the *principal formulas* of the inference. (One or two; none in the axiom.)
(6) There is an obvious *new formula* below the line in each inference, except for Cut.
(7) Each new and each side formula in the conclusion of each rule is associated with zero, one or two parent formulas in the premises.

Table 1. The Gentzen systems.

Definition 3A.4 (Proofs)**.** The set of Gentzen **proofs** of depth $\leq d$ and the **endsequent** of each proof are defined together by the following recursion on the natural number $d \geq 1$.

1. For each formula ϕ, the pair $(\emptyset, \phi \Rightarrow \phi)$ is a proof of depth ≤ 1 and endsequent $\phi \Rightarrow \phi$. We picture it in **tree form** by:

$$\frac{}{\phi \Rightarrow \phi}$$

2. If Π is a proof of depth $\leq d$ and endsequent α and

$$\frac{\alpha}{\beta}$$

is a one-premise inference rule, then the pair (Π, β) is a proof of depth $\leq (d+1)$ and endsequent β. We picture (Π, β) in tree form by:

$$\frac{\Pi}{\beta}.$$

3. If Π_1, Π_2 are proofs of depth $\leq d$ and respective endsequents α_1, α_2, and if

$$\frac{\alpha_1 \qquad \alpha_2}{\beta}$$

is a two-premise inference rule, then the pair $((\Pi_1, \Pi_2), \beta)$ is a proof of depth $\leq (d+1)$. We picture $((\Pi_1, \Pi_2), \beta)$ in tree form by:

$$\frac{\Pi_1 \qquad \Pi_2}{\beta}$$

A **proof** Π in **G** of **GI** is a proof of depth d, for some d, and it is a proof of its endsequent; it is a **propositional proof** if none of the four rules about the quantifiers are used in it. We denote the relevant relations by

$$\mathbf{G} \vdash A \Rightarrow B, \ \mathbf{G} \vdash_{\text{prop}} A \Rightarrow B, \ \mathbf{GI} \vdash A \Rightarrow B, \ \text{or } \mathbf{GI} \vdash_{\text{prop}} A \Rightarrow B$$

accordingly.

We let $\mathbf{G}_{\text{prop}}$ and $\mathbf{GI}_{\text{prop}}$ be the restricted systems in which only formulas for the Propositional Calculus 1K.1 and only propositional rules are allowed.

Proposition 3A.5 (Parsing for Gentzen proofs)**.** *Each proof* Π *satisfies exactly one of the following three conditions.*

1. $\Pi = (\emptyset, \beta)$, *where* β *is an axiom.*
2. $\Pi = (\Sigma, \beta)$, *where* Σ *is a proof of smaller depth and endsequent some* α, *and there is a one premise rule* $\frac{\alpha}{\beta}$.

3. $\Pi = ((\Sigma_1, \Sigma_2), \beta)$, *where* Σ_1, Σ_2 *are proofs of smaller depth and respective endsequents* α_1, α_2, *and there is a two premise rule* $\dfrac{\alpha_1 \quad \alpha_2}{\beta}$.

In all cases, a proof is a pair and the second member of that pair is its endsequent.

Proofs in the Gentzen systems are displayed in tree form, as in the following examples which prove in **G** three of the propositional axioms of the Hilbert system:

$$
\begin{prooftree}
\AxiomC{$\chi \Rightarrow \chi$}
\RightLabel{$(\Rightarrow \neg)$}
\UnaryInfC{$\Rightarrow \chi, \neg\chi$}
\RightLabel{$(\neg \Rightarrow)$}
\UnaryInfC{$\neg\neg\chi \Rightarrow \chi$}
\RightLabel{$(\Rightarrow\rightarrow)$}
\UnaryInfC{$\Rightarrow \neg\neg\chi \rightarrow \chi$}
\end{prooftree}
\qquad
\begin{prooftree}
\AxiomC{$\phi \Rightarrow \phi$}
\RightLabel{(T)}
\UnaryInfC{$\phi, \psi \Rightarrow \phi$}
\RightLabel{$(\Rightarrow\rightarrow)$}
\UnaryInfC{$\phi \Rightarrow \psi \rightarrow \phi$}
\RightLabel{$(\Rightarrow\rightarrow)$}
\UnaryInfC{$\Rightarrow \phi \rightarrow (\psi \rightarrow \phi)$}
\end{prooftree}
$$

$$
\begin{prooftree}
\AxiomC{$\phi \Rightarrow \phi$}
\RightLabel{(T)}
\UnaryInfC{$\phi, \psi \Rightarrow \phi$}
\AxiomC{$\psi \Rightarrow \psi$}
\RightLabel{(T)}
\UnaryInfC{$\phi, \psi \Rightarrow \psi$}
\RightLabel{$(\Rightarrow \&)$}
\BinaryInfC{$\phi, \psi \Rightarrow \phi \;\&\; \psi$}
\RightLabel{$(\Rightarrow\rightarrow)$}
\UnaryInfC{$\phi \Rightarrow \psi \rightarrow (\phi \;\&\; \psi)$}
\RightLabel{$(\Rightarrow\rightarrow)$}
\UnaryInfC{$\Rightarrow \phi \rightarrow (\psi \rightarrow (\phi \;\&\; \psi))$}
\end{prooftree}
$$

Notice that the first of these proofs is in **G**, while the last two are in **GI**.

In the next example of a **GI**-proof of another of the Hilbert propositional axioms we do not label the rules, but we put in boxes the principal formulas for each application:

$$
\begin{prooftree}
\AxiomC{$\phi \Rightarrow \boxed{\phi}$}
\AxiomC{$\phi \Rightarrow \boxed{\phi}$}
\AxiomC{$\psi \Rightarrow \boxed{\psi}$}
\AxiomC{$\boxed{\chi} \Rightarrow \chi$}
\BinaryInfC{$\psi, \boxed{\psi \rightarrow \chi} \Rightarrow \chi$}
\BinaryInfC{$\phi, \boxed{\psi}, \phi \rightarrow (\psi \rightarrow \chi) \Rightarrow \chi$}
\BinaryInfC{$\boxed{\phi}, \phi \rightarrow \psi, \phi \rightarrow (\psi \rightarrow \chi) \Rightarrow \boxed{\chi}$}
\UnaryInfC{$\phi \rightarrow \psi, \boxed{\phi \rightarrow (\psi \rightarrow \chi)} \Rightarrow \boxed{\phi \rightarrow \chi}$}
\UnaryInfC{$\boxed{\phi \rightarrow \psi} \Rightarrow \boxed{\phi \rightarrow (\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi)}$}
\UnaryInfC{$\Rightarrow (\phi \rightarrow \psi) \rightarrow ((\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow (\phi \rightarrow \chi))$}
\end{prooftree}
$$

The form of the rules of inference in the Gentzen systems makes it much easier to discover proofs in them rather than in the Hilbert system. Consider, for example, the following, which can be constructed step-by-step starting with the last sequent (which is what we want to show) and trying out the most plausible inference which gives it:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\phi \Rightarrow \phi}{\forall v\phi \Rightarrow \phi}\,(\forall \Rightarrow)}{\forall v\phi \Rightarrow \exists u\phi}\,\Rightarrow \exists)}{\exists u\forall v\phi \Rightarrow \exists u\phi}\,(\exists \Rightarrow,\ u \text{ not free on the right})}{\exists u\forall v\phi \Rightarrow \forall v\exists u\phi}\,(\Rightarrow \forall,\ v \text{ not free on the left})}{\Rightarrow \exists u\forall v\phi \to \forall v\exists u\phi}\,(\Rightarrow\to)$$

In fact these guesses are unique in this example, except for Thinnings, Contractions and Cuts, an it is quite common that the most difficult proofs to construct are those which required T's and C's—especially as we will show that Cuts are not necessary.

Theorem 3A.6 (Strong semantic soundness of **G**). *Suppose*

$$\mathbf{G} \vdash \phi_1, \dots, \phi_n \ \Rightarrow\ \psi_1, \dots, \psi_m,$$

and **A** *is any structure (of the fixed signature): then for every assignment* π *into* **A***,*

$$\textit{if } \mathbf{A}, \pi \models \phi \ \&\ \dots\ \&\ \phi_n, \ \textit{then } \mathbf{A}, \pi \models \psi \vee \dots \vee \psi_m.$$

Here the empty conjunction is interpreted by 1 and the empty disjunction is interpreted by 0.

Theorem 3A.7 (Proof-theoretic soundness of **G**). *If* $\mathbf{G} \vdash A \ \Rightarrow\ B$*, then* $A \vdash \vee B$ *in the Hilbert system, by a deduction in which no free variable of* A *is quantified and the Identity Axioms* (5) – (17) *are not used.*

Theorem 3A.8 (Proof-theoretic completeness of **G**). *If* $A \vdash \phi$ *in the Hilbert system by a deduction in which no free variable of* A *is quantified and the Identity Axioms* (5) – (17) *are not used, then* $\mathbf{G} \vdash A \ \Rightarrow\ \phi$*.*

These three theorems are all proved by direct (and simple, if a bit cumbersome) inductions on the given proofs.

3A.9. Remark. The condition in Theorem 3A.8 is necessary, because (for example)

(68) $$R(x) \vdash \forall x R(x)$$

but the sequent

$$R(x) \ \Rightarrow\ \forall x R(x)$$

is not provable in **G**, because of the strong Soundness Theorem 3A.6. The Hilbert system satisfies the following weaker Soundness Theorem, which does not contradict the deduction (68): *if* $A \vdash \phi$ *and every assignment* π *into* **A** *satisfies* A*, then every assignment* π *into* **A** *satisfies* ϕ*.* (We have stated the Soundness Theorem for the Hilbert system in **4.3** only for sets of sentences as hypotheses, but to prove it we needed to show this stronger statement.)

Theorem 3A.10 (Semantic Completeness of **G**). *Suppose* $\psi, \phi_1, \ldots, \phi_n$ *are* τ*-formulas such that for every* τ*-structure* $\mathbf{A}$ *and every assignment* π *into* $\mathbf{A}$,

$$\textit{if } \mathbf{A}, \pi \models \phi_1 \ \& \ \cdots \ \& \ \phi_n, \ \textit{then } \mathbf{A}, \pi \models \psi;$$

it follows that

$$\mathbf{G} \vdash \mathrm{IA}, \phi_1, \ldots, \phi_n \ \Rightarrow \ \psi,$$

where IA *are the* (finitely many) *identity axioms for the relation and function symbols which occur in* $\psi, \phi_1, \ldots, \phi_n$.

Proof This follows easily from Theorem 3A.8 and the Completeness Theorem for the Hilbert system. ⊣

3A.11. The intuitionistic Gentzen system GI. The system **GI** is a formalization of L. E. J. Brouwer's *intuitionistic logic*, the logical foundation of constructive mathematics. This was developed near the beginning of the 20th century. It was Gentzen's ingenious idea that constructive logic can be captured simply by restricting the number of formulas on the right of a sequent. About constructive mathematics, we will say a little more later on; for now, we just use **GI** as a tool to understand the combinatorial methods of analyzing formal proofs that pervade proof theory.

3B. Cut-free proofs

Cut is the only **G**-rule which "loses the justification" for the truth of its conclusion, just as Modus Ponens (which is a simple version of it) does in the Hilbert system. As a result, *Cut-free* Gentzen proofs (which do not use the Cut) have important special properties.

Proposition 3B.1. *If one of the logical symbols* $\neg$, &, $\vee$, $\rightarrow$, $\forall$ *or* $\exists$ *does not occur in the endsequent of a Cut-free proof* Π, *then that logical symbol does not occur at all in* Π, *and hence neither of the rules involving that logical symbol are applied in* Π.

Definition 3B.2. The **subformulas** of a formula of $\mathbb{FOL}(\tau)$ are defined by the following recursion.

1. If $\chi \equiv p, \chi \equiv R(t_1, \ldots, t_n)$ or $\chi \equiv s = t$ is prime, then χ is the only subformula of itself.
2. If χ is a propositional combination of ϕ and ψ, then the subformulas of χ are χ itself, and all the subformulas of ϕ and ψ.

3. If $\chi \equiv \exists x \phi(x)$ or $\chi \equiv \forall x \phi(x)$, then the subformulas of χ are χ and all subformulas of substitution instances $\phi(t)$, where t is an arbitrary term, free for x in $\phi(x)$. (Here t may be a variable, since variables are terms, and in particular $\phi(x)$ is a subformula of χ.)

For example, the subformulas of $\exists x R(x, y)$ are all $R(t, y)$, and there are infinitely many of them; if a formula has only finitely many subformulas, then it is propositional.

Theorem 3B.3 (Subformula Property)**.** *If* Π *is a* **Cut-free proof** *with endsequent* α*, then every formula which occurs in* Π *is a subformula of some formula in* α*.*

Corollary 3B.4. *If a constant* c*, a relation symbol* R *or a function symbol* f *does not occur in the endsequent of a Cut-free proof* Π*, then* c*,* R *or* f *does not occur at all in* Π*.*

3C. Cut Elimination

We outline here (with few details) a proof of the following, fundamental theorem of Gentzen, to the effect that up to alphabetic changes in bound variables, every provable sequent has a Cut-free proof:

Theorem 3C.1 (Cut Elimination Theorem, Gentzen's Hauptsatz)**.** *From a proof in* **G** *or* **GI** *of a sequent* α *in which no variable occurs both free and bound, we can construct a pure variable, Cut-free proof of* α *in the same system.*

Pure variable proofs will be defined below in Definition 3C.8.

This is the basic result of Proof Theory, and it has a host of important consequences in all parts of logic (and some parts of classical mathematics as well).

3C.2. The Mix rule. This is a strengthening of the Cut rule, which allows us to Cut simultaneously all occurrences of the Cut formula:

$$\frac{A_1 \Rightarrow B_1 \qquad A_2 \Rightarrow B_2}{A_1, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\}, B_2} \text{ assuming that } \chi \in A_2 \cap B_1.$$

For a multiset D, by $D \setminus \{\chi\}$ we mean the result of removing all occurrences of χ from D.

By $\mathbf{G}^m$ and $\mathbf{GI}^m$ we understand the systems in which the Cut Rule has been replaced by the Mix Rule.

Lemma 3C.3. *If we replace the Cut Rule by the Mix Rule, we get exactly the same provable sequents, both for* **G** *and for* **GI**.

In fact*: every proof* Π *of* **G** *or* **GI** *can be converted into a proof* Π^m *in* $\mathbf{G}^m$ *or* $\mathbf{GI}^m$ *respectively, in which exactly the same logical rules are used—i.e., by replacing the Cuts by Mixes and* (possibly) *introducing some applications of structural rules; and vice versa.*

From now on by "proof" we will mean "proof in $\mathbf{G}^m$ or $\mathbf{GI}^m$", unless otherwise stated.

Definition 3C.4. To each (occurrence of a) sequent α in a proof Π, we assign **the part of the proof above** α by the following recursion.

1. If α is the endsequent of a proof Π, then the part of Π above α is the entire Π.
2. If $\Pi = (\Sigma, \beta)$ is a proof and α occurs in Σ, then the part of Π above α is the part of Σ above α. (Here Σ is a proof, by the Parsing Lemma for proofs.)
3. If $\Pi = ((\Sigma_1, \Sigma_2), \beta)$ is a proof and α occurs in Σ_1, then the part of Π above α is the part of Σ_1 above α; and if α occurs in Σ_2, then the part of Π above α is the part of Σ_2 above α. (Again Σ_1, Σ_2 are proofs here.)

Lemma 3C.5. *If* α *occurs in a proof* Π*, then the part of* Π *above* α *is a proof with endsequent* α*.*

The proof of Mix Elimination for propositional proofs is substantially easier than the proof for the full systems, especially as *all propositional proofs have the pure variable property.* We give this first.

Theorem 3C.6 (Main Propositional Lemma)**.** *Suppose we are given a propositional proof*

$$\dfrac{\dfrac{\Pi_1}{A_1 \Rightarrow B_1} \qquad \dfrac{\Pi_2}{A_2 \Rightarrow B_2}}{A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2}$$

in $\mathbf{G}^m$ *or* $\mathbf{GI}^m$ *which has exactly one Mix as its last inference; we can then construct a Mix-free, propositional proof of the endsequent*

$$A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2 \tag{69}$$

which uses the same logical rules.

Equivalently: *given any propositional, Mix-free proofs of*

$$A_1 \Rightarrow B_1 \quad \textit{and} \quad A_2 \Rightarrow B_2$$

such that a formula χ *occurs in both* B_1 *and* A_2*, we can construct a propositional, Mix-free proof of* (69) *which uses the same logical rules.*

Outline of the proof. We define the *left Mix rank* to be the number of consecutive sequents in the proof which ends with $A_1 \Rightarrow B_1$ starting from the last one and going up, in which χ occurs on the right; so this is at least 1. The *right Mix rank* is defined similarly, and the *rank* of the Mix is their sum. *The minimum Mix rank is* 2. The *grade* of the Mix is the number of logical symbols in the Mix formula χ.

The proof is *by induction on the grade*. Both in the basis (when χ is a prime formula) and in the induction step, we will need an *induction on the rank*, so that the proof really is by *double induction*.

Lemma 1. If the Mix formula χ occurs in A_1 or in B_2, then we can eliminate the Mix using Thinnings and Contractions.

Lemma 2. If the left Mix rank is 1 *and the last left inference is by a T or a C, then the Mix can be eliminated; similarly if the right Mix rank is* 1 *and the last right inference is a C or a T.* (Actually the last left inference cannot be a C if the left Mix rank is 1.)

Main part of the proof. We now consider cases on what the last left inference and the last right inference is, and we may assume that the Main Lemma holds for all cases of smaller grade, and for all cases of the same grade but smaller rank. The cases where one of the ranks is > 1 are treated first, and are messy but fairly easy. The main part of the proof is in the consideration of the four cases (one for each propositional connective) where the rank is exactly 2, so that χ is introduced by the last inference on both sides: in these cases we use the induction hypothesis on the grade, reducing the problem to cases of smaller grade (but possibly larger rank). ⊣

Proof of Theorem 3C.1 for propositional proofs is by induction on the number of Mixes in the given proof, with the basis given by Lemma 3C.6; in the Inductive Step, we simply apply the same Lemma to an *uppermost Mix*, one such the part of the proof above its conclusion has no more Mixes. ⊣

The proof of the Hauptsatz for the full (classical and intuitionistic) systems is complicated by the extra hypothesis on free-and-bound occurrences of the same variable, which is necessary because of the following example whose proof we will leave for the problems:

Proposition 3C.7. *The sequent $\forall x \forall y R(x, y) \Rightarrow R(y, y)$ is provable in* **GI***, but it is not provable without a Cut* (even in the stronger system **G**).

To deal with this problem, we need to introduce a "global" restriction on proofs, as follows.

3C.8. Definition. A **pure variable proof** (in any of the four Gentzen systems we have introduced) is a proof Π with the following two properties.

1. No variable occurs both free and bound in Π.
2. If v is the active variable in an application of one of the two rules which have a restriction,

$$\frac{A \Rightarrow B, \phi(v)}{A \Rightarrow B, \forall x\phi(x)} \quad \text{or} \quad \frac{A, \phi(v) \Rightarrow B}{A, \exists x\phi(x) \Rightarrow B},$$

then v occurs only in the part of the proof above the premise of this application.

Lemma 3C.9. *In a pure variable proof, a variable v can be used at most once in an application of the $\Rightarrow \forall$ or the $\exists \Rightarrow$ rules.*

Proposition 3C.10 (Pure Variable Lemma)**.** *If α is a sequent in which no variable occurs both free and bound, then from every proof of α we can construct a pure variable proof of α, employing only replacement of some variables by fresh variables.*

With this result at hand, we can establish an appropriate version of Lemma 3C.6 which applies to the full systems:

Theorem 3C.11 (Main Lemma)**.** *Suppose we are given a pure variable proof*

$$\frac{\dfrac{\Pi_1}{A_1 \Rightarrow B_1} \qquad \dfrac{\Pi_2}{A_2 \Rightarrow B_2}}{A_1, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\}, B_2}$$

in $\mathbf{G}^m$ or $\mathbf{GI}^m$ which has exactly one Mix as its last inference; we can then construct a Mix-free, pure variable proof of the endsequent

$$A_1, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\}, B_2 \tag{70}$$

which uses the same logical rules.

Equivalently: *from any given, pure variable, Mix-free proofs of*

$$A_1 \Rightarrow B_1 \quad \textit{and} \quad A_2 \Rightarrow B_2$$

such that a formula χ occurs in both B_1 and A_2 and no free variable of one of them occurs bound in the other, we can construct a pure variable, Mix-free proof of (70) *which uses the same logical rules.*

The proof of this is an extension of the proof of Lemma 3C.6 which requires the consideration of two, additional cases in the induction step with rank 2—quite simple, as it happens, because the quantifier rules have only one premise.

Outline of proof of Theorem 3C.1. It is enough to prove the theorem for pure variable proofs in the system with Mix instead of Cut; and we do this by induction on the number of Mixes in the given, pure variable proof, using the Main Lemma 3C.11. ⊣

3D. The Extended Hauptsatz

For sequents of formulas in prenex form, the Gentzen Hauptsatz provides a particularly simple and useful form.

3D.1. Normal proofs. A proof Π in $\mathbf{G}$ is **normal** if it is a pure variable, Cut-free proof and a **midsequent** $A^* \Rightarrow B^*$ occurs in it with the following properties.

1. Every formula which occurs above the midsequent $A^* \Rightarrow B^*$ is quantifier free.
2. The only rules applied below the midsequent are quantifier rules or Contractions.

Notice that by the first of these properties, *no quantifier rules are applied in a normal proof above the midsequent*—only propositional and structural rule applications. So a normal proof looks like

$$\frac{\Pi}{A^* \Rightarrow B^*}$$
$$\vdots$$
$$A \Rightarrow B$$

where Π is a propositional proof and in the "linear trunk" which follows the provable, quantifier-free sequent only one-premise Contractions and quantifier inferences occur.

Theorem 3D.2 (The Extended Hauptsatz). *If $A \Rightarrow B$ is a sequent of prenex formulas in which no variable occurs both free and bound, and if $A \Rightarrow B$ is provable in $\mathbf{G}$, then there exists a normal proof of $A \Rightarrow B$.*

Outline of proof. This is a constructive argument, which produces the desired normal proof of $A \Rightarrow B$ from any given proof of it.

Step 1. By the Cut Elimination Theorem we get a new proof, which is Cut-free and pure variable.

Step 2. We replace all Axioms and all Thinnings by Axioms and Thinnings on prime (and hence quantifier free) formulas (without destroying the Cut-free, pure variable property).

The *order* of a quantifier rule application in the proof is the number of Thinnings and propositional inferences below it, down to the endsequent, and the *order of the proof* is the sum of the orders of all quantifier rule applications in the proof. If the order of the proof is 0, then there is no quantifier rule application above a Thinning or a propositional rule application, and then the proof (easily) is normal.

Proof is by induction on the order of the given proof. We begin by noticing that if the order is > 0, then there must exist some quantifier rule application *immediately above* a Thinning or a propositional rule application; we choose one such, and alter the proof to one with a smaller order and the same endsequent. The heart of the proof is the consideration of cases on *what these two inferences immediately above each other are*, the top one a quantifier rule application and the bottom one a propositional rule application or a T. It is crucial to use the fact that all the formulas in the endsequent are prenex, and hence (by the subformula property) all the formulas which occur in the proof are prenex; this eliminates a great number of inference pairs. ⊣

This proof of the Extended Hauptsatz uses the *permutability of inferences property* of the Gentzen systems, which has many other applications.

Theorem 3D.3 (Herbrand's Theorem)**.** *If a prenex formula*

$$\theta \equiv (Q_1 x_1) \cdots (Q_n x_n)\phi(x_1, \dots , x_n)$$

is provable in $\mathbb{FOL}$ *without the Axioms of Identity* (15) – (17) *, then there exists a quantifier free tautology of the form*

$$\phi^* \equiv \phi_1 \vee \cdots \vee \phi_n$$

such that:

(1) *Each* ϕ_i *is a substitution instance of the matrix* $\phi(x_1, \dots , x_n)$ *of* θ*, and*
(2) θ *can be proved from* ϕ^* *by the use of the following four Herbrand rules of inferences which apply to disjunctions of formulas:*

$$\frac{\psi_1(t) \vee \cdots \vee \psi_n}{\exists x\psi(x) \vee \cdots \chi \cdots \vee \psi_n}\ (\exists) \qquad \frac{\psi_1 \vee \cdots \chi_1 \vee \chi_2 \cdots \vee \psi_n}{\psi \vee \cdots \chi_2 \vee \chi_1 \cdots \vee \psi_n}\ (I)$$

$$\frac{\psi_1 \vee \cdots \chi \vee \chi \vee \psi_n}{\psi_1 \vee \cdots \chi \cdots \vee \psi_n}\ (C) \qquad \frac{\psi_1(v) \vee \cdots \vee \psi_n}{\forall x\psi(x) \vee \cdots \vee \psi_n}\ (\forall)\ (\mathbf{Restr})$$

(**Restr**)**:** *The variable* v *does not occur free in the conclusion.*

3D.4. Remarks. The Herbrand rules obviously correspond to the Gentzen quantifier rules and Contraction, together with the Interchange rule which we do not need for multiset sequents; and the restriction on the ∀-rule is the same, the variable v must not be free in the conclusion. A provable disjunction which satisfies the conclusion of the theorem is called a *Herbrand expansion* of θ; by extension, we often refer to the midsequent of a Gentzen normal proof as a Herbrand expansion of the endsequent.

There is an obvious version of the theorem for implications of the form

$$\theta_1 \to \theta_2$$

with both θ_1, θ_2 prenex.

3E. The propositional Gentzen systems

The Semantic Completeness Theorem 3A.10 combined with the Hauptsatz imply easily the following result, where *propositional tautologies* were defined in the brief Section 1K.1.

Theorem 3E.1 (Completeness of $\mathbf{G}_{\rm prop}$). *A propositional formula ϕ is a tautology if and only if there is a Cut-free proof in $\mathbf{G}_{\rm prop}$ of the sequent $\Rightarrow \phi$.*

This, however, is an unnecessarily complex proof: we should not need either the Completeness Theorem for $\mathbb{FOL}$ or the full Hauptsatz to establish a basically simple fact. We outline here a more direct proof of this result, and we incidentally collect some basic facts about the Propositional Calculus which we have (somehow) avoided to discuss before now.

3E.2. Truth tables. Suppose ϕ is a propositional formula with n distinct propositional variables. There are 2^n n-tuples of 0's and 1's, and so the truth values of ϕ under all possible assignments of truth values to its variables can be pictured in a table with n columns and 2^n lines (rows), one for each assignment of truth values to the variables. For example, in the case of the formula $\phi \equiv \neg p \mathbin{\&} q$ which has two variables (and including a column for the subformula $\neg p$ which is used in the computation):

p	q	$\neg p$	$\neg p \mathbin{\&} q$
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	0

Consider also the following truth table, which specifies succinctly the *truth-value* (or *bit*) *function* which is defined by the primitive, propositional connectives:

p	q	$\neg p$	$p \mathbin{\&} q$	$p \vee q$	$p \rightarrow q$
0	0	1	0	0	1
0	1	1	0	1	1
1	0	0	0	1	0
1	1	0	1	1	1

A propositional formula ϕ is a tautology if it only has 1s in the column of its truth table which catalogues its value.

Outline of Kalmar's proof of Theorem 3E.1. Fix a list of distinct propositional variables $p_1, \dots, p_n$, and for each assignment π, let

$$\pi p_i \equiv \begin{cases} p_i, & \text{if } \pi(p_i) = 1, \\ \neg p_i, & \text{if } \pi(p_i) = 0. \end{cases}$$

Set

$$\text{Line}_\pi(\vec{p}) = \text{Line}_\pi \equiv \pi p_1, \pi p_1, \dots, \pi p_n. \tag{71}$$

As a multiset, Line_π expresses formally the hypotheses on the propositional variables in the line corresponding to π in the truth table of any formula in which only the letters $p_1, \dots, p_n$ occur.

Step 1. If only the letters $p_1, \dots, p_n$ occur in ϕ, then for every π,

$$\text{if value}(\phi, \pi) = 1, \text{ then } \mathbf{G}_{\text{prop}} \vdash \text{Line}_\pi \Rightarrow \phi,$$
$$\text{if value}(\phi, \pi) = 0, \text{ then } \mathbf{G}_{\text{prop}} \vdash \text{Line}_\pi \Rightarrow \neg\phi.$$

This is proved by an induction on ϕ which is routine, but necessarily messy, since it must use every inference rule of $\mathbf{G}_{\text{prop}}$.

For each assignment π to $p_1, \dots, p_n$ and each $i \leq n$, let

$$L_i(\pi) = \pi p_{i+1}, \pi p_{i+2}, \dots, \pi p_n,$$

so that

$$L_0(\pi) \equiv \text{Line}(\pi), \quad L_n(\pi) = \emptyset,$$
$$\text{and for every } i < n, L_i(\pi) \equiv \pi p_i, L_{i+1}(\pi).$$

Step 2. If only the letters $p_1, \dots, p_n$ occur in ϕ and ϕ is a propositional tautology, then for every $i \leq n$ and for every assignment π,

$$L_i(\pi) \Rightarrow \phi$$

is provable in $\mathbf{G}_{\text{prop}}$.

This is proved by induction on $i \leq n$, simultaneously for all assignments, and the Basis Case is Step 1, while the last Case $i = n$ gives the required result. For the inductive step, the Induction Hypothesis applied to the two assignments

$$\pi\{p_i := 1\}, \quad \pi\{p_i := 0\}$$

gives us proofs of

$$p_i, L_{i+1}(\pi) \Rightarrow \phi \text{ and } \neg p_i, L_{i+1}(\pi) \Rightarrow \phi,$$

since ϕ is a tautology; and from these two proofs we easily get a proof of $L_{i+1}(\pi) \Rightarrow \phi$ in $\mathbf{G}_{\text{prop}}$, which uses a Cut. The proof is completed by appealing to the propositional case of the Hauptsatz 3C.1. $\dashv$

Proposition 3E.3. *For every valid, quantifier-free τ-formula ϕ with n, distinct prime subformulas $\phi_1, \ldots, \phi_n$ and no occurrence of the identity symbol $=$, there is a propositional tautology ψ with n distinct propositional variables such that*

$$\phi \equiv \psi\{p_1 :\equiv \phi_1, \ldots, p_n :\equiv \phi_n\}.$$

3F. Craig Interpolation and Beth definability (via proofs)

The midsequent of a normal proof in **G** is a valid, quantifier-free formula, and so (by Proposition 3E.3), it can be obtained from a propositional tautology by replacing the propositional variables by prime formulas. This fact can be used to derive several interesting results about $\mathbb{FOL}$ from their propositional versions, which are generally much easier to establish. We illustrate the process here with two, basic results about first order definability.

Theorem 3F.1 (The Propositional Interpolation Theorem)**.** *Suppose*

$$\phi(\vec{p}, \vec{q}) \to \psi(\vec{p}, \vec{r})$$

is a propositional tautology, where we have indicated all the (distinct) letters which may occur in the formulas, and there is at least one p_i; then there exists a formula $\chi(\vec{p})$ in which none of the q's or r's occur, such that

$$\phi(\vec{p}, \vec{q}) \to \chi(\vec{p}), \quad \chi(\vec{p}) \to \psi(\vec{p}, \vec{r})$$

are both tautologies.

For an example: if the given tautology is

$$p \mathbin{\&} q \to p \vee r,$$

we can take $\chi \equiv p$, with which both $p \mathbin{\&} q \to p$ and $p \to p \vee r$ are tautologies. In fact this is the interpolant which will come out of the general proof in this case.

OUTLINE OF PROOF. If no assignment π satisfies ϕ, we can then take

$$\chi(\vec{p}) \equiv p_i \mathbin{\&} \neg p_i$$

with the assumed p_i which occurs in both ϕ and ψ. So we may assume that at least one assignment satisfies ϕ.

Generalizing the definition of lines in (71) and making explicit the implied conjunction, we set for each assignment π,

$$L(\pi, \vec{p}) \equiv \bigwedge \mathrm{Line}_\pi(\vec{p}) \equiv \pi p_1 \mathbin{\&} \pi p_2 \mathbin{\&} \cdots \mathbin{\&} \pi p_n.$$

Notice that, immediately from the definition,

$$\mathrm{value}(L(\pi, \vec{p}), \pi) = 1.$$

We now take $\chi(\vec{p})$ to be the disjunction of these conjunctions over all assignments π which satisfy ϕ:

$$\chi(\vec{p}) \equiv \bigvee\!\!\!\!\bigvee\{L(\pi,\vec{p}) \mid \mathrm{value}(\phi,\pi)=1\}.$$

Clearly, $\phi \to \chi(\vec{p})$ is a tautology, because if $\mathrm{value}(\pi,\phi)=1$, then $L(\pi,\vec{p})$ is one of the disjuncts of $\chi(\vec{p})$ and π satisfies it. For the second claim, suppose towards a contradiction that there is a π such that

$$\mathrm{value}(\chi(\vec{p}),\pi)=1, \quad \text{and} \quad \mathrm{value}(\psi,\pi)=0;$$

now the definition of $\chi(\vec{p})$ implies that $\mathrm{value}(\phi,\pi)=1$, and so $\mathrm{value}(\psi,\pi)=1$ by the hypothesis, which is a contradiction. $\dashv$

Theorem 3F.2 (The Craig Interpolation Theorem)**.** *Suppose*

$$\phi(\vec{Q}) \to \psi(\vec{R}) \tag{72}$$

is valid, where the formulas $\phi(\vec{Q})$ and $\psi(\vec{R})$ may have symbols from some signature τ in addition to the (fresh, distinct) symbols exhibited. From a proof of (72)*, we can construct a formula χ in $\mathbb{FOL}(\tau)$ and proofs of the implications*

$$\phi(\vec{Q}) \to \chi, \quad \chi \to \psi(\vec{R}).$$

Outline of the proof. The argument involves some unavoidable detail, primarily to deal with the identity symbol $=$ about which the Gentzen system knows nothing.

We start with the construction of prenex formulas $\phi'(\vec{Q})$ and $\psi'(\vec{R})$ such that the equivalences

$$\phi(\vec{Q}) \leftrightarrow \phi'(\vec{Q}), \quad \psi(\vec{R}) \leftrightarrow \psi'(\vec{R})$$

are valid and no variable occurs both free and bound in the (assumed valid) implication

$$\phi'(\vec{Q}) \to \psi'(\vec{R}).$$

By Theorem 3A.10 (the Semantic Completeness of **G**),

$$\mathbf{G} \vdash \mathrm{IA}(\tau), \mathrm{IA}(\vec{Q}), \mathrm{IA}(\vec{R}) \Rightarrow \phi'(\vec{Q}) \to \psi'(\vec{R}),$$

where $\mathrm{IA}(\tau)$, $\mathrm{IA}(\vec{Q}), \mathrm{IA}(\vec{R})$ are the identity axioms for the relation and function symbols which occur in τ, $\phi'(\vec{Q})$ and $\psi'(\vec{R})$ (in prenex form); and then, easily,

$$\mathbf{G} \vdash \mathrm{IA}(\tau), \mathrm{IA}(\vec{Q}), \phi'(\vec{Q}) \Rightarrow (\mathrm{IA}(\vec{R}) \to \psi'(\vec{R})). \tag{73}$$

We now replace the identity symbol $=$ by a fresh, binary relation symbol E, i.e., we replace each prime formula of the form $t = s$ by $E(t,s)$, to obtain formulas

$$\mathrm{IA}(E,\tau), \mathrm{IA}(E,\vec{Q}), \phi'(E,\vec{Q}), \mathrm{IA}(E,\vec{R}), \psi'(E,\vec{R});$$

and since the proof in $\mathbf{G}$ which establishes (73) does not use any special properties of the identity symbol, if we replace $=$ by E in it, we get

$$\mathbf{G} \vdash \mathrm{IA}(E,\tau), \mathrm{IA}(E,\vec{Q}), \phi'(E,\vec{Q}) \Rightarrow (\mathrm{IA}(E,\vec{R}) \rightarrow \psi'(E,\vec{R})).$$

We now apply the Extended Hauptsatz to get a normal proof Π of this sequent. The midsequent

$$A^* \Rightarrow B^*$$

of Π is a valid, quantifier-free sequent with no occurrence of $=$, and so (easily, by Proposition 3E.3), there is a valid propositional sequent

$$A^{**} \Rightarrow B^{**}$$

from which $A^* \Rightarrow B^*$ can be obtained by replacing its propositional variables with prime formulas. Moreover, prime formulas which involve symbols in $\vec{Q}$ occur only in A^{**}, and prime formulas which involve symbols in $\vec{Q}$ occur only in B^{**}, and so by the Propositional Interpolation Theorem 3F.1, there is a (τ, E)-formula χ^{**} such that

$$\mathbf{G} \vdash A^{**} \Rightarrow \chi^{**}; \qquad \mathbf{G} \vdash \chi^{**} \Rightarrow B^{**}.$$

If we now replace back E by $=$, we get a τ-formula χ^* such that

$$\mathbf{G} \vdash A^* \Rightarrow \chi^*, \qquad \mathbf{G} \vdash \chi^* \Rightarrow B^*. \tag{74}$$

This completes the preparation or the proof. In the main argument, *we apply to each of these two sequents* (essentially) *the same sequence of quantifier rule applications and contractions which are used to get* $\mathrm{IA}(E,\vec{Q}), \phi'(E,\vec{Q}) \Rightarrow (\mathrm{IA}(E,\vec{R}) \rightarrow \psi'(E,\vec{R}))$ from $A^* \Rightarrow B^*$, to obtain in the end a new τ-formula χ and and proofs of the required

$$\mathbf{G} \vdash \mathrm{IA}(\tau), \mathrm{IA}(\vec{Q}) \;\&\; \phi(\vec{Q}) \Rightarrow \chi, \quad \mathbf{G} \vdash \chi \Rightarrow (\mathrm{IA}(\vec{R}) \rightarrow \psi(\vec{R})). \qquad \dashv$$

Theorem 3F.3 (The Beth Definability Theorem). *Suppose $\phi(R)$ is a sentence in $\mathbb{FOL}(\tau \cup \{R\})$, where the n-ary relation symbol R is not in the signature τ, and the sentence*

$$\phi(R) \;\&\; \phi(S) \rightarrow (\forall \vec{x})[R(\vec{x}) \leftrightarrow S(\vec{x})]$$

is provable (or equivalently valid). From any proof of it we can construct a $\chi(\vec{x})$ in $\mathbb{FOL}(\tau)$ such that

$$\phi(R) \rightarrow (\forall \vec{x})[R(\vec{x}) \leftrightarrow \chi(\vec{x})]$$

is provable.

The Beth Theorem says that *implicit first order definability* coincides with *explicit first order definability.* In addition to their obvious foundational significance, both of these results are among the most basic of Model Theory, with many applications.

3G. The Hilbert program

The discovery of paradoxes in set theory (especially the Russell Paradox) in the beginning of the 20th century created a “foundational crisis” in mathematics which was not completely resolved until the middle 1930s. There were essentially three main responses to it:

(1) *Axiomatic set theory.* Introduced by Zermelo in 1908 in direct response to the paradoxes, this led rapidly to substantial mathematical developments, and eventually to a new notion of *grounded set* which replaced Cantor's intuitive approach and, in a sense, “justified the axioms”: in any case, no contradictions have been discovered in *Zermelo-Fraenkel set theory* since its formalization was complete in the 1930s. Working “within ZFC” is now the standard, “mathematical” approach to the foundations of mathematics.

(2) *Constructive mathematics* (intuitionism), advocated primarily by Brouwer. This rejected set theory and classical logic as “meaningless”, and attempted to reconstruct a new kind of mathematics on constructive principles. It did not succeed in replacing classical mathematics as the language of science, but it has influenced deeply the philosophy of mathematics.

(3) *Formalism*, introduced by Hilbert, who formulated the *Hilbert program*, a sequence of mathematical conjectures whose proof would solve the problem posed by the paradoxes. The basic elements of the Hilbert Program (vastly oversimplified) are as follows:

Step 1. Formulate mathematics (or a substantial part of it) as a *formal, axiomatic theory* T, so it can be studied as a mathematical object using standard, combinatorial techniques.

Our modern conception of formal, first-order logic, with its precisely defined terms, formulas, proofs, etc., was developed as part of this first step of the Hilbert Program—it had never been so rigorously formulated before.

Step 2. Prove that T is *complete*: i.e., for each sentence θ of T,

$$\text{either } T \vdash \theta \ \text{ or } \ T \vdash \neg\theta.$$

Step 3. Prove that T is consistent, i.e., there is not sentence θ such that

$$T \vdash \theta \ \text{ and } \ T \vdash \neg\theta.$$

Basic methodological principle: the proofs in the last two steps must be *finitistic*, i.e., (roughly) constructive, utterly convincing combinatorial arguments about finite objects, such as natural numbers, symbols, strings of symbols and the like. There is no attempt to define rigorously the pre-mathematical notion of *finitistic proof*: it is assumed that we can recognize a finitistic argument—and be convinced by it—when we see it.

The basic idea is that if Steps 1 – 3 can be achieved, then *truth* can be replaced in mathematics by *proof*, so that metaphysical questions (like *what is a set*) are simply by-passed.

Hilbert and his school worked on this program as mathematicians do, trying first to complete it for weak theories T and hoping to develop methods of proof which would eventually apply to number theory, analysis and even set theory. They had some success, and we will examine two representative results in Sections 3H and 3J. But Gödel's fundamental discoveries in the 1930s established conclusively that the Hilbert Program cannot go too far. They will be our main concern.

It should be emphasized that the notions and methods introduced as part of the Hilbert Program have had an extremely important role in the development of modern, mathematical logic, and even Gödel's work depends on them: in fact, Gödel proved his fundamental results in response to questions which arose (explicitly or implicitly) in the Hilbert Program.

3H. The finitistic consistency of Robinson's Q

Robinson's Q was defined in 1G.11. We introduce its *Skolemized version* Q_s, which has an additional (unary) function symbol Pd and for axioms (in full) the universal closures of the following formulas:

1. $\neg[S(x) = 0]$.
2. $S(x) = S(y) \rightarrow x = y$.
3. $x + 0 = x,\ x + S(y) = S(x + y)$.
4. $x \cdot 0 = 0,\ x \cdot (Sy) = x \cdot y + x$.
5. $\mathrm{Pd}(0) = 0$.
6. $\mathrm{Pd}(S(x)) = x$.
7. $x = 0 \vee x = S(\mathrm{Pd}(x))$.
8. $x = x \ \&\ (x = y \rightarrow y = x) \ \&\ [(x = y \ \&\ y = z) \rightarrow x = z]$.
9. $x = y \rightarrow [S(x) = S(y) \ \&\ \mathrm{Pd}(x) = \mathrm{Pd}(y)]$.
10. $(x = y \ \&\ u = v) \rightarrow [x + u = y + v \ \&\ x \cdot u = y \cdot v$.

Aside from the explicit inclusion of the relevant Axioms of Identity, the basic difference between Q and Q_s is that all the axioms of Q_s are universal sentences, while the characteristic axiom

$$\forall x[x = 0 \vee (\exists y)[x = S(y)]]$$

of Q has an existential quantifier in it. Axiom 7 of Q_s is the "Skolemized version" of the Robinson axiom; in this case we can obviously see that the

"Skolem function" $\mathrm{Pd}(x)$ is the predecessor function

$$\mathrm{Pd}(x) = \begin{cases} 0, & \text{if } x = 0, \\ x - 1, & \text{otherwise.} \end{cases} \tag{75}$$

However, this *Skolemization* which eliminates existential quantifiers by introducing new function symbols can be done in arbitrary sentences, and in each case we can prove the analog of the following, simple fact:

Lemma 3H.1. *We can prove in* $\mathbf{G}$ *the sequent*

$$\forall x[x = 0 \vee x = S(\mathrm{Pd}((x)))] \Rightarrow \forall x[x = 0 \vee (\exists y)[x = S(y)]],$$

and so for any sentence θ*,*

$$\textit{if } \mathbf{G} \vdash \mathsf{Q} \Rightarrow \theta, \textit{ then } \mathbf{G} \vdash \mathsf{Q}_s \Rightarrow \theta.$$

It follows that if Q_s *is consistent, then so is* Q*.*

Theorem 3H.2. *Robinson's theory* Q *is* (finitistically) *consistent.*

OUTLINE OF PROOF. We assume, towards a contradiction that (with $1 = S(0)$), $\mathsf{Q}_s \vdash 0 = 1$, so that there is a proof in $\mathbf{G}$ of the sequent

$$\mathsf{Q}_s \Rightarrow 0 = 1;$$

and since all the axioms on Q_s are prenex, by the Extended Hauptsatz, there is a normal proof of this sequent. Consider the midsequent of such a normal proof: it is of the form

$$\theta_1, \ldots, \theta_n \Rightarrow 0 = 1$$

where each θ_i is a substitution instance of the *matrix* of one of the axioms of Q_s, something like

$$Sx + S(u \cdot Sx) = S(Sx + (u \cdot Sx))$$

in the case of Axiom 3. Now *replace by* 0 *all the (free) variables which occur in the part of the proof above the midsequent*, so that in the example the midsequent becomes the equation

$$S0 + S(0 \cdot S0) = S(S0 + (0 \cdot S0)).$$

The (propositional) proof above the midsequent remains a proof, and it establishes the sequent

$$\theta_1^*, \ldots, \theta_n^* \Rightarrow 0 = 1$$

where each θ_i^* is a *numerical identity.* But these numerical identities are all true with the standard interpretation of the symbols $0, S, +, \mathrm{Pd}, \cdot$; and so we cannot have a proof by logic alone which leads from them to the obviously false identity $0 = 1$. $\dashv$

Discussion: In some sense, all we have done is to say that we have a model of Q_s, and hence the theory must be consistent. The "finitistic" justification for the proof is that (1), the model is *constructive*—its universe is the set $\mathbb{N}$ of natural numbers, we can compute all the values of the functions $S, \mathrm{Pd}, +, \cdot$ involved, and we can verify numerical equations among them; and (2), we only need to understand and accept finitely many numerical instances of universal sentences, which we can verify "by hand". In other words, all we need to believe about the natural numbers is that we can define $Sx, \mathrm{Pd}(x), x{+}y$ and $x{\cdot}y$ on some initial segment of $\mathbb{N}$ (comprising the specific numbers which occur in the assumed contradictory midsequent) so that their basic, numerically verifiable identities are true. The Extended Hauptsatz is used precisely to replace a general understanding of "truth in $(\mathbb{N}, 0, S, +, \cdot)$" for arbitrary sentences with quantifiers by this limited understanding of "numerical truth".

3I. Primitive recursive functions

We introduce here and establish the basic properties of the *primitive recursive* functions and relations on $\mathbb{N}$, which have numerous applications in many parts of logic.

3I.1. We will use the following specific functions on $\mathbb{N}$:

1. The successor, $S(x) = x + 1$.
2. The n-ary constants, $C^n_q(\vec{x}) = q$.
3. The projections, $P^n_i(x_1, \dots , x_n) = x_i$, $(1 \le i \le n)$. Notice that $P^1_1(x) = id(x)$ is the identity.

Definition 3I.2. A function $f : \mathbb{N}^n \to \mathbb{N}$ is defined by **composition** from given functions h, $g_1, \dots , g_m$, if for all $\vec{x} \in \mathbb{N}^n$,

$$f(\vec{x}) = h(g_1(\vec{x}), \dots , g_m(\vec{x})).$$

Here f and all the g_i are n-ary and h is m-ary. Example:

$$f(x) = x + x = +(id(x), id(x)) = 2x$$

is a composition of addition with the identity (taken twice). The function

$$S^2_1(x, y) = S(P^2_1(x, y)) = x + 1$$

is the binary function which adds 1 to its first argument.

A function f is defined by **primitive recursion** from h, g, if for all $y, \vec{x} \in \mathbb{N}^n$,

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

Here f is $n+1$-ary, g is n-ary and h is $n+2$-ary. We also include (by convention) the degenerate case where g is just a number and a unary function is being defined:

$$f(0) = q,$$
$$f(y+1) = h(f(y), y).$$

Examples: if

$$f(0, x) = id(x) = x, \quad f(y+1, x) = S^2_1(f(y, x), y),$$

then (by an easy induction on y),

$$f(y, x) = y + x.$$

Definition 3I.3. The class of **primitive recursive functions** is the smallest set of functions (of all arities) on $\mathbb{N}$ which contains the successor S, the constants C^n_q, and the projections P^n_i, and which is closed under composition and primitive recursion.

A relation $R \subseteq \mathbb{N}^k$ is **primitive recursive** if its characteristic function is, where

$$\chi_R(\vec{x}) = \begin{cases} 1, & \text{if } R(\vec{x}), \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 3I.4. (1) *If* $\mathbf{A} = (\mathbb{N}, f_0, \dots, f_k)$ *where* $f_0, \dots, f_k$ *are primitive recursive and* f *is* $\mathbf{A}$*-explicit, then* f *is primitive recursive.*

(2) *Primitive recursive functions and relations are arithmetical.*

PROOF is easy, using Theorems 1D.2 (the closure properties of $\mathcal{E}(\mathbf{A})$) and 1E.2. $\dashv$

3I.5. A **primitive recursive derivation** is a sequence of functions

$$f_0, f_1, \dots, f_k,$$

where each f_i is S, a constant C^n_q or a projection P^n_i, or is defined by composition or primitive recursion from functions before it in the sequence.

Lemma 3I.6. *A function is primitive recursive if and only of it occurs in some primitive recursive derivation.*

Lemma 3I.7. *The following functions are primitive recursive.*

1. $x + y$.
2. $x \cdot y$.
3. $x! = 1 \cdot 2 \cdot 3 \cdots x$, *with* $0! = 1$.
4. $\mathrm{pd}(x) = x - 1$, *with* $pd(0) = 0$.
5. $x \dot{-} y = \max(0, x - y)$.
6. $\min(x, y)$.
7. $\min(x_1, \dots, x_n)$.
8. $\max(x, y)$.

9. $\max(x_1, \ldots, x_n)$.
10. $\max(x_1, \ldots, x_n)$.
11. $\mathrm{bit}(x) = \begin{cases} 0, & \textit{if } x = 0, \\ 1, & \textit{if } x > 0. \end{cases}$
12. $\overline{\mathrm{bit}}(x) = 1 \dot{-} \mathrm{bit}(x)$.

Lemma 3I.8. *If h is primitive recursive, then so are f and g where:*
(1) $f(x, \vec{y}) = \sum_{i<x} h(i, \vec{y})$, $(= 0$ when $x = 0)$.
(2) $g(x, \vec{y}) = \prod_{i<x} h(i, \vec{y})$, $(= 1$ when $x = 0)$.

Proof is left for Problem x4.1. ⊣

Lemma 3I.9 (Closure properties of primitive recursive relations)**.** (1) *The identity relation $x = y$ is primitive recursive.*

(2) *The negation of a primitive recursive relation is primitive recursive; and the conjunction of primitive recursive relations is primitive recursive.* (So the class of primitive recursive relations is closed under all propositional logic operations.)

(3) *If $P(i, \vec{y})$ is primitive recursive, then so are the relations defined from it by bounded quantification:*

$$Q(x, \vec{y}) \iff_{\mathrm{df}} (\exists i < x) P(i, \vec{y}),$$
$$R(x, \vec{y}) \iff_{\mathrm{df}} (\forall i < x) P(i, \vec{y}).$$

(4) *If P and $f_1, \ldots, f_k$ are primitive recursive, then so is the relation*

$$R(\vec{x}) \iff_{\mathrm{df}} P(f_1(\vec{x}), \ldots, f_k(\vec{x})).$$

(5) *If R is primitive recursive, then so is the function*

$$f(x, \vec{y}) = (\mu i < x) R(i, \vec{y});$$

here μi is read "the least i", and if there is no $i < x$ which satisfies $R(i, \vec{y})$, then $f(x, \vec{y}) = x$.

Lemma 3I.10. *The following functions and relations are primitive recursive.*
(1) $\mathrm{quot}(x, y) =$ the (integer) quotient of x by y, *set* $= 0$ *if* $y = 0$.
(2) $\mathrm{rem}(x, y) =$ the remainder of the division of x by y, set $= x$ if $y = 0$.
(3) $\mathrm{Prime}(x) \iff x > 1$ & x has no divisors other than 1 and itself.
(4) $p(i) = p_i =$ the i'th prime number.

For $y > 0$, the integer quotient $q = \mathrm{quot}(x, y)$ and remainder $r = \mathrm{rem}(x, y)$ are the unique natural numbers which satisfy

$$x = yq + r, \quad 0 \leq r < y.$$

Next we introduce a coding of tuples from $\mathbb{N}$ which is more convenient than the one we defined using the β-function in Section 1E.

3I.11. Definition. A **coding** of a set X in the set C is any injective (one-to-one) function $\pi : X \rightarrowtail C$.

With each coding $\langle\ \rangle : \mathbb{N}^* \rightarrowtail \mathbb{N}$ of the finite sequences of numbers into the numbers, we associate the following functions and relations:

1. $\langle x_1, \dots, x_n\rangle_n = \langle x_1, \dots, x_n\rangle$, the n-ary function (for each fixed n) which codes n-tuples, for very n including $n = 0$: so $\langle \epsilon \rangle$ is some fixed number, the code of the empty tuple. (In using this notation, we never write the n.)
2. $\mathrm{Seq}(w) \iff_{\mathrm{df}} (\exists x_0, \dots, x_{n-1})[w = \langle x_0, \dots, x_{n-1}\rangle]$, the *sequence coding relation*.
3. $\mathrm{lh}(w) = n$, if $w = \langle x_0, \dots, x_{n-1}\rangle$, the *length function* (=0 if w is not a sequence number).
4. $\mathrm{proj}(w, i) = (w)_i = x_i$, if $w = \langle x_0, \dots, x_{n-1}\rangle$ and $i < n$, the *projection function* (=0 if w is not a sequence number or $i \geq \mathrm{lh}(w)$).
5. $\mathrm{append}(u, t) = \langle x_0, \dots, x_{n-1}, t\rangle$ if $u = \langle x_0, \dots, x_{n-1}\rangle$, $= 0$ otherwise.

A sequence coding on the set $\mathbb{N}$ of numbers is **primitive recursive** if these associated functions and relations are all primitive recursive.

The *restriction* of a sequence code u to its first i elements is defined by the primitive recursion

$$u \restriction 0 = \langle \epsilon \rangle, \quad u \restriction (i+1) = \mathrm{append}(u \restriction i, (u)_i), \tag{76}$$

so that

$$\langle u_0, \dots, u_{n-1}\rangle \restriction i = \langle u_o, \dots, u_{i-1}\rangle \quad (i < n).$$

Using the appending function, we can also define by primitive recursion the *concatenation* of codes of sequences, setting

$$\begin{aligned} f(0, u, v) &= u, \\ f(i+1, u, v) &= \mathrm{append}(f(i, u, v), (v)_i), \\ u * v &= f(\mathrm{lh}(v), u, v). \end{aligned} \tag{77}$$

It follows easily that when u, v are sequence codes, then $u * v$ codes their concatenation.

Lemma 3I.12. *The following function on $\mathbb{N}^*$ is a primitive recursive coding:*

$$\langle \epsilon \rangle = 1 \quad \text{(the code of the empty tuple is 1)}$$
$$\langle x_0, \dots, x_n\rangle = p_0^{x_0+1} \cdot p_1^{x_1+1} \cdots p_n^{x_n+1} \quad (n \geq 0).$$

It satisfies the following additional properties for all $x_0, \dots, x_{n-1}$ and all sequence codes u, v, w:

$$x_i < \langle x_0, \dots, x_{n-1}\rangle, \quad (i < n),$$
$$\textit{if } v, u * w \neq 1, \textit{ then } v < u * v * w.$$

This is the *standard* or *prime power coding* of tuples from $\mathbb{N}$.

Lemma 3I.13 (Complete Primitive Recursion). *Suppose g is primitive recursive, $\langle\ \rangle$ is a primitive recursive coding of tuples and the function f satisfies the identity*

$$f(x) = g(x, \langle f(0), \dots, f(x-1)\rangle);$$

it follows that f is primitive recursive.

Similarly with parameters, when

$$f(x, \vec{y}) = g(x, \vec{y}, \langle f(0, \vec{y}), \dots, f(x-1, \vec{y})\rangle).$$

Proof. The function

$$\overline{f}(x) = \langle f(0), \dots, f(x-1)\rangle$$

satisfies the identities

$$\overline{f}(0) = \langle \epsilon \rangle,$$
$$\overline{f}(x+1) = \overline{f}(x) * \langle g(x, \overline{f}(x))\rangle,$$

so that it is primitive recursive; and then

$$f(x) = (\overline{f}(x+1))_x. \qquad \dashv$$

Lemma 3I.14. *If $\langle\ \rangle_1$ and $\langle\ \rangle_2$ are primitive recursive number codings of tuples, then there exists a primitive recursive function $\pi : \mathbb{N} \to \mathbb{N}$ which computes one coding from the other, i.e. for all sequences,*

$$\pi(\langle x_0, \dots, x_{n-1}\rangle_1) = \langle x_0, \dots, x_{n-1}\rangle_2.$$

This result often allows us to establish results about the simple, standard, power coding of Lemma 3I.12 and then infer that they hold for all primitive recursive codings. The standard coding is very inefficient, and much better primitive recursive codings exist, cf. Problems x4.6* − x4.9; but we are not concerned with efficiency here, and so, to simplify matters, **we adopt the standard power coding of tuples** for these notes, so that we may use without mention its special properties listed in Lemma 3I.12.

3J. Further consistency proofs

We outline here the proof of (basically) the strongest consistency result which can be shown finitistically.

Definition 3J.1 (Primitive Recursive Arithmetic, I). For each primitive recursive derivation

$$\vec{f} = (f_0, \dots, f_k),$$

we define a formal axiomatic system PRA($\vec{f}$) as follows.

(1) The signature of $\mathrm{PRA}(\vec{f})$ has the constant 0, the successor symbol S, the predecessor symbol Pd, function symbols for $f_1, \ldots, f_k$ and the identity symbol $=$. (This is an $\mathbb{FOL}$ theory.) We assume the identity axioms for the function symbols in the signature, the two axioms for the successor,

$$S(x) \neq 0, \quad S(x) = S(y) \to x = y,$$

and the three axioms for the predecessor:

$$\mathrm{Pd}(0) = 0, \quad \mathrm{Pd}(S(x)) = x, \quad x \neq 0 \vee x = S(\mathrm{Pd}(x)).$$

(2) For each f_i we have its *defining equations* which come from the derivation as axioms. For example, if $f_3 = C^3_2$, then the corresponding axiom is

$$f_3(x, y, z) = S(S(0)).$$

If f_i is defined by primitive recursion from preceding functions f_l, f_m, we have the corresponding axioms

$$\begin{aligned} f_i(0, \vec{x}) &= f_l(\vec{x}), \\ f_i(S(y), \vec{x}) &= f_m(f_i(y, \vec{x}), y, \vec{x}). \end{aligned}$$

(3) *Quantifier free induction scheme.* For each quantifier free formula $\phi(y, \vec{z})$ we take as axiom the universal closure of the formula

$$\phi(0, \vec{z}) \;\&\; (\forall y)[\phi(y, \vec{z}) \to \phi(S(y), \vec{z})] \;\to\; \forall x \phi(x, \vec{z}).$$

Notice that from the axiom

$$x = 0 \vee x = S(\mathrm{Pd}(x))$$

relating the successor and the predecessor functions, we can get immediately (by $\exists$-elimination) the Robinson axiom

$$x = 0 \vee (\exists y)[x = S(y)],$$

so that all the axioms of the Robinson system Q defined in **3.10** are provable in $\mathrm{PRA}(\vec{f})$, once the primitive recursive derivation $\vec{f}$ includes the defining equations for addition and multiplication.

The term **primitive recursive arithmetic** is used loosely for the "union" of all such $\mathrm{PRA}(\vec{f})$. More precisely, we say that a proposition can be *expressed and proved* in primitive recursive arithmetic, if it can be formalized and proved in some $\mathrm{PRA}(\vec{f})$.

Definition 3J.2 (Primitive Recursive Arithmetic, II)**.** For each primitive recursive derivation $\vec{f}$, let $\mathrm{PRA}^*(\vec{f})$ be the axiomatic system with the same signature as $\mathrm{PRA}(\vec{f})$ and with axioms (1) and (2) above, together with

(3)* For each of the function symbols h in the signature,

$$\{h(0, \vec{z}) = 0 \mathbin{\&} (\forall y)[h(S(y), \vec{z}) = S(h(y, \vec{z}))]\} \rightarrow (\forall x)[h(x, \vec{z}) = x]. \tag{78}$$

Theorem 3J.3 (Key Lemma)**.** *For each primitive recursive derivation $\vec{f}$, the system* PRA*$(\vec{f})$ *is* (finitistically) *consistent.*

Proof. First we replace the new axiom (78), for each function symbol h by its "Skolemized form"

$$(\forall x)\Big[\{h(0, \vec{z}) = 0 \mathbin{\&} [h(S(g_h(x, \vec{z})), \vec{z}) = S(h(g_h(x, \vec{z}), \vec{z})]\} \rightarrow h(x, \vec{z}) = x\Big], \tag{79}$$

where g_h is a new function symbol. This axiom easily implies (78), by $\exists$-elimination: so it is enough to show that this system PRA**$(\vec{f})$ is consistent.

If the system PRA**$(\vec{f})$ is inconsistent, then it proves $0 = 1$, so by the Extended Hauptsatz we have a normal proof with endsequent

$$\phi_1, \dots, \phi_n \Rightarrow 0 = 1,$$

where each ϕ_i is either one of the basic axioms about the successor S and the predecessor Pd, a (universally quantified) defining equation for one of the primitive recursive functions in $\vec{f}$, or (79) for some $h = f_i$. The midsequent of this proof is of the form

$$\psi_1, \dots, \psi_m \Rightarrow 0 = 1,$$

where now each ψ_i is a (quantifier free) substitution instance of the matrix of some ϕ_j. *We now replace all variables above the midsequent by* 0; what we get is a propositional proof whose conclusion

$$\psi_1^*, \dots, \psi_m^* \Rightarrow 0 = 1$$

has on the left a sequence of closed, quantifier free sentences, each of them making a numerical assertion about S, Pd, the primitive recursive functions f_i and the (still unspecified) functions g_h. If we define

$$g_h(x, \vec{z}) = \max\{y \leq x : h(y, \vec{z}) = y\},$$

then we can recognize immediately that for any x,

$$h(x, \vec{z}) \neq x \Longrightarrow h(g_h(x, \vec{z})) \neq g_h(x, \vec{z}),$$

and from this it is immediate that all these numerical assertions in the midsequent are true: for example, a typical sentence in the left of the midsequent might be

$$f_2(f_5(S(0)), S(0) = f_1(S(0), 0),$$

which can be verified by computing the numerical values of the functions involved from their (primitive recursive) definitions and then just checking. On the other hand, the right of the midsequent has the single false assertion $0 = 1$, which is absurd. $\dashv$

Remark: In effect all we have done is to say that we have a model for $\mathrm{PRA}^{**}(\vec{f})$, and hence the theory must be consistent. The "finitistic" justification for the proof is that (1), the model is constructive—we can compute all the values of the functions involved, and we can verify numerical equations among them; and (2), we only need understand the truth of closed (numerical) quantifier free sentences about the model, not arbitrary sentences with quantifiers. The Extended Hauptsatz is used precisely to allow us to deal with quantifier free sentences rather than arbitrary ones.

Lemma 3J.4. *For each primitive recursive derivation $\vec{f}$ and each quantifier free formula $\phi(x, \vec{z})$ in its language, we can find a longer derivation $\vec{f}, h, \vec{g}$ such that the theory $T = \mathrm{PRA}^*(\vec{f}, h, \vec{g})$ proves the instance of quantifier free induction*

$$\phi(0, \vec{z}) \ \&\ (\forall y)[\phi(y, \vec{z}) \to \phi(S(y), \vec{z})] \to (\forall x)\phi(x, \vec{z}).$$

Outline of proof. We skip the parameters $\vec{z}$.

Consider again the Skolemized version of the given instance of quantifier free induction

$$\phi(0) \ \&\ [\phi(h(x)) \to \phi(S(h(x)))] \to \phi(x) \tag{80}$$

which implies easily the non-Skolemized form; so it suffices to find a primitive recursive derivation with a letter h in it so that the theory T proves (80). The idea is to take the function h defined by the following primitive recursion.

$$\begin{aligned} h(0) &= 0, \\ h(S(y)) &= \begin{cases} S(h(y)), & \text{if } \phi(h(y)) \ \&\ \phi(S(h(y))), \\ h(y), & \text{if } \phi(h(y)) \ \&\ \neg\phi(S(h(y))), \\ 0, & \text{if } \neg\phi(h(y)). \end{cases} \end{aligned}$$

We omit the details of the proof that this h is primitive recursive, and that in the theory T which includes its primitive recursive derivation we can establish the following theorems, which express the cases in its definition.

$$\phi(h(y)) \ \&\ \phi(S(h(y))) \to h(S(y)) = S(h(y)), \tag{81}$$

$$\phi(h(y)) \ \&\ \neg\phi(S(h(y))) \to S(h(y)) = h(y), \tag{82}$$

$$\neg\phi(h(y)) \to h(S(y)) = 0. \tag{83}$$

Once we have these theorems from T, we assume the hypothesis

$$\phi(0), \phi(h(x)) \to \phi(S(h(x))) \tag{84}$$

of the implication to prove and we argue as follows, within T.

(1) $(\forall x)\phi(h(x))$. By Robinson's property, either $x = 0$, and then $h(0) = 0$ and $\phi(0)$ give the result, of $x = S(y)$ for some y, and then we can verify the conclusion taking cases in the hypothesis of (81) - (83).

(2) $(\forall y)[h(S(y)) = S(h(y))]$. This follows now from (81) – (83), since (83) cannot occur by (1) and (82) cannot occur by the hypothesis (84).

(3) $(\forall x)[h(x) = x]$, by $h(0) = 0$ and (2), together with the last axiom of T.

From (1) and (3) now we get the required $(\forall x)\phi(x)$. ⊣

Remark: It is important, of course, that no induction is used in this proof, only the consideration of cases.

Theorem 3J.5 (Main Consistency Result). *For each primitive recursive derivation $\vec{f}$, the system* PRA($\vec{f}$) *is* (finitistically) *consistent.*

Primitive recursive arithmetic is much more powerful than it might appear. As an example, here is one of its theorems.

Proposition 3J.6. *In the system* PRA(+) *(with the defining axioms for addition) we can prove that + is associative and commutative,*

$$x + (y + z) = (x + y) + z, \quad x + y = y + x.$$

This cannot be proved in Robinson's Q.

3K. Problems for Chapter 3

Problem x3.1. Prove Theorem 3A.10, the (strong) Semantic Completeness of **G**.

Problem x3.2. Suppose Π is a Cut-free proof in **G** of a sequent $\Rightarrow \phi$, where ϕ is in prenex form and has n quantifiers; prove that every formula in Π is prenex with at most n quantifiers.

Problem x3.3. Suppose Π is a Cut-free proof in **G** with endsequent $A \Rightarrow B$, in which there are no applications of the (four) logical rules that involve the symbols $\neg$ and $\rightarrow$. Prove that every formula ϕ which occurs on the left of some sequent in Π is a subformula of some formula in A; and every formula ψ which occurs on the right of some sequent in Π is a subformula of some formula in B.

Problem x3.4. Construct a Cut-free **GI** proof of

$$(\phi \rightarrow \psi) \rightarrow ((\phi \rightarrow \neg\psi) \rightarrow \neg\phi)$$

Problem x3.5. Construct a Cut-free **GI** proof of

$$(\phi \to \chi) \to ((\psi \to \chi) \to ((\phi \vee \psi) \to \chi))$$

Problem x3.6. Construct a Cut-free **G** proof of *Peirce's Law*,

$$(((p \to q) \to p) \to p)$$

Problem x3.7. Prove each of the following sequents in **G**, if possible in **GI**.

1. $\neg(\phi \ \&\ \psi) \ \Rightarrow\ \neg\phi \vee \neg\psi$.
2. $\neg\phi \vee \neg\psi \ \Rightarrow\ \neg(\phi \ \&\ \psi)$.
3. $\Rightarrow\ \phi \vee \neg\phi$.
4. $\neg\neg\neg\phi \ \Rightarrow\ \neg\phi$.

Problem x3.8. Prove each of the following sequents in **G**, if possible in **GI**.

1. $\exists x R(x) \ \Rightarrow\ \neg\forall x \neg R(x)$.
2. $\neg\forall x \neg R(x) \ \Rightarrow\ \exists x R(x)$.
3. $\neg\exists x \forall y) R(x, y) \ \Rightarrow\ \forall x \exists y \neg R(x, y)$.
4. $\neg\exists x \forall y) R(x, y) \ \Rightarrow\ \forall x \neg\forall y) R(x, y)$.

Problem x3.9*. Construct a proof in **GI** of the sequent

$$\forall x \forall y) R(x, y) \ \Rightarrow\ R(y, y).$$

Problem x3.10. Assume the Cut Elimination Theorem for *gentzeni* and prove that

$$\text{if } \mathbf{GI} \vdash \Rightarrow\ \phi \vee \psi, \text{ then } \mathbf{GI} \vdash \Rightarrow\ \phi \text{ or } \mathbf{GI} \vdash \Rightarrow\ \psi.$$

Problem x3.11. Prove that the sequent in Problem x3.9* does not have a Cut-free proof in **G**.

Problem x3.12*. Assume the Cut Elimination Theorem for **GI** and prove that the sequent

$$\neg\neg R(x) \ \Rightarrow\ R(x)$$

in not provable in the intuitionistic system **GI**.

Problem x3.13*. Assume the Cut Elimination Theorem for **GI** and prove all the assertions of unprovability in **GI** that you made in Problems x3.7 and x3.8.

Problem x3.14. Prove Proposition 3E.3—that every valid, quantifier-free formula can be obtained by replacing each propositional variable in some tautology by a quantifier-free formula.

Problem x3.15. Suppose $R(i,j)$ is a relation defined for $i,j \leq n$, choose a double sequence of propositional variables $\{p_{ij}\}_{i,j\leq n}$, and consider the assignment

$$\pi(p_{ij}) = \begin{cases} 1, & \text{if } R(i,j), \\ 0, & \text{otherwise.} \end{cases}$$

The variables $\{p_{ij}\}$ can be used to express various properties about the relation R, for example

$$R \text{ is symmetric} \iff \pi \models \bigwedge\!\!\!\bigwedge_{i,j\leq n}[p_{ij} \leftrightarrow p_{ji}].$$

Find similar formulas which express the following properties of R:

(a) R is the graph of a function.
(b) R is the graph of a one-to-one function.
(c) R is the graph of a surjection—a function from $\{0,\dots,n\}$ onto $\{0,\dots,n\}$.

CHAPTER 4

INCOMPLETENESS AND UNDECIDABILITY

This is the main part of this (or any other) first course in logic, in which we will establish and explain the fundamental incompleteness and undecidability phenomena of first order logic due (primarily) to Gödel. There are three "waves" of results, each requiring a little more technique than the preceding one and establishing deeper and more subtle facts about first order logic.

4A. Tarski and Gödel (First Incompleteness Theorem)

The key to Gödel theory is the method of **coding** (or *arithmetization*), which makes it possible to express properties of formulas, sentences and proofs within number theory. Here we will define these codings, establish their basic properties and use them to derive the simplest (and most basic) incompleteness results.

Recall from the proof of Theorem 1J.5 the function $n \mapsto \Delta n$ from natural numbers to terms of the language of Peano Arithmetic PA which is defined by the recursion

$$\Delta 0 \equiv 0, \quad \Delta(n+1) \equiv S(\Delta n).$$

We also set $1 \equiv \Delta 1 \equiv S(0)$, to avoid the annoying notation $\Delta 1$. These numerals provide names for all numbers and allow us to reduce satisfiability of formulas to truth of sentences for the structure $\mathbf{N}$:

Lemma 4A.1. *For every full extended formula $\phi(v_1, \dots, v_n)$ in the language of arithmetic and all number $x_1, \dots, x_n$,*

$$\mathbf{N} \models \phi[x_1, \dots, x_n] \iff \mathbf{N} \models \phi(\Delta x_1, \dots, \Delta x_n). \tag{85}$$

Proof. First we show by structural induction that for every full extended term $t(v_1, \dots, v_n)$ and any numbers $x_1, \dots, x_n$, in the notation introduced at the end of Section 1C,

$$\text{if } t^{\mathbf{N}}[x_1, \dots, x_n] = w, \text{ then } \mathbf{N} \models t(\Delta x_1, \dots, \Delta x_n) = \Delta w,$$

and then we prove the lemma by structural induction on formulas. $\dashv$

We will be using without comment synonymously the expressions at the two sides of (85), as it suits the purpose at hand.

Definition 4A.2 (Coding)**.** Let τ be a finite signature with k (relation, constant and function) symbols $s_1, \dots, s_k$. We assign numbers to the *symbols* of $\mathbb{FOL}(\tau)$ by enumerating them as follows,

$$\neg \ \rightarrow \ \ \& \ \ \vee \ \forall \ \exists \ = \ (\ ) \ , \ s_1 \ \dots \ s_k \ \mathrm{v}_0 \ \mathrm{v}_1 \ \dots$$

so that the code $\#\neg$ of $\neg$ is 0 and the code $\#s_1$ of the first symbol of τ is 10. The v_i are the variables, and $\#\mathrm{v}_i = 10 + k + i$. We code *strings of symbols* using the standard coding of tuples,

$$\#(a_1 a_2 \dots a_n) = \langle \#a_1, \dots, \#a_n \rangle;$$

and we code *finite sequences of strings* using the same idea.

We code terms and formulas of $\mathbb{FOL}(\tau)$ by viewing them as strings of symbols.

Lemma 4A.3 (The Substitution Lemma)**.** *Fix a finite signature τ and set*

$$\begin{aligned}
\mathrm{Term}_0(a) &\iff_{\mathrm{df}} a \text{ is a code of a term } t,\\
\mathrm{Formula}_0(e) &\iff_{\mathrm{df}} e \text{ is a code of a formula } \phi,\\
\mathrm{Formula}(e,i,j) &\iff_{\mathrm{df}} e \text{ is a code of a formula } \phi\\
&\qquad\quad \text{and } \mathrm{v}_i \text{ occurs free as the } j\text{th symbol of } \phi.
\end{aligned}$$

(a) *The relations* $\mathrm{Term}(a)$, $\mathrm{Formula}_0(e)$ *and* $\mathrm{Formula}(e,i,j)$ *are primitive recursive.*

(b) *There is a primitive recursive function* $\mathrm{sub}(e,i,a)$*, such that if a term t is free for v_i in an extended formula $\phi(\mathrm{v}_i)$, then*

$$\mathrm{sub}(\#\phi(\mathrm{v}_i), i, \#t) = \#\phi(t). \tag{86}$$

PROOF. (a) The characteristic functions of these relations are defined by Complete Primitive Recursions, Lemma 3I.13, using the closure properties of primitive recursive relations in Lemma 3I.9 and the bounds for subsequences of the standard, power coding in Lemma 3I.12. We illustrate the method for the relation $\mathrm{Term}_0(a)$ in the simple case where the signature $\tau = (0, S, +)$ has only one constant, one unary function symbol S and one binary symbol $+$. In this case, the term relation satisfies the equivalence

$$\begin{aligned}
\mathrm{Term}_0(a) \iff & a = \langle \#0 \rangle\\
&\vee (\exists u < a)[\mathrm{Term}_0(u) \ \& \ a = \langle \#S, \#(\rangle * u * \langle \#) \rangle]\\
&\vee (\exists u, v < a)[\mathrm{Term}_0(u) \ \& \ \mathrm{Term}_0(v)\\
&\qquad\qquad \& \ a = \langle \#+, \#(\rangle * u * \langle \#, \rangle * v * \langle \#) \rangle],
\end{aligned}$$

which makes it clear how it can be checked for each a if we know it on all the numbers smaller than a. From this we derive an identity for the characteristic function of the term relation, of the form

$$\chi(a) = g(a, \langle \chi(0), \ldots, \chi(a-1) \rangle)$$

where

$$g(a,w) = \begin{cases} 1, & \text{if } a = \langle \#0 \rangle, \\ 1, & \text{ow., if } (\exists u < a)[(w)_u = 1 \;\&\; a = \langle \#S, \#(\rangle * u * \langle \#) \rangle], \\ 1, & \text{ow., if } (\exists u, v < a)[(w)_u = 1 \;\&\; (w)_v = 1 \\ & \qquad \& \; a = \langle \#+, \#(\rangle * u * \langle \#, \rangle * v * \langle \#) \rangle], \\ 0, & \text{otherwise.} \end{cases}$$

Now $g(a,w)$ is primitive recursive, and so $\chi(a)$ is primitive recursive by Lemma 3I.13. In the case of a signature with k (rather than 3) symbols, the definition of $g(a,w)$ would have $k+1$ cases, and the arguments for the other relations in (a) are similar.

(b) One way to prove this is to define by primitive recursion (on j) the substitution function

$$f(e,i,a,j) = \mathrm{sub}(e \restriction j, i, a)$$

on initial segments of e, using part (a) of the Lemma to make sure that the substitutions are made in the proper places; this implies (b) since $\mathrm{sub}(e,i,a) = f(e,i,a,\mathrm{lh}(e))$. We leave the details for Problem x4.13. ⊣

This coding of syntactic quantities (terms and formulas here, proofs later) was introduced by Gödel, and so the codes of these "metamathematical" objects are also called **Gödel numbers**. We should add that there is nothing special about the specific syntactic relations proved "primitive recursive in the codes" in Lemma 4A.3, except that we will use them in what follows; in practice all natural, "effectively decidable" syntactic relations are primitive recursive in the codes, by similar arguments—and hence they are arithmetical, by Proposition 3I.4. We exploit this fact in the next, key result.

For each formula ϕ in the language of arithmetic, we let

(87) $$\ulcorner \phi \urcorner = \Delta \# \phi = \text{the numeral of the code of } \phi;$$

the closed term $\ulcorner \phi \urcorner$ is a "name" by which the language of PA can refer to ϕ. In particular, if a full extended formula $\psi(v)$ defines an arithmetical relation $P(x)$, then for each sentence θ,

$$P(\#\theta) \iff \mathbf{N} \models \psi(\Delta\#\theta) \iff \mathbf{N} \models \psi(\ulcorner \theta) \urcorner).$$

Theorem 4A.4 (The Semantic Fixed Point Lemma)**.** *For each full extended formula $\psi(v)$ of* PA*, there is a sentence θ such that*

$$\mathbf{N} \models \theta \leftrightarrow \psi(\ulcorner\theta\urcorner). \tag{88}$$

PROOF. Let

$$\mathrm{Sub}(e, m) = \mathrm{sub}(e, 0, \#\Delta m)$$

where $\mathrm{sub}(e, i, a)$ is the substitution function of Lemma 4A.3, so that for each extended formula $\phi(\mathrm{v}_0)$ and every number m,

$$\mathrm{Sub}(\#\phi(\mathrm{v}_0), m) = \#\phi(\Delta m).$$

The function $\mathrm{Sub}(e, m)$ is primitive recursive, and hence arithmetical; so let $\mathbf{Sub}(x, y, z)$ define its graph in $\mathbf{N}$, so that

$$\mathrm{Sub}(e, m) = z \iff \mathbf{N} \models \mathbf{Sub}(\Delta e, \Delta m, \Delta z),$$

and set

$$\phi(\mathrm{v}_0) :\equiv (\exists z)[\mathbf{Sub}(\mathrm{v}_0, \mathrm{v}_0, z) \ \&\ \psi(z)],$$

with the given $\psi(v)$, choosing a fresh variable z so that the indicated substitutions are all free. Finally, set

$$\theta :\equiv \phi(\Delta e), \text{ where } e = \#\phi(\mathrm{v}_0).$$

By the remarks above,

$$\mathrm{Sub}(e, e) = \#\phi(\Delta e) = \#\theta.$$

To prove (88), we compute:

$$\begin{aligned} \mathbf{N} \models \theta &\iff \mathbf{N} \models \phi(\Delta e) \\ &\iff \mathbf{N} \models \exists z[\mathbf{Sub}(\Delta e, \Delta e, z) \ \&\ \psi(z)] \\ &\iff \text{there is some } x \text{ such that } x = \mathrm{Sub}(e, e) \text{ and } \mathbf{N} \models \psi(\Delta x) \\ &\iff \mathbf{N} \models \psi(\Delta\#\theta) \\ &\iff \mathbf{N} \models \psi(\ulcorner\theta\urcorner). \end{aligned}$$ ⊣

The Semantic Fixed Point Lemma says that every unary arithmetical relation asserts of (the code of) some sentence θ of PA exactly what θ asserts about $\mathbf{N}$. As a first illustration of its power, we prove a classical non-definability result about the **truth relation** of the structure $\mathbf{N}$,

$$\mathrm{Truth}^{\mathbf{N}}(e) \iff e = \#\theta \text{ for some } \theta \text{ such that } \mathbf{N} \models \theta. \tag{89}$$

Theorem 4A.5 (Tarski's Theorem)**.** *The truth relation for the standard model of* PA *is not arithmetical.*

Proof. If the truth relation were arithmetical, then its negation would also be arithmetical, and so there would exist a full extended formula $\psi(v)$ such that for every sentence θ of PA,

$$\mathbf{N} \not\models \theta \iff \neg\mathrm{Truth}^{\mathbf{N}}(\#\theta) \iff \mathbf{N} \models \psi(\ulcorner\theta\urcorner). \tag{90}$$

By the Semantic Fixed Point Lemma, there is a sentence θ such that

$$\mathbf{N} \models \theta \iff \mathbf{N} \models \psi(\ulcorner\theta\urcorner),$$

which is absurd, since with (90) it implies that

$$\mathbf{N} \models \theta \iff \mathbf{N} \not\models \theta. \qquad \dashv$$

To derive incompleteness results about PA by this method, we need to check that the *provability relation* of PA is arithmetical. We introduce the appropriate more general notions, which we will also need in the sequel.

Definition 4A.6 (Axiomatizations). Let T be a τ-theory, i.e., (by 1G.2) any set of sentences in $\mathbb{FOL}(\tau)$.

A **set of axioms** for T is any set S of sentences of $\mathbb{FOL}(\tau)$ such that for all θ,

$$S \vdash \theta \iff T \vdash \theta; \tag{91}$$

T is **finitely axiomatizable** if it has a finite set of axioms; and T is (primitive recursively) **axiomatizable** if its signature τ is finite and T has a set of axioms S which is primitive recursive (in the codes), i.e., such that the set of codes

$$\#S = \{\#\theta \mid \theta \in S\} \tag{92}$$

is primitive recursive.

Notice that if a τ-theory is axiomatizable, then (by definition) τ is a finite signature, and the codes in (92) are computed relative to some enumeration $s_1, \dots, s_k$ of the symbols in τ. Some results about axiomatizable theories depend on the selection of a specific (primitive recursive) axiomatization, and in a few cases this is important; we will make sure to indicate these instances.

Note. In some books, by "theory" they mean a set T of sentences in a language which is closed under deducibility, i.e., such that

$$T \vdash \theta \Longrightarrow \theta \in T \quad (\theta \text{ in the vocabulary of } T).$$

We have not done this here, and so we must be careful in understanding correctly results stated when this alternative usage is in effect.

Lemma 4A.7. *Every finite theory is axiomatizable;* PA *is axiomatizable; and if T_1 and T_2 are both axiomatizable, then so is their union $T_1 \cup T_2$.* (Cf. Problem x4.14.)

Definition 4A.8 (Proof predicates)**.** We code the proofs of a theory T as sequences of strings:

$$\begin{aligned}\mathrm{Proof}_T(e,y) &\iff e \text{ is the code of a formula } \phi \\ &\qquad \text{and } y \text{ is the code of a proof of } \phi \text{ from } T \\ &\iff \text{there exist formulas } \phi, \phi_1, \dots, \phi_{n-1} \text{ such that} \\ &\qquad e = \#\phi \text{ and } y = \langle \#\phi_1, \dots, \#\phi_{n-1}, \#\phi \rangle \\ &\qquad \text{and } \phi_1, \dots, \phi_{n-1}, \phi \text{ is a proof of } T.\end{aligned}$$

It is simpler here to use proofs in the Hilbert-style proof system for $\mathbb{FOL}$ defined in Section 1H, but we could use proofs in the Gentzen system with only a minor complication in the codings.

Lemma 4A.9. *If T is an axiomatizable theory, then its proof predicate* $\mathrm{Proof}_T(e,y)$ (with respect to any primitive recursive axiomatization) *is primitive recursive.* (Cf. Problem x4.15.)

Proof is tedious but basically trivial, because the axioms and the rules of inference of first order logic can be checked"primitive recursively" in the codes. ⊣

Recall from Definition 1H.9 that a τ-theory T is **complete** if for each τ-sentence θ,

$$\text{either } T \vdash \theta \text{ or } T \vdash \neg\theta;$$

so T is **incomplete** if there is a τ-sentence θ such that

$$\text{neither } T \vdash \theta \text{ nor } T \vdash \neg\theta.$$

Theorem 4A.10 (Gödel's First Incompleteness Theorem)**.** *Every axiomatizable, sound theory T in the language of arithmetic is incomplete.*

In particular, PA *is incomplete.*

Proof. The proof predicate $\mathrm{Proof}_T(e,y)$ constructed from a primitive recursive axiomatization of T is primitive recursive, hence arithmetical, and so it is defined by some full extended formula $\mathbf{Proof}_T(e,y)$. The Semantic Fixed Point Lemma 4A.4 applied to the formula

$$\psi(\mathrm{v}_0) \equiv (\forall y)\neg\mathbf{Proof}_T(\mathrm{v}_0, y),$$

yields a sentence γ_T such that

$$\mathbf{N} \models \gamma_T \iff \mathbf{N} \models (\forall y)\neg\mathbf{Proof}_T(\ulcorner\gamma_T\urcorner, y),$$

and we can compute, using properties of the satisfaction relation:

$$\begin{aligned}\mathbf{N} \models \gamma_T &\iff \mathbf{N} \models (\forall y)\neg\mathbf{Proof}_T(\ulcorner\gamma_T\urcorner, y)\\ &\iff \text{for every } m, \mathbf{N} \models \neg\mathbf{Proof}_T(\ulcorner\gamma_T\urcorner, \Delta m)\\ &\iff \text{for every } m, \neg\mathrm{Proof}_T(\#\gamma_T, m)\\ &\iff T \nvdash \gamma_T.\end{aligned}$$

It follows that $\mathbf{N} \models \gamma_T$, since otherwise (by this equivalence) $T \vdash \gamma_T$—and then γ_T is true by the soundness of T, and so it cannot be that $T \vdash \neg\gamma_T$; and since $\mathbf{N} \models \gamma_T$, by the same equivalence, $T \nvdash \gamma_T$. $\dashv$

Notice that the Gödel sentence γ_T depends on the specific axiomatization of T chosen for the proof; but the theorem—that T is incomplete—does not refer to any specific axiomatization of T, or to any particular method of coding the syntactic objects of T. In applying the result to a specific theory, e.g., PA, we do not even need to refer to the *possibility of coding*: we introduce a coding and check the axiomatizability of PA *as part of the proof.*

4B. Numeralwise representability in Q

Gödel's First Incompleteness Theorem 4A.10 applies only to sound theories; and while this may appear to be not a serious limitation (because who would be interested in theories which prove false number-theoretic facts), its extension to (all interesting) *axiomatizable, consistent theories* has, in fact, many applications and reveals new and deeper limitations of first order axiomatic theories. To prove these results, we need to do some proof theory.

Our aim in this section is to introduce the relevant notions and to show that the axiomatic theory Q defined in 1G.11 is strong enough to prove many fundamental properties of primitive recursive functions and relations, even though it is otherwise very weak, cf. Problems x1.33 and x4.10. Using these facts, we will establish the Fixed Point Theorem 4B.14, a proof-theoretic version of Theorem 4A.4 which is the main tool for the stronger results of Gödel Theory.

Definition 4B.1. Let T be a theory in the language of PA. A full extended formula $\mathbf{F}(v_1, \dots, v_n, y)$ **numeralwise represents** in T an n-ary function $f : \mathbb{N}^n \to \mathbb{N}$, if for all $x_1, \dots, x_n, w \in \mathbb{N}$,

$$\begin{aligned}f(x_1, \dots, x_n) = w \implies\ & T \vdash \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w)\\ & \text{and } T \vdash (\exists! y)\mathbf{F}(\Delta x_1, \dots, \Delta x_n, y).\end{aligned}$$

A full extended formula $\mathbf{R}(v_1, \dots, v_n)$ **numeralwise expresses** in T an n-ary relation $R \subseteq \mathbb{N}^n$, if for all $x_1, \dots, x_n \in \mathbb{N}$,

$$R(x_1, \dots, x_n) \implies T \vdash \mathbf{R}(\Delta x_1, \dots, \Delta x_n),$$
$$\neg R(x_1, \dots, x_n) \implies T \vdash \neg\mathbf{R}(\Delta x_1, \dots, \Delta x_n).$$

Lemma 4B.2. (a) *If T is sound* (for the standard model $\mathbf{N}$) of PA *and $\mathbf{R}(v_1, \dots, v_n)$ is a full extended formula which numeralwise expresses R in T, then $\mathbf{R}(v_1, \dots, v_n)$ defines R in $\mathbf{N}$, and so R is arithmetical.*

(b) *If $T_1 \subseteq T_2$ and $\mathbf{R}$ numeralwise expresses R in T_1, then $\mathbf{R}$ numeralwise expresses R in T_2, and the same is true of numeralwise representability.*

(c) *If T is inconsistent, then every relation on $\mathbb{N}$ is numeralwise expressible in T and every function $f : \mathbb{N}^n \to \mathbb{N}$ is numeralwise representable in T.*

So these notions are interesting only for consistent theories.

Notice also that if $\mathbf{F}$ numeralwise represents a function f in T, then $\mathbf{F}$ numeralwise expresses in T the graph of f,

$$G_f(x_1, \dots, x_n, w) \iff f(x_1, \dots, x_n) = w,$$

but the converse is not true: numeralwise representability is stronger than the mere numeralwise expressibility of the graph, as it demands that "T knows" for each tuple of specific numbers the existence of a unique value of $f(x_1, \dots, x_n)$. On the other hand, it may be that $\mathbf{F}(v_1, \dots, v_n, y)$ numeralwise represents a function f in T without "T knowing" that the formula defines the graph of a function, which would amount to

$$T \vdash (\forall v_1, \dots, v_n)(\exists! y)\mathbf{F}(v_1, \dots, v_n, y).$$

The notions (due to Gödel) are subtle and chosen just right so that the computations go through.

Our aim in the remainder of this section is to establish Theorem 4B.13, that all primitive recursive functions are numeralwise representable in Q.

Lemma 4B.3. *The successor function, the constant functions and the projection functions are all numeralwise representable in* Q.

Lemma 4B.4. *If $g_1(\vec{x}), \dots, g_m(\vec{x})$ and $h(u_1, \dots, u_m)$ are all numeralwise representable in Q, then so is the composition*

$$f(\vec{x}) = h(g_1(\vec{x}), \dots, g_m(\vec{x})).$$

To prove that the class of functions which are numeralwise representable in Q is also closed under primitive recursion, we need to formalize the basic constructions of Section 1E.

Definition 4B.5. We introduce the formal abbreviations

$$\begin{aligned} x \le y &\equiv (\exists z)[z + x = y],\\ x < y &\equiv x \le y \;\&\; \neg(x = y),\\ (\exists u \le y)\phi &\equiv (\exists u)[u \le y \;\&\; \phi],\\ (\forall u \le y)\phi &\equiv (\forall u)[u \le y \to \phi]. \end{aligned}$$

The use of $z + x$ rather than $x + z$ in the definition of $x \le y$ is important, because (as we have shown) Q cannot prove the commutativity of addition.

Lemma 4B.6. Q *can prove all true propositional combinations of closed equalities and inequalities between terms; i.e., if θ is a propositional sentence in the signature $(0, S, +, \cdot, \le)$, then*

$$\mathbf{N} \models \theta \iff \mathsf{Q} \vdash \theta.$$

(Cf. Problem x4.11*.)

Proof. Check first by structural induction, that for each closed term t in the language of arithmetic, if value$(t) = n$, then $\mathsf{Q} \vdash t = \Delta n$, and then prove by structural induction that for every quantifier free sentence θ,

$$\mathbf{N} \models \theta \iff \mathsf{Q} \vdash \theta \text{ and } \mathbf{N} \models \neg\theta \iff \mathsf{Q} \vdash \neg\theta. \qquad \dashv$$

Lemma 4B.7. $\mathsf{Q} \vdash (\forall x)[x \le \Delta m \to x = \Delta 0 \vee x = \Delta 1 \vee \cdots \vee x = \Delta m]$. *As a consequence,*

$$\mathsf{Q}, \phi(\Delta 0), \ldots, \phi(\Delta m) \vdash (\forall u \le \Delta m)\phi(u).$$

(Q knows all the predecessors of a numeral and can quantify over the initial segment below a numeral.)

Proof is by induction on the number m. $\dashv$

Lemma 4B.8. *The remainder function* rem(x, y) *is numeralwise representable in* Q*, and hence so is the Gödel β-function*

$$\beta(c, d, i) = \text{rem}(c, 1 + (i + 1)d).$$

Lemma 4B.9. *For every $m \in \mathbb{N}$,*

$$\mathsf{Q} \vdash S(z) + \Delta m = z + S(\Delta m).$$

Proof is by induction on m. $\dashv$

Lemma 4B.10. *For $m \in \mathbb{N}$,*

$$\mathsf{Q} \vdash (\forall x)[x \le \Delta m \vee \Delta(m + 1) \le x].$$

Proof is by induction on m. $\dashv$

Lemma 4B.11. *If $f(x_1, \dots, x_n)$ is numeralwise representable in* Q*, then there exists a full extended formula* $\mathbf{F}(v_1, \dots, v_n, y)$ *such that the following hold for all numbers* $x_1, \dots, x_n, w$*:*

1. $f(x_1, \dots, x_n) = w \Longrightarrow \mathsf{Q} \vdash \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w)$.
2. $\mathsf{Q}, \mathbf{F}(v_1, \dots, v_n, \Delta w), \mathbf{F}(v_1, \dots, v_n, y) \vdash y = \Delta w$.

In particular, $\mathbf{F}(v_1, \dots, v_n, y)$ *numeralwise represents* f (in a very strong way).

Proof. Let $\mathbf{F}_1(v_1, \dots, v_n, y)$ numeralwise represent f, and take

$$\mathbf{F}(v_1, \dots, v_n, y) \equiv \mathbf{F}_1(v_1, \dots, v_n, y) \ \&\ (\forall u < y)\neg \mathbf{F}_1(v_1, \dots, v_n, u),$$

where $u < y$ abbreviates $u \le y \ \&\ u \neq y$. ⊣

Lemma 4B.12. *If f is defined by the primitive recursion*

$$f(0, \vec{x}) = g(\vec{x}), \quad f(t+1, \vec{x}) = h(f(t, \vec{x}), t, \vec{x})$$

and g, h are numeralwise representable in Q*, then so is f; and the same holds for primitive recursion without parameters* (5).

Proof. We start with Dedekind's analysis of the primitive recursive definition,

$$\begin{aligned} f(t, \vec{x}) = w \iff & \text{ there exists a sequence } (w_0, \dots, w_t) \text{ such that} \\ & w_0 = g(\vec{x}) \ \&\ (\forall s < t)[w_{s+1} = h(w_s, s, \vec{x})] \ \&\ w = w_t; \end{aligned}$$

we then choose formulas $\mathbf{B}(c, d, i, y)$, $\mathbf{G}(\vec{x}, u)$ and $\mathbf{H}(u, t, \vec{x}, w)$ which numeralwise represent the β-function, g and h in the strong sense of the preceding Lemma; and we set

$$\begin{aligned} \mathbf{F}(t, \vec{x}, w) \equiv & [t = 0 \ \&\ \mathbf{G}(\vec{x}, w)] \\ & \vee (\exists c)(\exists d)[(\exists q)[\mathbf{G}(\vec{x}, w) \ \&\ \mathbf{B}(c, d, 0, q)] \\ & \quad \&\ (\forall i < t)(\forall u)(\forall v)[[\mathbf{B}(c, d, i, u) \ \&\ \mathbf{H}(u, \vec{x}, i, v)] \\ & \qquad\qquad \to \mathbf{B}(c, d, S(i), v)] \\ & \quad \&\ \mathbf{B}(c, d, i, w)]. \end{aligned}$$ ⊣

Theorem 4B.13. *Every primitive recursive function is numeralwise representable in* Q*; and every primitive recursive relation is numeralwise expressible in* Q.

Proof. For the second assertion, let $\mathbf{F}(\vec{v}, y)$ numeralwise represent the characteristic function of R and set

$$\mathbf{R}(\vec{v}) \equiv \mathbf{F}(\vec{v}, 1);$$

proof that this formula numeralwise expresses R follows from the assumption that for all $x_1, \dots, x_n$,

$$\mathsf{Q} \vdash (\exists! y)\mathbf{F}(\Delta x_1, \dots, \Delta x_n, y).$$ ⊣

It is important for the applications, to notice that the next, basic result applies to theories in the language of PA which need not be sound for the standard model **N**.

Theorem 4B.14 (The Fixed Point Lemma)**.** *If T is a theory in the language of arithmetic which extends Robinson's system Q, then for each full extended formula $\psi(v)$, we can find a sentence θ such that*

(93) $$T \vdash \theta \leftrightarrow \psi(\ulcorner\theta\urcorner).$$

PROOF. As in the proof of Theorem 4A.4, let

$$\mathrm{Sub}(e, m) = \mathrm{sub}(e, 0, \#\Delta m)$$

where $\mathrm{sub}(e, i, a)$ is the substitution function of the Substitution Lemma 4A.3, so that for each extended formula $\phi(\mathrm{v}_0)$,

$$\mathrm{Sub}(\#\phi(\mathrm{v}_0), m) = \#\phi(\Delta m).$$

The function $\mathrm{Sub}(e, m)$ is primitive recursive; so let $\mathbf{Sub}(x, y, z)$ numeralwise represent it in T (and such that v_0 does not occur in it), and set

$$\phi(\mathrm{v}_0) :\equiv (\exists z)[\mathbf{Sub}(\mathrm{v}_0, \mathrm{v}_0, z) \ \&\ \psi(z)],$$

choosing again a fresh variable z, so that the indicated substitutions are all free. Set

$$\theta :\equiv \phi(\Delta e), \ \text{where } e = \#\phi(\mathrm{v}_0),$$

so that by the remark above,

$$\mathrm{Sub}(e, e) = \#\phi(\Delta e) = \#\theta.$$

From the definition of numeralwise representability (and the definition of $\ulcorner\theta\urcorner = \Delta\#\theta$), we have

(94) $$T \vdash \mathbf{Sub}(\Delta e, \Delta e, \ulcorner\theta\urcorner),$$

(95) $$\text{and } T \vdash (\forall z)[\mathbf{Sub}(\Delta e, \Delta e, z) \rightarrow z = \ulcorner\theta\urcorner].$$

To prove (93), argue in T as follows: if $\psi(\ulcorner\theta\urcorner)$, we have

$$\mathbf{Sub}(\Delta e, \Delta e, \ulcorner\theta\urcorner) \ \&\ \psi(\ulcorner\theta\urcorner)$$

from (94), which yields

$$(\exists z)[\mathbf{Sub}(\Delta e, \Delta e, z) \ \&\ \psi(z)],$$

i.e., $\phi(\Delta e)$, i.e., θ; and if θ, we have

$$(\exists z)[\mathbf{Sub}(\Delta e, \Delta e, z) \ \&\ \psi(z)],$$

which with (95) yields $\psi(\ulcorner\theta\urcorner)$, and completes the proof. $\dashv$

4C. Rosser, more Gödel and Löb

If T_1, T_2 are theories in the same language $\mathbb{FOL}(\tau)$, we (naturally) say that

$$T_1 \text{ is weaker than } T_2 \text{ and } T_2 \text{ is stronger than } T_1 \iff \text{for all } \tau\text{-sentences } \theta, T_1 \vdash \theta \Longrightarrow T_2 \vdash \theta;$$

the next definition extends this idea in a natural way to theories in different languages.

4C.1. Interpretations. Let T_1, T_2 be theories, in two (possibly different) languages $\mathbb{FOL}(\tau_1)$, $\mathbb{FOL}(\tau_2)$ of finite signatures. A (propositionally faithful, minimal) **interpretation** of T_1 in T_2 is a primitive recursive function π from the *sentences* of T_1 to sentences of T_2 such that the following hold.

(1) $T_1 \vdash \theta \Longrightarrow T_2 \vdash \pi(\theta)$.
(2) $T_2 \vdash \pi(\neg\theta) \leftrightarrow \neg\pi(\theta)$.
(3) $T_2 \vdash \pi(\phi \;\&\; \psi) \leftrightarrow \pi(\phi) \;\&\; \pi(\psi)$.

Here we call $\pi : \text{Sentences}(T_1) \to \text{Sentences}(T_2)$ *primitive recursive* if there is a primitive recursive function $\pi^* : \mathbb{N} \to \mathbb{N}$ such that

$$\#\pi(\phi) = \pi^*(\#\phi) \quad (\phi \text{ any sentence of } T_1),$$

where # denotes the coding function of $\mathbb{FOL}(\tau_2)$ on the left and the coding function of $\mathbb{FOL}(\tau_1)$ on the right. Notice that (2) and (3) together imply that an interpretation preserves the propositional structure of sentences, for example

$$T_2 \vdash \pi(\phi \to \psi) \leftrightarrow (\pi(\phi) \to \pi(\psi)).$$

Directly from the definition, we get:

Lemma 4C.2. *If T_1' is weaker than T_1, T_2 is weaker than T_2', and π interprets T_1 in T_2, then π interprets T_1' in T_2'.*

When $T_2 = T_1$ or the language of T_2 is the same (or an expansion) of the language of T_1 and T_2 has more axioms, then the identity function interprets T_1 in T_2. For an example of an interpretation between entirely different languages, we note (without proof) the classical interpretation of Peano arithmetic in the axiomatic set theories specified in Definition 1G.12, which is constructed by "defining" the natural numbers within set theory:

Proposition 4C.3. *Peano arithmetic* PA *is interpretable in Zermelo's set theory without choice* Z*, and hence every subtheory of* PA *is interpretable in all the* (stronger) *axiomatic set theories listed in Definition 1G.12.*

Much stronger notions of interpretation exist and are often useful, but this is all we need now; and for the theorems we will prove, the weaker the notion of interpretation employed, the better.

Theorem 4C.4 (Rosser's form of Gödel's First Theorem). *If T is a consistent, axiomatizable theory and Q is interpretable in T, then T is incomplete.*

Proof. Fix an interpretation π of Q in T, set

$$\begin{aligned}
\mathrm{Proof}_{\pi,T}(e,y) \iff\ & e \text{ codes a sentence } \phi \text{ of } \mathsf{PA} \\
& \text{and } y \text{ codes a proof in } T \text{ of the translation } \pi(\phi), \\
\mathrm{Refute}_{\pi,T}(e,y) \iff\ & e \text{ codes a sentence } \phi \text{ of } \mathsf{PA} \\
& \text{and } y \text{ codes a proof in } T \text{ of the translation } \pi(\neg\phi),
\end{aligned}$$

and let $\mathbf{Proof}_{\pi,T}(e,y)$, $\mathbf{Refute}_{\pi,T}(e,y)$ be formulas of number theory which numeralwise express in Q these primitive recursive relations. By the Fixed Point Lemma for Q, we can construct a sentence

$$\rho = \rho(T,\pi)$$

in the language of PA, such that

$$\mathsf{Q} \vdash \rho \leftrightarrow (\forall y)[\mathbf{Proof}_{\pi,T}(\ulcorner\rho\urcorner, y) \to (\exists u \le y)\mathbf{Refute}_{\pi,T}(\ulcorner\rho\urcorner, u)]. \tag{96}$$

The *Rosser sentence* ρ expresses the unprovability of its translation in T, but in a round-about way: it asserts that "for each one of my proofs, there is a shorter (not longer) proof of my negation".

(a) Suppose towards a contradiction that there is a proof of $\pi\rho$ in T, with code m, so by the hypotheses,

$$\mathsf{Q} \vdash \mathbf{Proof}_{\pi,T}(\ulcorner\rho\urcorner, \Delta m).$$

Taking $y = \Delta m$ and appealing to the hypothesis and basic facts about Q, we get that

$$\mathsf{Q} \vdash (\exists y)[\mathbf{Proof}_{\pi,T}(\ulcorner\rho\urcorner, y)\ \&\ (\forall u \le y)\neg\mathbf{Refute}_{\pi,T}(\ulcorner\rho\urcorner, u)];$$

thus with (96), $\mathsf{Q} \vdash \neg\rho$, hence $T \vdash \pi(\neg\rho)$, i.e., $T \vdash \neg\pi(\rho)$, contradicting the assumed consistency of T.

(b) Suppose now that there is a proof in T of $\neg\pi(\rho)$, hence a proof of $\pi(\neg\rho)$, and let m be its code. We know that

$$\mathsf{Q} \vdash \mathbf{Refute}_{\pi,T}(\ulcorner\rho\urcorner, \Delta m),$$

among other things. To prove

$$(\forall y)[\mathbf{Proof}_{\pi,T}(\ulcorner\rho\urcorner, y) \to (\exists u \le y)\mathbf{Refute}_{\pi T}(\ulcorner\rho\urcorner, u)] \tag{97}$$

in Q, we take cases (by Lemma 4B.10) on whether

$$y \le \Delta m \vee \Delta(m+1) \le y;$$

in the first of these cases we know (by Lemma 4B.7, in Q) that $y = i$ for some $i \leq m$, and it is trivial to verify that $\neg\mathbf{Proof}_{\pi,T}(\ulcorner\rho\urcorner, y)$, since this sentence is true and Q knows such true assertions about the values of $\mathrm{Proof}_{\pi,T}$ by Lemma 4B.6. In the second case, Q knows $\Delta m \leq y$, in which case the conclusion of the implication in (97) follows immediately. So we have proved (97) which is equivalent in Q to ρ by (96), contradicting (a).⊣

Notice (again) that the Rosser sentence ρ we constructed depends on a specific axiomatization of T chosen for the proof, as well as a specific interpretation of Q into T; but the result—the incompleteness of T—is independent of these parameters, and for specific theories T, we can incorporate the verification of axiomatizability in the proof and derive a result which is entirely independent of any particular coding. This is certainly the case for the axiomatic theories of Definition 1G.12, for which the result is very clean, e.g., *if* ZFC *is consistent, then it is incomplete.*

4C.5. Remarks. Rosser's form of Gödel's Theorem 4C.4 is much more general than Gödel's First Incompleteness Theorem 4A.10, as it does not make any *soundness* assumptions of T: it applies, for example, to the theory $\mathsf{PA} + \neg\gamma_{\mathsf{PA}}$, which is consistent but certainly not sound, cf. Problem x4.16. It also applies to axiomatic set theories, for which it is easy to establish that they interpret Q, but it is not clear exactly in what sense they are sound, and (in some cases) it is not even completely clear that they are consistent!

Next we identify a specific, especially interesting fact that sufficiently strong, consistent theories can express but cannot prove:

Definition 4C.6. For each axiomatizable theory T, let

$$\mathbf{Consis}_T \equiv \neg(\exists e)(\exists u)(\exists v)[\mathbf{Proof}_T(e, u) \;\&\; \mathbf{Refute}_T(e, v)];$$

this is the sentence of number theory which expresses formally the consistency of T—with respect, again, to a specific axiomatization of T.

Lemma 4C.7. *If T is axiomatizable and consistent, π is an interpretation of Q in T, and ρ_T is the Rosser sentence of T for π, then*

$$\mathsf{PA} \vdash \mathbf{Consis}_T \rightarrow \rho_T.$$

PROOF. The proof of (a) Theorem 4C.4 is elementary, and it can be formalized in Peano Arithmetic; thus

$$\mathsf{PA} \vdash \mathbf{Consis}_T \rightarrow (\forall y)\neg\mathbf{Proof}(\ulcorner\rho_T\urcorner, y).$$

On the other hand, ρ_T expresses precisely its unprovability, albeit in a round-about way, but still,

$$\mathsf{PA} \vdash \rho_T \leftrightarrow (\forall y)\neg\mathbf{Proof}(\ulcorner\rho_T\urcorner, y);$$

and these two claims, together, yield the Lemma. ⊣

Theorem 4C.8 (Gödel's Second Incompleteness Theorem)**.** *If T is an axiomatizable, consistent theory such that* PA *is interpretable into it by some function π, then $\pi\mathbf{Consis}_T$ is not a theorem of T.*

In particular, PA *cannot prove its own consistency, unless it is inconsistent.*

Proof is immediate from the Lemma, since $T \nvdash \pi\rho_T$. ⊣

For any sentence θ in the language of PA, clearly

$$\mathbf{N} \models (\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y) \rightarrow \theta; \tag{98}$$

this is just a formal expression of the soundness of PA. It should be that PA can prove this basic principle—recognize that it is sound—but it cannot, except when it is trivial:

Theorem 4C.9 (Löb's Theorem)**.** *For each sentence θ of number theory,*

$$\text{if } \mathsf{PA} \vdash (\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y) \rightarrow \theta, \text{ then } \mathsf{PA} \vdash \theta.$$

Proof. Towards a contradiction, we assume that

$$\mathsf{PA} \vdash (\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y) \rightarrow \theta \quad \text{but} \quad \mathsf{PA} \nvdash \theta$$

for some θ, so that the theory

$$T = \mathsf{PA} \cup \{\neg\theta\}$$

is consistent. We now argue (in outline) that some metamathematical arguments can be formalized in PA, to infer that $T \vdash \mathbf{Consis}_T$, contrary to the Second Incompleteness Theorem for T.

From the hypothesis,

$$\mathsf{PA} \vdash \neg\theta \rightarrow \neg(\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y),$$

so that

$$T \vdash \neg(\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y).$$

Next we claim that

$$\mathsf{PA} \vdash (\exists y)\mathbf{Proof}_T(\ulcorner 0 = 1\urcorner, y) \leftrightarrow (\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\neg\theta \rightarrow (0 = 1)\urcorner, y),$$

i.e., that PA recognizes (in effect) the Deduction Theorem; and also that

$$\mathsf{PA} \vdash (\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\neg\theta \rightarrow (0 = 1)\urcorner, y) \leftrightarrow (\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y),$$

i.e., that PA recognizes that it can do proofs by contradiction. Replacing PA by the stronger T and combining these two equivalences, we get

$$T \vdash \neg(\exists y)\mathbf{Proof}_T(\ulcorner 0 = 1\urcorner, y) \leftrightarrow \neg(\exists y)\mathbf{Proof}_{\mathsf{PA}}(\ulcorner\theta\urcorner, y);$$

and since T proves the right-hand-side of this equivalence, it also proves the left-hand-side, which implies (in PA) $\mathbf{Consis}_T$. ⊣

It should be clear that the appropriate version of Löb's Theorem holds for any consistent, axiomatizable theory T in which PA can be interpreted, cf. Problem x4.19*.

4C.10. Provability theory. It is convenient to introduce a notation for the sentences which express formally provability, and so for a fixed axiomatizable T in the language of PA and any sentence θ, we set:

$$\Box_T(\theta) :\equiv (\exists y)\mathbf{Proof}_T(\ulcorner\theta\urcorner, y). \tag{99}$$

This sentence depends, of course, on the specific axiomatization of T we choose to define the proof predicate.

With this notation, Löb's Theorem takes the simple form

$$\text{if } \mathsf{PA} \vdash \Box_{\mathsf{PA}}(\theta) \to \theta, \text{ then } \mathsf{PA} \vdash \theta,$$

and the question arises whether its formal version can be proved in PA, i.e., whether the following holds for each sentence θ:

$$\mathsf{PA} \vdash \Box_{\mathsf{PA}}(\Box_{\mathsf{PA}}(\theta) \to \theta) \to \Box_{\mathsf{PA}}(\theta).$$

This is indeed true, and has interesting consequences. To show it, we must look a little more carefully at how various informal (mathematical) claims can be *formalized and proved* in axiomatized theories, a topic which is generally referred to as *provability theory*. We will confine ourselves here to just a few, basic facts.

4C.11. Bounded and Σ_1 formulas. A formula ϕ in the language of PA is **bounded** if it contains only bounded quantifiers as in Definition 4B.5, i.e., more precisely, if it belongs to the smallest set of formulas which contains all the prime formulas of the form $s = t$ and is closed under the propositional connectives and bounded quantification, i.e., the formation rules

$$\psi \mapsto (\exists \mathrm{v}_i \le \mathrm{v}_j)\psi,\ \psi \mapsto (\forall \mathrm{v}_i \le \mathrm{v}_j)\psi.$$

A formula ϕ is Σ_1 if

$$\phi \equiv \exists x_1 \cdots \exists x_n \psi$$

where ψ is a bounded formula.

For any theory T in the language of PA, a formula ϕ is T-**bounded** or T-Σ_1 if there is a bounded or Σ_1 formula ϕ^* such that

$$T \vdash \phi \leftrightarrow \phi^*;$$

and a formula ϕ is T-Δ_1, if both ϕ and $\neg\phi$ are T-Σ_1.

Proposition 4C.12. *Suppose T is an extension of* PA, *in the language of* PA.

(1) *The class of T-Σ_1 formulas includes all prime formulas and is closed under the positive propositional connectives & and $\vee$, bounded quantification of both kinds, and unbounded existential quantification.*

(2) *For each primitive recursive function $f(\vec{x})$, there is a T-Δ_1 formula $\phi(\vec{v}, w)$ which numeralwise represents $f(\vec{x})$ in T.*

(3) *Each primitive recursive relation is numeralwise expressible in T by a T-Δ_1 formula.*

Proof of these propositions can be extracted by reading with some care the proofs in Section 4B, and formalizing in the given T some easy, informal arguments. For example, to show for the proof of (1) that the class of T-Σ_1 formulas is closed under universal bounded quantification, it is enough to show that for any extended formula $\phi(x, y, z)$,

$$T \vdash (\forall x \leq y)(\exists z)\phi(x, y, z) \leftrightarrow (\exists w)(\forall x \leq y)(\exists z \leq w)\phi(x, y, z);$$

the equivalence expresses an obvious fact about numbers, which can be easily proved by induction on y—and this induction can certainly be formalized in PA.

(2) and (3) can be read-off the proof of the basic Theorem 4B.13, by computing the forms of all the formulas used in that proof and appealing to (1) of this Proposition. $\dashv$

Proposition 4C.13. *Suppose T is an axiomatizable extension of* PA*, in the language of* PA*.*

(1) *The proof predicate* $\mathrm{Proof}_T(e, y)$ *of T is numeralwise expressible by a T-Δ_1 formula* $\mathbf{Proof}_T(e, y)$*; and hence, for each sentence θ, the provability assertion $\Box_T(\theta)$ is a T-Σ_1 sentence.*

(2) *For every T-Σ_1 sentence ϕ,*

$$T \vdash \phi \rightarrow \Box_T(\phi).$$

(3) *For every sentence θ,*

$$T \vdash \Box_T(\theta) \rightarrow \Box_T(\Box_T(\theta)).$$

Proof. (1) The formula $\mathbf{Proof}_T(e, y)$ is T-Δ_1 by (3) of the preceding theorem, and so $\Box_T(\theta)$ is T-Σ_1 by its definition (99).

(2) Notice that this is not a trivial claim, because it does not, in general, hold for sentences which are not T-Σ_1: if, for example, T is sound and γ_T is its Gödel sentence, then $\gamma_T \rightarrow \Box_T(\gamma_T)$ is not true, and so it is not a theorem of T. To prove the claim, let

$$\begin{aligned}\mathrm{Proof}^n_T(e, x_1, \dots, x_n, y) \iff\ & e \text{ is the code of}\\ & \text{a full extended formula } \phi(v_1, \dots, v_n)\\ & \text{and } y \text{ is the code of a proof of } \phi(\Delta x_1, \dots, \Delta x_n) \text{ from } T.\end{aligned}$$

This is a generalization of the proof relation $\mathrm{Proof}_T(e,y)$, so that, in fact

$$\mathrm{Proof}_T(e,y) \iff \mathrm{Proof}^0_T(e,y),$$

and it is also primitive recursive. Let $\mathbf{Proof}^n_T(x_0,x_1,\dots,x_n,y)$ be a formula which numeralwise expresses $\mathrm{Proof}^n_T(e,x_1,\dots,x_n,y)$ in T. The heart of the proof is to show that *for every full extended bounded formula* $\psi(v_1,\dots,v_n)$,

(100) $T \vdash \psi(x_1,\dots,x_n) \rightarrow (\exists y)\mathbf{Proof}^n_T(\ulcorner\psi(x_1,\dots,x_n)\urcorner, x_1,\dots,x_n,y).$

This is verified by induction on the construction of bounded formulas, i.e., it is shown first for prime formulas, and then it is shown that it persists under the positive propositional connectives and bounded quantification. Notice, again, that a detailed (complete) proof would involve a good deal of work: for example, to show (part of) the basic case

(101) $$T \vdash u+v=w \rightarrow (\exists y)\mathbf{Proof}^3_T(\ulcorner u+v=w\urcorner, u,v,w,y),$$

we must formalize in T the informal claim

$$\text{if } u+v=w, \text{ then } T \vdash \Delta u + \Delta v = \Delta w;$$

the proof of the informal claim is by induction on v—and so the formal proof of (101) requires induction within T. This is why we assume in the theorem that T extends PA—there is no way to show this result for weak theories like Q. On the other hand, PA is a powerful theory in which we can formalize inductive proofs, and so (100) is plausible, and can be verified with some computation.

To complete the proof of (2), suppose

$$\phi \equiv (\exists x_1)\cdots(\exists x_n)\psi(x_1,\dots,x_n)$$

is a Σ_1 sentence with $\psi(x_1,\dots,x_n)$ bounded and having no free variables other than the indicated $x_1,\dots,x_n$, and argue in T. Assume $\psi(x_1,\dots,x_n)$, and infer

$$(\exists y)\mathbf{Proof}^n_T(\ulcorner\psi(x_1,\dots,x_n)\urcorner, x_1,\dots,x_n,y)$$

by (100). From this, by trivial properties of the provability relations (which can be formally established in PA), infer that

$$(\exists y)\mathbf{Proof}(\ulcorner(\exists x_1)\cdots(\exists x_n)\psi(x_1,\dots,x_n)\urcorner, y).$$

So we have shown that

$$T \vdash \psi(x_1,\dots,x_n) \rightarrow (\exists y)\mathbf{Proof}(\ulcorner(\exists x_1)\cdots(\exists x_n)\psi(x_1,\dots,x_n)\urcorner, y),$$

from which we get immediately the required

$$T \vdash (\exists x_1)\cdots(\exists x_n)\psi(x_1,\dots,x_n) \\ \rightarrow (\exists y)\mathbf{Proof}(\ulcorner(\exists x_1)\cdots(\exists x_n)\psi(x_1,\dots,x_n)\urcorner, y).$$

Finally, (3) follows from (1) and (2). ⊣

By methods like these, we can show that the statement and proof of Löb's Theorem for any axiomatizable extension of PA, can also be formalized in PA:

Theorem 4C.14. *For any axiomatizable extension T of* PA*, and every sentence θ,*

$$\mathsf{PA} \vdash \Box_T(\Box_T(\theta) \to \theta) \to \Box_T(\theta).$$

The most complex part of the argument is the formalization in PA of the proof of the Second Incompleteness Theorem of Gödel 4C.8.

And, finally, to prove the following considerably deeper result, we also need to formalize in PA the Gentzen Hauptsatz:

Theorem 4C.15. PA *is not finitely axiomatizable.*

This is somewhat different from the preceding is that its *statement* (as opposed to its proof) does not depend on any particular coding of formulas, proofs, etc.: the result simple asserts that no finite set of sentences in the language of PA has exactly the same consequences as PA.

4D. Computability and undecidability

Is it possible to determine "effectively" whether an arbitrary sentence of arithmetic is true? Gödel's First Incompleteness Theorem shows that this cannot be done by the classical axiomatic method, i.e., by singling out some "obvious" arithmetical truths and then (formally) proving all the others, but it may be argued that this exhibits only a fundamental *incompleteness of the axiomatic method*: it may be that some other method (unrelated to logic) might "identify" effectively all arithmetical truths, without necessarily justifying them (by reducing them to some few, obvious axioms). We will show in this and the next two sections that this cannot be done, by proving that *there is no general method which can decide effectively whether a given sentence of the language of arithmetic is true.* The methods we will use (due to Turing, Church and Kleene) will yield a host of related *undecidability results* which are among the most fundamental applications of logic.

For each set Λ of "symbols", Λ^* is the set of *strings* (words, finite sequences) from Λ, including the empty string ϵ. For example, the sets of terms and formulas of $\mathbb{FOL}(\tau)$ for a specific finite signature τ are sets of strings from the alphabet

$$\neg \ \to \ \& \ \vee \ \forall \ \exists \ = \ (\ ) \ , \ s_1 \ \ldots \ s_k \ \mathrm{v}_0 \ \mathrm{v}_1 \ \ldots$$

of $\mathbb{FOL}(\tau)$. We can replace this by the finite alphabet

$$V_\tau = \{\neg, \rightarrow, \ \& \ , \vee, \forall, \exists, =, (,), \ , , s_1, \ldots s_k, \mathrm{v}, |\}$$

where v (for "variable") and the tally | are new symbols and we identify the variable v_i with the string of v followed by $i+1$ tallies,

$$\mathrm{v}_0 \equiv \mathrm{v}|, \mathrm{v}_1 \equiv \mathrm{v}||, \mathrm{v}_2 \equiv \mathrm{v}|||, \ldots$$

If we further think of *proofs* in $\mathbb{FOL}(\tau)$ as sequences of formulas separated by commas, then proofs are also words in this finite alphabet V_τ, i.e., members of ${V_\tau}^*$. Thus the notion that we need to make precise is that of a *computable function*

$$f : \Lambda^* \rightarrow \Lambda^*$$

for an arbitrary finite Λ; a set of words $A \subseteq \Lambda^*$ will be *decidable* if its characteristic function

$$\chi_A(\alpha) = \begin{cases} T & \text{if } \alpha \in A \\ F & \text{otherwise,} \end{cases}$$

where T and F are any two, specific, distinct strings standing for truth and falsity.

Alan Turing had (in 1936) the fundamental intuition that a string function is computable if its values can be computed by some "mechanical device" (machine) which has access to the string argument of the function and an unbounded amount of "scratch paper" for each computation. Turing's abstract, mathematical model of "machine" was introduced before actual computers had been built, but it has proved very robust and (in all interesting aspects other than efficiency, which does not concern us here) equivalent to the electronic computers we use today.

4D.1. Turing machines. A Turing machine is a structure

$$M = (S, Q_0, \Sigma, \sqcup, \mathrm{Table}),$$

where the following hold.

(1) S is a finite set, the set of (internal) *states* of M, and $Q_0 \in S$ is a specified *initial state*.

(2) Σ is a finite set, the set of *symbols* (alphabet) of M, and $\sqcup \in \Sigma$ is a specified member of Σ standing for "the blank symbol" (empty space).

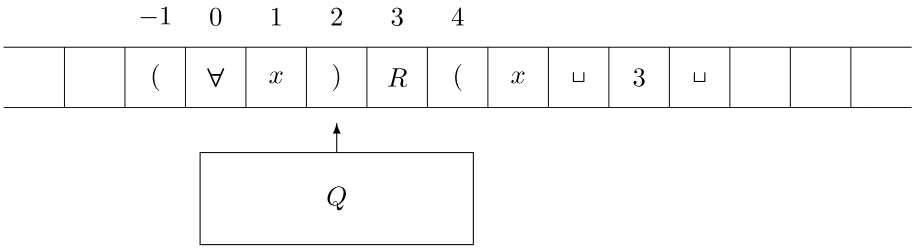
(3) The Table of M is a finite set of *transitions*, i.,e., quintuples of the form

$$Q, X \mapsto X', Q', m \tag{102}$$

where Q and Q' are states; X and X' are symbols; and the *move* of the transition $m \in \{0, -1, +1\}$. We say that the pair (Q, X) *activates* the transition.

A machine M is *deterministic* if for each state Q and each symbol X there is at most one transition which is activated by the pair (Q, X), otherwise it is *non-deterministic*.

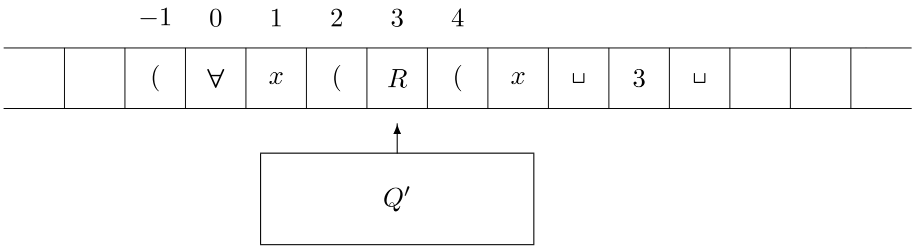
Turing's image is that the machine is situated in front of a two-way infinite *tape* which has a finite number of symbols from the alphabet placed on it; the machine can only see the symbol on the *cell* just in front of it—it cannot see any other symbols and it cannot see the coordinate of that cell, i.e., it does not "know" where it is on the tape.



If the machine is in state Q and the *visible symbol* is X, then each transition (102) in the machine's Table which is activated by the pair (Q, X) produces a change in this *situation*, overwriting the symbol X by the *new symbol* X', changing from the *current state* Q to the *new state* Q' and *moving* one-cell-to-the-left if the move $m = -1$, not-at-all if $m = 0$, and one-cell-to-the-right if $m = 1$. For example, the transition

$$Q,) \mapsto (, Q', +1$$

will change the situation in the picture above to the new situation:



Finally, a *computation* of M is a sequence of successive situations produced by transitions of M in this way, starting with an *initial situation* involving the initial state Q_0.

Without further explanation of this simple idea, we proceed to the precise definitions of the notions italicized in these remarks.

Definition 4D.2. For a fixed Turing machine $M = (S, Q_0, \Sigma, \sqcup, \text{Table})$, we define:

(1) A *tape* (description) is any function $\tau : \mathbb{Z} \to \Sigma$, which assigns a symbol of M to each rational integer

$$i \in \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\},$$

such that for all but finitely many i, $\tau(i) = \sqcup$.

(2) A *situation* of M is any triple

$$s = (Q, \tau, i),$$

where Q is a state, τ is a tape and $i \in \mathbb{Z}$. The *state* of M in this situation is Q; the *place* of M in s is the integer i; and the *visible symbol* in s is $\tau(i)$. We call s *initial* if Q is the initial state Q_0 of M and $i = 0$; and we call s *terminal* if either there is no transition in the table of M activated by the pair $(Q, \tau(i))$ or the only transition activated by this pair is a "stand-pat" transition

$$Q, X \mapsto X, Q, 0.$$

(3) A situation $s' = (Q', \tau', i')$ is a *next situation* to $s = (Q, \tau, i)$ if s is not terminal, if

$$j \neq i \Longrightarrow \tau(j) = \tau'(j),$$

and if the Table of M contains the transition

$$Q, \tau(i) \mapsto \tau'(i), Q', i' - i.$$

Notice that this implies $|i' - i| \leq 1$, since $i' - i$ is a move; that (by the definition) there is no s' next to s if s is terminal; and that if M is deterministic, then there is at most one s' next to s, since at most one transition can be activated by the given pair $(Q, \tau(i))$.

(4) A *computation* of M is any (finite or infinite) sequence of situations

$$s_0, s_1, \dots,$$

such that s_0 is initial and each s_{i+1} is next to s_i, diagrammatically

$$s_0 \mapsto s_1 \mapsto s_2 \mapsto \cdots$$

A computation is *maximal* if no extension of it is a computation, and a maximal, finite computation is called *convergent.* For each initial situation s_0, we set

(103) $M : s_0\!\downarrow$

$$\iff \text{there exists a convergent computation } s_0 \mapsto \cdots \mapsto s_m$$

and we read "$M : s_0\!\downarrow$" as "*M halts*" (or *converges*) *on* s_0.

It follows easily that if M is deterministic, then for each initial situation $s_0 = (Q_0, \tau, 0)$ there is exactly one maximal computation which starts with s_0, and that a maximal computation is either finite, ending with a terminal situation, or infinite (and with no terminal situations in it). We picture these possibilities in the following, simple examples of Turing machines.

4D.3. Example. The machine with just one state Q_0 on the alphabet $\{1, \sqcup\}$ and just two transitions

$$Q_0, 1 \mapsto 1, Q_0, +1$$
$$Q_0, \sqcup \mapsto 1, Q_0, +1$$

is deterministic, and starting from any initial situation, it moves to the right forever, printing a 1 on every cell to the right of the origin which does not already have a 1 in it.

4D.4. Example. On the same alphabet $\{1, \sqcup\}$, consider the machine with the following transitions (and the states which occur in these transitions):

(a) $$Q_0, 1 \mapsto 1, Q_0, +1$$

(b) $$Q_0, \sqcup \mapsto 1, Q_1, 0$$

(c) $$Q_1, 1 \mapsto 1, Q_1, -1$$

(d) $$Q_1, \sqcup \mapsto \sqcup, Q_2, +1$$

For each number x, let

$$\text{in}(x) = \cdots \sqcup\sqcup \underbrace{11 \ldots 1}_{x+1}, \sqcup\sqcup \ldots$$

be the tape with $x + 1$ 1s on and to the right of the origin and no other symbols but blanks, and consider the computation of this deterministic machine starting with the initial situation $(Q_0, \text{in}(x), 0)$. It will start with $x + 1$ executions of the transition (a), as long at is sees a 1, and then execute (b) just once, to write a 1 on the first blank cell on the right; it will then execute (c) $x + 3$ times, until it is back to the left of the origin, where it finds the first blank on the left, and finally execute (d) just once to move to the origin and stop, in the situation $(Q_2, \text{in}(x + 1), 0)$.

For each string $\alpha \equiv \alpha_0\alpha_1 \cdots \alpha_{n-1} \in \Lambda^*$, let

$$\text{in}(\alpha)(i) = \begin{cases} \alpha_i, & \text{if } 0 \leq i < n, \\ \sqcup, & \text{otherwise;} \end{cases}$$

this is the tape that we use to represent a string α an an *input* to a computation by a Turing machine whose alphabet includes Λ. Similarly, for each tape τ, let

$$\begin{aligned}\mathrm{out}(\tau) =& \tau(0)\tau(1)\cdots\tau(m-1)\\ & \text{for the least } m \in \mathbb{N} \text{ such that } \tau(m) = \sqcup,\end{aligned}$$

so that if $\tau(0) = \sqcup$, then $\mathrm{out}(\tau) = \epsilon$ (the empty string), and if $\tau(0) = N$, $\tau(1) = O$ and $\tau(2) = \sqcup$, then $\mathrm{out}(\tau) = NO$.

Definition 4D.5 (Turing computable functions)**.** A Turing machine

$$M = (S, Q_0, \Sigma, \sqcup, \mathrm{Table})$$

computes a function

$$f : \Lambda^* \to \Lambda^*$$

if $\Lambda \subseteq \Sigma$; $\sqcup \notin \Lambda$; and for all strings α, $\beta \in \Lambda^*$,

$$\begin{aligned}f(\alpha) = \beta \iff & \text{there exists a convergent computation } s_0, s_1, \dots s_m \text{ of } M\\ & \text{such that } s_0 = (Q_0, \mathrm{in}(\alpha), 0) \text{ and } s_m = (Q, \tau', i), \text{ with } \mathrm{out}(\tau') = \beta.\end{aligned}$$

Similarly, and representing each tuple $x_1, \dots, x_n$ of numbers by the string of 1s and blanks

$$\mathrm{in}(x_1, \dots, x_n) = \dots \sqcup\sqcup \underbrace{11\dots1}_{x_1+1} \sqcup \underbrace{11\dots1}_{x_2+1} \dots \sqcup \underbrace{11\dots1}_{x_n+1} \sqcup\sqcup \dots$$

(with $\mathrm{in}(x_1, \dots, x_n)(0) =$ the first 1), a Turing machine M as above computes a function

$$f : \mathbb{N}^n \to \mathbb{N}$$

if the alphabet of M includes the symbol 1 and for all $x_1, \dots, x_n$, w,

$$\begin{aligned}f(x_1, \dots, x_n) = w \iff & \text{there exists a convergent computation}\\ & s_0, s_1, \dots s_m \text{ of } M \text{such that}\\ & s_0 = (Q_0, \mathrm{in}(x_1, \dots, x_n), 0)\\ & \text{and } s_m = (Q, \tau', i), \text{ with } \mathrm{out}(\tau') = \underbrace{11\dots1}_{w+1}.\end{aligned}$$

Note that in both situations, if the machine M is deterministic, then for each input, there will be exactly one convergent computation ("the computation") of M which computes the value of the function.

A string or number-theoretic function is **Turing computable** if it is computed by a deterministic Turing machine.

After giving these definitions, Turing claimed that his simple, restricted machines can actually compute all functions on strings which are "intuitively computable", so that his precise definition can be used to prove rigorously that specific functions *are not computable in any way whatsoever*, by showing that they cannot be computed by a Turing machine. Alonzo Church had made a similar proposal for another, precisely defined class of functions (subsequently proved to coincide with the class of Turing computable functions), so that the next, fundamental claim carries now both their names:

4D.6. The Church-Turing Thesis. *A string function* $f : \Lambda^* \to \Lambda^*$ (on a finite alphabet Λ) *is computable exactly when it is Turing computable*; *and a set of strings* $A \subseteq \Lambda^*$ *is decidable exactly when its characteristic function is decidable, taking* (for concreteness) $T = \text{in}(1)$ *and* $F = \text{in}(0)$.

Since the operations

$$x_1, \dots, x_n \mapsto \text{in}(x_1, \dots, x_n) \quad \text{and} \quad \text{in}(w) \mapsto w$$

which code and decode numbers by strings of 1s are evidently computable (in a very basic, intuitive sense), the Church-Turing Thesis implies its version for functions on the natural numbers:

4D.7. The Church-Turing Thesis for functions on $\mathbb{N}$. *A number-theoretic function* $f : \mathbb{N}^n \to \mathbb{N}$ *is computable exactly when it is Turing computable; and a relation* $R \subseteq \mathbb{N}^n$ *is decidable exactly when its characteristic function is Turing computable.*

4D.8. Remarks. The Church-Turing Thesis is not a theorem and cannot be rigorously proved, as it identifies the premathematical, intuitive notion of "computability" with a precisely defined (set-theoretic) notion of "computability by a Turing machine". At the same time, the Thesis is not a "definition by stipulation", in the sense that when we adopt it we simply *decide* (arbitrarily and for convenience) to call a function "computable" exactly when it is Turing computable—it would not be useful if that were all it is. Its status is similar to the "definitions" of *area* and *volume* in Geometry or *work* in Physics, which within a rigorous development of mathematics are treated as arbitrary, stipulative definitions, but whose significance for applications derives from the fact that they are not-at-all arbitrary: when we prove that the volume of a ball of radius r is $(4/3)\pi r^3$ using the "definition" of volume via an integral, we make a claim that the physical approximations to ideal balls we meet in our world will exhibit this relationship between their radius and their volume—and experimentation verifies this. In the same way, when we prove that a certain function $f : \mathbb{N} \to \mathbb{N}$ is not Turing computable, we claim (through the Church-Turing Thesis) that nobody, ever will devise an "algorithm" which (effectively and uniformly) will compute each value $f(m)$ from the argument m, and this claim is subject to experimentation and verification.

The main arguments supporting the truth of the Church-Turing Thesis are

(1) Turing's original analysis of the notion of "machine computability", strengthened immensely by our current, much better understanding

of *symbolic computation* gained from our experience with actual computers;

(2) the great wealth of Turing computable functions, and the very strong closure properties of the class of Turing computable functions; and

(3) the experience of more than seventy years, which has failed to produce plausible counterexamples.

We will not elaborate on any of these here, except that the main evidence for (2) will be detailed in the subsequent sections on *computability theory.*

The main applications of the Church-Turing Thesis are *negative*, in proofs which establish that certain functions are not computable by proving (rigorously) that they are not Turing computable and appealing to the Thesis. It is customary to claim sometimes that "f is Turing computable, since we have given intuitive instructions for computing it", but what is always meant by this is "f is Turing computable, but I do not want to take the time to prove this in detail because it is boring and routine (to someone who has understood the justification of the Church-Turing thesis)".

4E. Computable partial functions

Not every deterministic Turing machine computes a string function, because the computation from any given string α may fail to terminate, as in Example 4D.3, where the computation *on every input* is infinite and fails to return a value; however, every Turing machine computes a "partial string function", where these objects are defined as follows:

Definition 4E.1. A **partial function**

$$f : X \rightharpoonup Y$$

on a set X to some set Y is any (ordinary, total) function

$$f : X_0 \to Y,$$

where X_0 is any subset of X. We call X_0 the *domain of convergence* of f, and set

$$\begin{aligned} f(x)\downarrow &\iff x \in X_0 \qquad (f(x) \text{ \textit{converges} or \textit{is defined}}) \\ f(x)\uparrow &\iff x \in X \setminus X_0 (f(x) \text{ \textit{diverges}}). \end{aligned}$$

Notice the special notation $\rightharpoonup$ which indicates that f is a partial function. Notice also that, by the definition, every total $f : X \to Y$ is a partial function (taking $X_0 = X$), and (at the other extreme), taking $X_0 = \emptyset$, we have the *totally undefined* partial function $f : X \rightharpoonup Y$ for which $f(x)\uparrow$, for every $x \in X$.

Turing computability for string and number-theoretic partial functions is defined (almost) exactly like the corresponding notion for total functions in 4D.5, except that we insist that the machine computation "converges" (is finite) exactly when the partial function converges. We repeat the definition to make precise this additional condition.

4E.2. Turing computable partial functions. A Turing machine

$$M = (S, Q_0, \Sigma, \sqcup, \text{Table})$$

computes a partial function

$$f : \Lambda^* \rightharpoonup \Lambda^*$$

if $\Lambda \subseteq \Sigma$; $\sqcup \notin \Lambda$; and for all strings α, $\beta \in \Lambda^*$,

$$\begin{aligned} f(\alpha)\downarrow &\iff M : (Q_0, \text{in}(\alpha), 0)\downarrow, \\ f(\alpha) = \beta &\iff \text{there exists a convergent computation } s_0, s_1, \dots s_m \text{ of } M \\ &\qquad \text{such that } s_0 = (Q_0, \text{in}(\alpha), 0) \text{ and } s_m = (Q, \tau', i), \\ &\qquad \text{with out}(\tau') = \beta; \end{aligned}$$

similarly, a Turing machine M as above computes a partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ if the alphabet of M includes the symbol 1, and for all $x_1, \dots, x_n$, w,

$$\begin{aligned} f(x_1, \dots, x_n)\downarrow &\iff M : (Q_0, \text{in}(x_1, \dots, x_n), 0)\downarrow, \\ f(x_1, \dots, x_n) = w &\iff \text{there exists a convergent computation } s_0, s_1, \dots s_m \\ &\qquad \text{of } M \text{ such that } s_0 = (Q_0, \text{in}(x_1, \dots, x_n), 0) \\ &\qquad \text{and } s_m = (Q, \tau', i), \text{ with out}(\tau') = \underbrace{11\dots1}_{w+1}. \end{aligned}$$

A string or number-theoretic partial function is **Turing computable** if it is computed by a deterministic Turing machine.

4E.3. The Church-Turing Thesis for partial functions. *A string partial function $f : \Lambda^* \rightharpoonup \Lambda^*$ is computable exactly when it is Turing computable*; and *a number-theoretic partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ is computable exactly when it is Turing computable.*

Number theoretic partial functions arise very naturally through the application of the following (unbounded) *minimalization* operator, which, on the surface, is unrelated to Turing computability.

Definition 4E.4 (Unbounded minimalization)**.** With each partial function

$$g : \mathbb{N}^{n+1} \rightharpoonup \mathbb{N},$$

we associate a new, n-ary partial function

$$\begin{aligned} f(\vec{x}) =& \mu y[g(\vec{x}, y) = 0] \\ &= \text{the least number } y \text{ such that} \\ &\quad (\forall u < y)(\exists w)[g(\vec{x}, u) = w + 1] \ \& \ g(\vec{x}, y) = 0, \end{aligned}$$

with the obvious domain of convergence,

$$\mu y[g(\vec{x}, y) = 0]\downarrow \iff (\exists y)\Big[(\forall u < y)(\exists w)[g(\vec{x}, u) = w + 1] \ \& \ g(\vec{x}, y) = 0\Big];$$

we say that f is defined from g by **minimalization**.

Note that if g is a total function such that for all $\vec{x}$ there is at least one y such that $g(\vec{x}, y) = 0$, then this is *exactly* minimalization,

$$\mu y[g(\vec{x}, y) = 0] = \text{the least number } y \text{ such that } g(\vec{x}, y) = 0;$$

but if (for example) $g(x, 0)\uparrow$ and $g(x, 1) = 0$, then $\mu y[g(x, y) = 0]\uparrow$.

We also use the minimalization operation on relations, in the obvious way:

$$\mu y R(\vec{x}, y) = \mu y[1 \dot{-} \chi_R(\vec{x}, y) = 0].$$

Definition 4E.5 (μ-recursion)**.** A **μ-recursive derivation** is a sequence of partial functions on $\mathbb{N}$

$$f_0, f_1, \ldots, f_k,$$

where each f_i is S, or a constant C^n_q or a projection P^n_i, or is defined by composition, primitive recursion or minimalization from functions before it in the sequence; and a partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ is **μ-recursive** if it occurs in a μ-recursive derivation.

In interpreting this definition, we must understand the operations of *composition* and *primitive recursion* correctly for partial functions, for example

$$f(g(\vec{x}), h(\vec{x})) = w \iff (\exists u)(\exists v)[g(\vec{x} = u \ \& \ h(\vec{x}) = v) \ \& \ f(u, v) = w].$$

It is clear that every primitive recursive function is μ-recursive, and that the class of μ-recursive partial functions is closed under composition, primitive recursion and minimalization.

The next result is proved by a sequence of tedious constructions of deterministic Turing machines ("Turing machine programming") which we will omit:

Theorem 4E.6. *Every μ-recursive partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ is Turing computable.*

4E.7. Coding. The converse—and much of the elementary theory of Turing computable functions—is derived by coding the theory of a fixed (possibly non-deterministic) Turing machine $M = (S, Q_0, \Sigma, \sqcup, \text{Table})$ as follows.

If $S = \{Q_0, \dots, Q_a\}$, let $[Q_i] = i$, so that 0 is the code of the initial state and the relation

$$\begin{aligned}\mathrm{State}_M(i) &\iff i \text{ is the code of a state of } M\\ &\iff i \leq a\end{aligned}$$

is primitive recursive. Similarly, if $\Sigma = \{\sqcup, R_1, \dots, R_b\}$, let $[R_j] = j$, so that 0 is the code of $\sqcup$ and the relation

$$\begin{aligned}\mathrm{Symbol}_M(j) &\iff j \text{ is the code of a symbol of } M\\ &\iff j \leq b\end{aligned}$$

is also primitive recursive.

The coding of tapes is messier, because we have to deal with negative numbers and tapes are "infinite", albeit with only finitely many symbols on them. It is convenient to allow many codes for the same tape. We let

$$\mathrm{Tape}_M(t) \iff \mathrm{Seq}(t) \;\&\; (\forall i < \mathrm{lh}(t))[\mathrm{Symbol}_M((t)_{i,0}) \;\&\; \mathrm{Symbol}_M((t)_{i,1})],$$

and with each t such that $\mathrm{Tape}_M(t)$ we associate the tape

$$\tau_t(i) = \begin{cases} R_{(t)_{i,0}} & \text{if } 0 \leq i < \mathrm{lh}(t)\\ R_{(t)_{-i,1}} & \text{if } i < 0 \text{ and } -i < \mathrm{lh}(t)\\ \sqcup & \text{otherwise,}\end{cases}$$

where we have used the notation $(u)_{i,j}$ for the j'th component of the i'th component of the sequence code u

(104) $$(u)_{i,j} = ((u)_i)_j.$$

It is that clear the tape relation is primitive recursive, that every tape gets many codes by this definition, and that "decoding" the tape from any of its codes is "primitive recursive".

Situations are coded as triples of codes, as usual:

$$\mathrm{Sit}_M(s) \iff \mathrm{Seq}(u) \;\&\; \mathrm{lh}(s) = 3 \;\&\; \mathrm{State}_M((s)_0) \;\&\; \mathrm{Tape}_M((s)_1);$$

here, $(s)_2$ codes $i \in \mathbb{Z}$ in some fixed way, e.g., $\mathrm{place}(s) = (s)_{2,0}$ if $(s)_{2,1} = 0$, and $\mathrm{place}(s) = -(s)_{2,0}$ if $(s)_{2,1} > 0$.

With these definitions it is not hard to verify that the relation

$$\begin{aligned}\mathrm{Next}_M(s, s') \iff\; & s \text{ codes a situation } \overline{s}\\ & \& \; s' \text{ codes a situation } \overline{s}'\\ & \& \; \overline{s}' \text{ is a next situation to } \overline{s}\end{aligned}$$

is primitive recursive, and, using it,

$$\mathrm{Terminal}_M(s) \iff s \text{ is a code of a terminal situation}$$

is primitive recursive too.

Theorem 4E.8. *For each Turing machine* $M = (S, Q_0, \Sigma, \sqcup, \mathrm{Table})$*:*

(1) *The relation*

$$\begin{aligned}\mathrm{Comp}_M(y) &\iff y \text{ is a code of a convergent computation of } M\\ &\iff \mathrm{Seq}(y)\\ &\qquad \& \ (\forall i < \mathrm{lh}(y))[i+1 < \mathrm{lh}(y) \Longrightarrow \mathrm{Next}_M((y)_i, (y)_{i+1})]\\ &\qquad \& \ \mathrm{Terminal}_M((y)_{\mathrm{lh}(y) \dot{-} 1})\end{aligned}$$

is primitive recursive.

(2) *For each* n*, there is a primitive recursive function* $\mathrm{input}_n : \mathbb{N}^n \to \mathbb{N}$ *such that for each tuple* $\vec{x} = (x_1, \ldots, x_n)$*,* $\mathrm{input}_n(\vec{x})$ *is a code of the initial situation* $(Q_0, \mathrm{in}(\vec{x}), 0)$*.*

(3) *There is a primitive recursive function* $\mathrm{output}(s)$*, such that if* s *is a code of a terminal situation* (Q, τ', j) *and* $\mathrm{out}(\tau') = \underbrace{11\ldots1}_{w+1}$*, then* $\mathrm{output}(s) = w$*.*

(4) *If a partial function* $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ *is computed by a* (possibly non-deterministic) *Turing machine, then it is* μ*-recursive.*

In particular: *every Turing computable partial function is* μ*-recursive.*

PROOF. (1) is immediate and (2) and (3) are verified by simple (if messy) explicit constructions. For (4), we note that, by the definitions,

$$\begin{aligned}&f(\vec{x}) = w\\ \iff\ &(\exists y)[\mathrm{Comp}_M(y) \ \& \ (y)_0 = \mathrm{input}_n(\vec{x}) \ \& \ \mathrm{output}((y)_{\mathrm{lh}(y) \dot{-} 1}) = w],\end{aligned}$$

so that the graph of f satisfies an equivalence of the form

$$f(\vec{x}) = w \iff (\exists y)R(\vec{x}, w, y)$$

with a primitive recursive relation R; but then

$$f(\vec{x}) = \Big(\mu y R(\vec{x}, (y)_0, (y)_1)\Big)_0,$$

and $f(\vec{x})$ is μ-recursive. ⊣

We introduce one more, proof-theoretic notion of computability for partial functions (due to Gödel), and a useful variation.

Definition 4E.9 (Reckonability)**.** Suppose $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$, $\mathbf{F}(v_1, \ldots, v_n, y)$ is a full extended formula in the language of PA, and T is a theory in the language of PA. We say that $\mathbf{F}(v_1, \ldots, v_n, y)$ **reckons** f **in** T if for all $\vec{x}, w$,

$$f(\vec{x}) = w \iff T \vdash \mathbf{F}(\Delta x_1, \ldots, \Delta x_n, \Delta w);$$

$\mathbf{F}(v_1, \dots, v_n, y)$ **soundly reckons** f **in** T if for all $\vec{x}, w$, the following two conditions hold:

$$f(\vec{x}) = w \implies T \vdash \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w),$$
$$\mathbf{N} \models \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w) \implies f(\vec{x}) = w.$$

It is clear that if T is sound and f is soundly reckonable in T, then f is reckonable in T, but otherwise these two notions are not easily related.

Theorem 4E.10. *For a partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$, the following are equivalent:*

(1) *f is μ-recursive.*

(2) *f is soundly reckonable in Q.*

(3) *f is reckonable in Q.*

(4) *f is reckonable in some axiomatizable theory T in the language of* PA.

(5) *The graph of f satisfies an equivalence of the form*

$$f(\vec{x}) = w \iff (\exists y) R(\vec{x}, w, y), \tag{105}$$

with some primitive recursive relation $R(\vec{x}, w, y)$.

Proof. (1) $\implies$ (2). It is enough to show that the class of partial functions which are soundly reckonable in Q contains the basic S, C^n_q and P^n_i and is closed under composition, primitive recursion and minimalization. We outline the argument for the last case, the others being similar (and a bit simpler).

So suppose that

$$f(x) = \mu y[g(x, y) = 0]$$

(taking a function of one variable for simplicity) and $\mathbf{G}(v_1, v_2, w)$ soundly reckons $g(x, y)$ in Q, and set

$$\mathbf{F}(v_1, y) \equiv \mathbf{G}(v_1, y, 0) \ \& \ (\forall z < y) \exists w \mathbf{G}(v_1, z, S(w)).$$

To prove that this formula reckons f soundly in Q, assume first that $f(x) = y$, so that

$$\begin{aligned} \mathsf{Q} \vdash \quad & \mathbf{G}(\Delta x, \Delta 0, \Delta w_0) \\ & \& \ \mathbf{G}(\Delta x, \Delta 1, \Delta w_1) \\ & \quad \vdots \\ & \& \ \mathbf{G}(\Delta x, \Delta(y-1), \Delta w_{y-1}) \\ & \& \ \mathbf{G}(\Delta x, \Delta y, \Delta 0) \end{aligned}$$

with suitable numbers $w_z \neq 0$ for $z < y$. The required conclusion, that $\mathsf{Q} \vdash \mathbf{F}(\Delta x, \Delta y)$ follows easily, by appealing to basic properties of Q.

To verify the second condition required of sound reckonability, suppose $\mathbf{N} \models \mathbf{F}(\Delta x, \Delta y)$, so that there are numbers $w_0, \dots, w_{y-1}$ all > 0, such that

$$\mathbf{N} \models \mathbf{G}(\Delta x, \Delta y, 0), \mathbf{G}(\Delta x, 0, \Delta w_0), \dots, \mathbf{G}(\Delta x, \Delta(y-1), \Delta w_{y-1};$$

now the hypothesis about g easily implies that $f(x) = y$.

(2) $\Longrightarrow$ (3) follows immediately from the soundness of Q, and (3) $\Longrightarrow$ (4) is trivial, taking $T = \mathsf{Q}$.

(4) $\Longrightarrow$ (5) The hypothesis implies that

$$f(\vec{x}) = w \iff (\exists y)\mathrm{Proof}_T(\#\mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w), y)$$

so that f satisfies (105) with

$$R(\vec{x}, w, y) \iff \mathrm{Proof}_T(\#\mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w), y),$$

which is primitive recursive.

(5) $\Longrightarrow$ (1) If f satisfies (105) with a primitive recursive R, then as in the proof of (4) of Theorem 4E.8,

$$f(\vec{x}) = \Big(\mu t R(\vec{x}, (t)_0, (t)_1)\Big)_0,$$

so that f is μ-recursive. ⊣

Thus for any partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$,

$$\begin{aligned} f \text{ is Turing computable} &\iff f \text{ is } \mu\text{-recursive} \\ &\iff f \text{ is reckonable in } \mathsf{Q} \\ &\iff f \text{ is reckonable in some axiomatizable } T \end{aligned}$$

and these equivalences are part of the evidence for the Church-Turing Thesis.

Definition 4E.11 (Recursive partial functions and relations)**.** From now on we will call **computable** or **recursive** the number-theoretic partial functions which are "μ-recursive" (equivalently: "Turing computable", etc.); and we will call **decidable** or **recursive** the relations on $\mathbb{N}$ whose characteristic function is recursive. The term "recursive" is the most common appellation for this class of partial functions and relations, and so we wii tend to use it most often; it derives not so much from μ-recursiveness but from another, fundamental characterization of computability which we will not introduce just yet.

There are two important corollaries of Theorem 4E.10 which appeal to condition (5):

Corollary 4E.12 (Definition by cases)**.** *If $P(\vec{x})$ is a recursive relation, g_1 and g_2 are recursive partial functions, and*

$$f(\vec{x}) = \begin{cases} g_1(\vec{x}), & \text{if } P(\vec{x}), \\ g_2(\vec{x}), & \text{otherwise,} \end{cases} \tag{106}$$

then f is recursive.

Proof. Given representations of g_1 and g_2 of the form (105) with respective primitive recursive relations $R_1(\vec{x}, w, y)$ and $R_2(\vec{x}, w, y)$, we verify easily that

$$f(\vec{x}) = w \iff (\exists y)\Big[(P(\vec{x})\ \&\ R_1(\vec{x}, w, y)) \vee (\neg P(\vec{x})\ \&\ R_2(\vec{x}, w, y))\Big];$$

now the relation within the brackets is primitive recursive, and so f is recursive. ⊣

Corollary 4E.13. *Recursive functions and recursive relations on* $\mathbb{N}$ *are arithmetical, and, in particular, the truth relation* $\mathrm{Truth}^{\mathbf{N}}(e)$ *for* $\mathbf{N}$ *is not recursive.*

Proof. Every recursive function is reckonable, and so its graph satisfies an equivalence (105) with primitive recursive—and hence arithmetical—R, so it is arithmetical. The second claim follows from this and Tarski's Theorem 4A.5. ⊣

4F. The basic undecidability results

The results in the preceding section add up to the following basic theorem, which is the key tool for proving undecidability theorems:

Theorem 4F.1 (Kleene's Normal form and Enumeration Theorem)**.** *Let*

$$U(y) = (y)_0$$

(to agree with classical notation)*, and for each n, let*

$$\begin{aligned} T_n(e, x_1, \dots, x_n, y) \iff\ & e \text{ is the code of a} \\ & \text{full extended formula } \psi(\mathrm{v}_0, \dots, \mathrm{v}_n) \\ & \text{in which } \mathrm{v}_0, \dots, \mathrm{v}_n \text{ actually occur (free)} \\ & \text{and } (y)_1 \text{ is the code of a proof in } \mathsf{Q} \\ & \text{of the sentence } \psi(\Delta x_1, \dots, \Delta x_n, \Delta(y)_0), \\ \varphi_e^n(x_1, \dots, x_n) \ =\ & U(\mu y T_n(e, x_1, \dots, x_n, y)), \end{aligned}$$

(1) *The function $U(y)$ and each relation $T_n(e, \vec{x}, y)$ are primitive recursive.*

(2) *Each* $\varphi^n_e(\vec{x})$ *is a recursive partial function, and so is the partial function which "enumerates" all these,*

$$\varphi^n(e, \vec{x}) = \varphi^n_e(\vec{x}).$$

(3) *For each recursive partial function* $f(x_1, \dots, x_n)$ *of* n *arguments, there exists some* e (a code of f) *such that*

$$f(\vec{x}) = \varphi^n_e(\vec{x}) = U(\mu y T_n(e, x_1, \dots, x_n, y)), \tag{107}$$

so that for each n*, the sequence*

$$\varphi^n_0, \varphi^n_1, \varphi^n_2, \dots$$

enumerates all n*-ary recursive partial functions.*

Proof. Only (3) needs to be proved, and for that we let e be the code of some formula $\psi(\mathrm{v}_0, \dots, \mathrm{v}_n)$ which reckons f in Q by Theorem 4E.10 and which is (easily) adjusted so that $\mathrm{v}_0, \dots, \mathrm{v}_n$ are the first $n+1$ individual variables and they all actually occur free in it; the verification of (107) is immediate. ⊣

Note: The technical requirement on the free variables of $\psi(\mathrm{v}_0, \dots, \mathrm{v}_n)$ is not needed for this proof; it will be useful in the proof of Theorem 5A.1 further on, and it is just convenient to include it in the definition of the T-predicate now.

Theorem 4F.2 (Undecidability of the Halting problem, Turing)**.** *The relation*

$$H(e, x) \iff \varphi^1_e(x)\downarrow \quad (\iff (\exists y) T_1(e, x, y))$$

is undecidable.

Proof. If $H(e, x)$ were a recursive relation, then the total function

$$f(x) = \begin{cases} \varphi^1_x(x) + 1 & \text{if } \varphi^1_x(x)\downarrow \\ 0 & \text{otherwise} \end{cases}$$

would be recursive, and so for some e and all x we would have

$$\varphi^1_e(x) = f(x) = \varphi^1_x(x) + 1;$$

but this is absurd for $x = e$. ⊣

The proof uses the undecidability of the "diagonal" relation

$$K(e) \iff (\exists y) T_1(e, e, y)$$

which is often useful in getting undecidability results. In fact most (elementary) undecidability results are shown by proving an equivalence of the form

$$P(\vec{x}) \iff R(f(\vec{x})),$$

where $f(\vec{x})$ is a recursive function and $P(\vec{x})$ a known, undecidable relation, often $H(e, x)$ or $K(e)$; this is called a **reduction** of $P(\vec{x})$ to $R(u)$, and it implies immediately that $R(u))$ cannot be recursive, else $P(\vec{x})$ would be too. Some of these applications appeal also to the following, trivial

Lemma 4F.3. *If $\mathbf{T}(v_1, v_2, v_3)$ is a formula which numeralwise expresses the primitive recusive relation $T_1(e, x, y)$ in Q, then*

$$\begin{aligned} H(e,x) \iff \varphi_e^1(x)\downarrow &\iff (\exists y)T_1(e,x,y) \\ &\iff \mathsf{Q} \vdash (\exists y)\mathbf{T}(\Delta e, \Delta x, y) \\ &\iff \mathbf{N} \models (\exists y)\mathbf{T}(\Delta e, \Delta x, y). \end{aligned}$$

Definition 4F.4. A theory T in a finite signature τ is **decidable**, if (the characteristic function of) the set (of codes of) its theorems

$$\#T = \{\#\theta \mid \theta \text{ is a } \tau\text{-sentence and } T \vdash \theta\}$$

is decidable , otherwise T is **undecidable**.

The next result extends considerably Corollary 4E.13:

Theorem 4F.5. *If T is a sound extension of Q in the language of PA, then T is undecidable.*

In particular, Q and PA are undecidable.

Proof. By Lemma 4F.3 and the hypothesis, for any $e, x \in \mathbb{N}$,

$$H(e,x) \Longrightarrow \mathsf{Q} \vdash \exists y \mathbf{T}(\Delta e, \Delta x, y) \Longrightarrow T \vdash \exists y \mathbf{T}(\Delta e, \Delta x, y);$$

and, conversely, by the assumed soundness of T,

$$T \vdash \exists y \mathbf{T}(\Delta e, \Delta x, y) \Longrightarrow \mathbf{N} \models \exists y \mathbf{T}(\Delta e, \Delta x, y) \Longrightarrow H(e,x),$$

again by Lemma 4F.3. Thus

$$H(e,x) \iff T \vdash \exists y \mathbf{T}(\Delta e, \Delta x, y),$$

and so if T were decidable so would $H(e,x)$ be decidable, which it is not.$\dashv$

The undecidability of Q also yields the undecidability of logical provability (i.e., logical truth):

Theorem 4F.6 (Church's Theorem)**.** *For some finite signature τ, the relation*

$$\mathrm{Th}_\tau(e) \iff e \text{ is the code of a sentence } \theta \text{ of } \mathbb{FOL}(\tau) \text{ and } \vdash \theta$$

is undecidable.

Proof. We take the signature τ of the language of arithmetic, and notice that if α_{Q} is the conjunction of the (finitely many) axioms of Robinson's Q, then for an arbitrary θ in this language,

$$\mathsf{Q} \vdash \theta \iff \vdash \alpha_{\mathsf{Q}} \to \theta,$$

and so by Lemma 4F.3,

$$H(e,x) \iff \vdash \alpha_{\mathsf{Q}} \to (\exists y)\mathbf{T}(\Delta e, \Delta x, y);$$

but the function

$$g(e,x) = \#(\alpha_{\mathsf{Q}} \to (\exists y)\mathbf{T}(\Delta e, \Delta x, y))$$

is primitive recursive, and so

$$H(e,x) \iff \mathrm{Th}(g(e,x))$$

and Th(e) cannot be recursive, since $H(e,x)$ is not. ⊣

To extend Theorem 4F.5 to consistent theories in languages richer than he language of PA and not necessarily sound, we need the following simple extension of the undecidability of the Halting Problem:

Theorem 4F.7. *There is a recursive partial function $u : \mathbb{N} \rightharpoonup \{0,1\}$ which has no recursive, total extension.*

PROOF. We let

$$u(t) = 1 \dot{-} \varphi_t(t) = 1 \dot{-} U(\mu y T_1(t,t,y)). \tag{108}$$

This is evidently μ-recursive. Suppose, towards a contradiction, that $f : \mathbb{N} \to \mathbb{N}$ is a total, recursive function which extends u, i.e., such that

$$u(t)\downarrow \implies u(t) = f(t),$$

and let e be a code of f, so that $f = \varphi_e$. Now

$$u(e) = 1 \dot{-} \varphi_e(e) = f(e) = \varphi_e(e),$$

which is absurd when $\varphi_e(e)\downarrow$. ⊣

Theorem 4F.8. *If T is a consistent theory in a language $\mathbb{FOL}(\tau)$ with finite τ and Q is interpretable in T, then T is undecidable.*

PROOF. Let $u : \mathbb{N} \rightharpoonup \{0,1\}$ be a recursive partial function which has no total, recursive extension, by Theorem 4F.7, and let $\phi(v,y)$ be a full extended formula which numeralwise represents u in Q, so that

$$\text{if } u(t) = w, \text{ then } \mathsf{Q} \vdash \phi(\Delta t, \Delta w) \text{ and } \mathsf{Q} \vdash \exists! y \phi(\Delta t, y).$$

In particular,

$$u(t) = 0 \Longrightarrow \mathsf{Q} \vdash \phi(\Delta t, 0). \tag{109}$$

We claim that also

$$u(t) = 1 \Longrightarrow \mathsf{Q} \vdash \neg\phi(\Delta, 0); \tag{110}$$

this is because if $u(t) = 1$, then (writing 1 for $\Delta 1$),

$$\mathsf{Q} \vdash \phi(\Delta t, 1) \;\&\; \exists! y \phi(\Delta t, y),$$

from which we get immediately get that $\mathsf{Q} \vdash \neg\phi(\Delta t, 0)$, since $\mathsf{Q} \vdash 0 \neq 1$. If π is the assumed interpretation of Q in T, then (109), (110) and one of the basic properties of interpretations yield that

$$u(t) = 0 \Longrightarrow T \vdash \pi\phi(\Delta t, 0), \quad u(t) = 1 \Longrightarrow T \vdash \neg\pi\phi(\Delta t, 0). \tag{111}$$

Now let

$$f(t) = \begin{cases} 0, & \text{if } T \vdash \pi\phi(\Delta t, 0), \\ 1, & \text{otherwise.} \end{cases}$$

This is a total function, and if T is a decidable theory, it is recursive. Clearly

$$u(t) = 0 \Longrightarrow f(t) = 0 = u(t);$$

and since T is consistent and so cannot prove both $\pi\phi(\Delta t, 0)$ and $\neg\pi\phi(\Delta t, 0)$, (111) implies that

$$u(t) = 1 \Longrightarrow f(t) = 1 = u(t).$$

Thus f is a total, recursive extension of u, which is a contradiction. $\dashv$

Notice that Theorem 4F.8 is a direct generalization of Rosser's Theorem 4C.4, because of Problem x5.2.

4G. Problems for Chapter 4

Problem x4.1 (Lemma 3I.8)**.** If h is primitive recursive, then so are f and g, where:

(1) $f(x, \vec{y}) = \sum_{i<x} h(i, \vec{y})$, $(= 0$ when $x = 0)$.
(2) $g(x, \vec{y}) = \prod_{i<x} h(i, \vec{y})$, $(= 1$ when $x = 0)$.

Problem x4.2. If P_1, P_2, g_1, g_2 and g_3 are primitive recursive, then so is f defined from them by cases:

$$f(\vec{x}) = \begin{cases} g_1(\vec{x}), & \text{if } P_1(\vec{x}), \\ g_2(\vec{x}), & \text{if } \neg P_1(\vec{x}) \;\&\; P_2(\vec{x}), \\ g_3(\vec{x}), & \text{otherwise.} \end{cases}$$

Problem x4.3. The functions f_0, f_1 are defined by *simultaneous primitive recursion* from w_0, w_1, h_0 and h_1 if they satisfy the identities:

$$\begin{aligned} f_0(0) &= w_0, & f_1(0) &= w_1, \\ f_0(x+1) &= h_0(f_0(x), f_1(x), x), & f_1(x+1) &= h_1(f_0(x), f_1(x), x). \end{aligned}$$

Prove that if h_0, h_1 are primitive recursive, then so are f_0 and f_1.

Problem x4.4. Prove that if $g(\vec{x}, y)$ and $h(\vec{x})$ are both primitive recursive, then so is the function

$$f(\vec{x}) = (\mu y < h(\vec{x}))[g(\vec{x}, y) = 0]$$
$$\text{(with } f(\vec{x}) = h(\vec{x}) \text{ if } (\forall y < h(\vec{x}))[g(\vec{x}, y) \neq 0]).$$

Problem x4.5*. A function f is defined by *nested recursion* from g, h and τ if it satisfies the following identities:

$$f(0, y) = g(y),$$
$$f(x+1, y) = h(f(x, \tau(x, y)), x, y).$$

Prove that if f is defined from primitive recursive functions by nested recursion, then it is primitive recursive.

Problem x4.6*. Prove that there is a primitive recursive, one-to-one function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, such that

$$g(x, y) \leq (x + y + 1)^2.$$

More generally: show that for each $n \geq 2$, there is a primitive recursive. one-to-one function $g_n : \mathbb{N}^n \to \mathbb{N}$, such that

$$g_n(x_1, \ldots, x_n) \leq P_n(x_1, \ldots, x_n), \tag{112}$$

where $P_n(x_1, \ldots, x_n)$ is a polynomial of degree n.

Problem x4.7. Prove that for every $n \geq 2$, there is no one-to-one function $g : \mathbb{N}^n \to \mathbb{N}$ which satisfies (112) with a polynomial of degree $\leq n - 1$.

Problem x4.8. Prove that there is a primitive recursive coding of tuples in $\mathbb{N}$ such that for every n and all $x_1, \ldots, x_n$,

$$\langle x_1, \ldots, x_n \rangle \leq 2^n P_n(x_1, \ldots, x_n),$$

where the polynomial P_n has degree n.

Problem x4.9. Prove that for every coding $\langle\ \rangle : \mathbb{N}^* \rightarrowtail \mathbb{N}$ of tuples from $\mathbb{N}$,

$$\max\{\langle x_1, \ldots, x_n \rangle \mid x_1, \ldots, x_n \leq k\} \geq 2^n \quad (k, n \geq 2)$$

Problem x4.10. Show that Q does not prove that addition is associative, i.e.,

$$\mathsf{Q} \nvdash x + (y + z) = (x + y) + z.$$

Problem x4.11* (Lemma 4B.6). Show that Q can prove all true propositional combinations of closed equalities and inequalities between terms; i.e., if θ is a propositional sentence in the signature $(0, S, +, \cdot, \leq)$, then

$$\mathbf{N} \models \theta \iff \mathsf{Q} \vdash \theta.$$

Problem x4.12. Prove that if a relation $R(y, \vec{x})$ is numeralwise expressible in Q, then so is the relation

$$P(z, \vec{x}) \iff (\exists y \leq z) R(y, \vec{x}).$$

Problem x4.13 (Lemma 4A.3)**.** Prove that there is a primitive recursive function $\mathrm{sub}(e, i, a)$, such that whenever e is the code of an extended formula $\phi(\mathrm{v}_i)$ and a is the code of a term t which is free for v_i in ϕ, then $\mathrm{sub}(e, i, a)$ is the code of $\phi(t)$, i.e., the result of replacing v_i by t in all the free occurrences of v_i in $\phi(\mathrm{v}_i)$.

Problem x4.14 (Lemma 4A.7)**.** Outline a proof that the theory PA of Peano Arithmetic is axiomatizable.

Problem x4.15 (Lemma 4A.9)**.** Outline a proof that the proof predicate $\mathrm{Proof}_T(e, y)$ of an axiomatizable theory T is primitive recursive.

Problem x4.16. Prove that the theory $T = \mathsf{PA} + \neg\gamma_{\mathsf{PA}}$, obtained by adding to PA the negation of its Gödel sentence is consistent, incomplete, and not sound (for the standard model $\mathbf{N}$ of PA).

Problem x4.17. Suppose T is an axiomatizable theory, π is an interpretation of Q into T, and ρ is the Rosser sentence for T (relative to some axiomatization and π): is ρ true or false?

Problem x4.18. Prove that the theory ZFC (Zermelo-Fraenkel set theory with choice) defined in Definition 1G.12 is incomplete, unless it is inconsistent. (This requires knowing some set theory.)

Problem x4.19* (Abstract Löb Theorem)**.** Suppose T is a consistent, axiomatizable theory into which PA can be interpreted. Prove that for any sentence θ in the language of T,

$$\text{if } T \vdash \pi\Big(\exists y \mathbf{Proof}_{\pi,T}(\ulcorner\theta\urcorner, y)\Big) \to \theta, \text{ then } T \vdash \theta,$$

where $\mathbf{Proof}_{\pi,T}(e, y)$ is defined in the proof of Theorem 4C.4.

Problem x4.20. (A corrected version of #2 in the Fall 1998 Logic Qual.) Let PA be Peano arithmetic. For each formula θ of the language of PA, let $\#(\theta)$ be the Gödel number of θ (in some canonical Gödel numbering). For each axiomatized theory T in the language of PA, let

$$\mathbf{Provable}_T(x) \equiv (\exists y)\mathbf{Proof}_T(x, y),$$

where $\mathbf{Proof}_T(x, y)$ numeralwise expresses in PA the proof predicate of T, so that $\mathbf{Provable}_T(x)$ defines the relation

$$\mathrm{Provable}(x) \iff x \text{ is the Gödel number of a sentence } \theta_x \text{ and } T \vdash \theta_x.$$

For each of the following assertions, determine whether the assertion is true for every formula θ and prove your answers by reference to appropriate theorems where necessary.

(a) $\mathsf{PA} \vdash \mathbf{Provable}_{\mathsf{PA}+\neg\theta}(\Delta\#(\theta)) \to \mathbf{Provable}_{\mathsf{PA}}(\Delta\#(\theta))$.
(b) $\mathsf{PA} \vdash \mathbf{Provable}_{\mathsf{PA}}(\Delta\#(\theta)) \to \neg\mathbf{Provable}_{\mathsf{PA}}(\Delta\#(\neg\theta))$.

Problem x4.21. (#3 in the Fall 2002 Qual.) For each sentence θ in the language of Peano arithmetic PA, let

$$\ulcorner\theta\urcorner = \text{the (formal) numeral of the Gödel number of } \theta,$$

and let $\mathbf{Provable}_{\mathsf{PA}}(n)$ be a formula with one free variable which expresses the relation of *provability* in Peano arithmetic, so that (in particular), for each sentence θ,

$$(\mathbb{N}, 0, 1, +, \cdot) \models \mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner) \iff \mathsf{PA} \vdash \theta.$$

Consider the following four sentences which can be constructed from an arbitrary sentence θ:

(a) $\theta \to \mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner)$

(b) $\mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner) \to \theta$

(c) $\mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner) \to \mathbf{Provable}_{\mathsf{PA}}(\ulcorner\mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner)\urcorner)$

(d) $\mathbf{Provable}_{\mathsf{PA}}(\ulcorner\mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner)\urcorner) \to \mathbf{Provable}_{\mathsf{PA}}(\ulcorner\theta\urcorner)$

Determine which of these four sentences are provable in PA (for every choice of θ), and justify your answers by appealing, if necessary, to standard theorems which are proved in 220.

Problem x4.22. (#8 in the Fall 2003 Qual.) Let $\mathbf{Prov}(v_1, v_2)$ represent in Peano Arithmetic (PA) the set of all pairs (a, b) such that a is the Gödel number of a sentence τ and b is the Gödel number of a proof of τ from the axioms of PA. Let σ be gotten from the Fixed Point Lemma applied to $\forall v_2 \neg\mathbf{Prov}(v_1, v_2)$. In other words, let σ be a sentence such that

$$\mathsf{PA} \vdash (\sigma \leftrightarrow \forall v_2 \neg\mathbf{Prov}(\mathbf{k}, v_2),$$

where k is the Gödel number of σ. Let T be the theory gotten from PA by adding $\neg\sigma$ as an axiom. Show that T is ω-inconsistent: that is, there is a formula $\psi(v_1)$ such that $T \vdash \exists v_1 \psi(v_1)$ and $T \vdash \neg\psi(\mathbf{n})$ for each numeral $\mathbf{n}$.

Problem x4.23. True or false: if T is an inconsistent theory, then every theory is interpretable in T.

Problem x4.24. (#3 in the Fall 2004 Qual.) A *sound interpretation* of Peano arithmetic into a theory T (in any language with finite signature) is a primitive recursive function $\theta \mapsto \theta^*$ on the sentences of PA to the sentences of T which satisfies the following properties, for every sentence θ in the language of PA:

(1) If $\mathsf{PA} \vdash \theta$, then $T \vdash \theta^*$.
(2) If $T \vdash \theta^*$, then θ is true.
(3) $\Big(\neg\theta\Big)^* \equiv \neg\theta^*$.

Prove that if T is axiomatizable and there exists a sound interpretation of PA into T, then T is incomplete.

Hint. Use the Fixed Point Lemma in Peano Arithmetic.

Problem x4.25. (#8 in the Winter 2005 Qual.) A sentence in the language of PA is Π_1 if it is of the form

$$\phi \equiv (\forall x_1) \cdots (\forall x_n)\theta$$

where θ has only bounded quantifiers of the form

$$(\exists x \leq y), \qquad (\forall x \leq y).$$

Let PA be Peano arithmetic and prove that for every Π_1 sentence ϕ,

$$\mathsf{PA}, \mathrm{Con}_P(\ulcorner \phi \urcorner) \vdash \phi,$$

where $\mathrm{Con}_P(\ulcorner \phi \urcorner)$ expresses in a natural way the consistency of ϕ with Peano arithmetic, in other words it is the sentence $\neg(\exists y)\mathbf{Proof}(\ulcorner \neg\phi \urcorner, y)$.

CHAPTER 5

INTRODUCTION TO COMPUTABILITY THEORY

The class of recursive functions was originally introduced as a tool for establishing undecidability results (via the Church-Turing Thesis); but it is a very interesting class, it has been studied extensively since the 1930s, and its theory has found important applications in many mathematical areas. Here we will give only a brief introduction to some of its aspects.

5A. Semirecursive relations

It is convenient to introduce the additional notation

$$\{e\}(\vec{x}) = \varphi_e^n(\vec{x})$$

for the recursive n-ary partial function with code e, as in the Normal Form Theorem 4F.1, which puts the "program" e and the "data" $\vec{x}$ on equal footing and eliminates the need for double and triple subscripts in the formulas to follow.

We start with a Corollary to the proof of Theorem 4F.1, which gives some additional information about the coding of recursive partial functions and whose significance will become apparent in the sequel.

Theorem 5A.1 (S_n^m-Theorem, Kleene)**.** *For all $m, n \geq 1$, there is a one-to-one, $m+1$-ary primitive recursive function $S_n^m(e, y_1, \ldots, y_m)$, such that for all $\vec{y} = y_1, \ldots, y_m$, $\vec{x} = x_1, \ldots, x_n$,*

$$\varphi_{S_n^m(e,\vec{y})}(\vec{x}) = \varphi_e(\vec{y}, \vec{x}), \text{ i.e., } \{S_n^m(e, \vec{y})\}(\vec{x}) = \{e\}(\vec{y}, \vec{x}).$$

Proof. For each sequence of numbers $e, \vec{y} = e, y_1, \ldots, y_m$, let

$$\theta' \equiv \Delta e = 0 \;\&\; \Delta y_1 = 0 \;\&\; \cdots \;\&\; \Delta y_m = 0 \;\&\; 0 = 1,$$

and for each full extended formula

$$\psi \equiv \psi(\mathrm{v}_0, \ldots, \mathrm{v}_{m-1}, \mathrm{v}_m, \ldots, \mathrm{v}_{m+n})$$

(as in the definition of $T_{n+m}(e, \vec{y}, \vec{x}, z)$ in Theorem 4F.1) let

$$\theta \equiv \phi(\mathrm{v}_0, \ldots, \mathrm{v}_n) \equiv \psi(\Delta y_1, \ldots, \Delta y_m, \mathrm{v}_0, \ldots, \mathrm{v}_n)$$

and put

$$S_n^m(e, \vec{y}) = \begin{cases} \text{the code of } \theta, & \text{if } e \text{ is the code of some } \psi \text{ as above} \\ \text{the code of } \theta', & \text{otherwise.} \end{cases}$$

It is clear that each $S_n^m(e, \vec{y})$ is a primitive recursive function, and it is also one-to-one, because the value $S_n^m(e, \vec{y})$ codes all the numbers $e, y_1, \dots , y_m$—this was the reason for introducing the extra restriction on the variables in the definition of the T predicate. Moreover:

$$\begin{aligned} T_{m+n}(e, \vec{y}, \vec{x}, z) &\iff e \text{ is the code of some } \psi \text{ as above,} \\ &\qquad \text{and } (z)_1 \text{ is the code of a proof in } \mathsf{Q} \text{ of} \\ &\qquad \phi(\Delta y_1, \dots , \Delta y_m, \Delta x_1, \dots , \Delta x_n, \Delta(z)_0) \\ &\iff S_n^m(e, \vec{y}) \text{ is the code of the associated } \theta \\ &\qquad \text{and } (z)_1 \text{ is the code of a proof in } \mathsf{Q} \text{ of} \\ &\qquad \theta(\Delta x_n, \dots , \Delta x_n, \Delta(z)_0) \\ &\iff T_n(S_n^m(e, \vec{y}), \vec{x}, z). \end{aligned}$$

To see this, check first the implications in the direction $\Longrightarrow$, which are all immediate—with the crucial, middle implication holding because (literally)

$$\theta(\Delta x_1, \dots , \Delta x_n, \Delta(z)_0) \equiv \psi(\Delta y_1, \dots , \Delta y_m, \Delta x_1, \dots , \Delta x_n, \Delta(z)_0).$$

For the implications in the direction $\Longleftarrow$, notice that if $T_n(S_n^m(e, \vec{y}), \vec{x}, z)$ holds, then $S_n^m(e, \vec{y})$ is the code of a true sentence, since $(z)_0$ is the code of a proof of it in Q, and so it cannot be the code of θ', which is false; so it is the code of θ, which means that e is the code of some ϕ as above, and then the argument runs exactly as in the direction $\Longrightarrow$.

From this we get immediately, by the definitions, that

$$\{S_n^m(e, \vec{y})\}(\vec{x}) = \{e\}(\vec{y}, \vec{x}). \qquad \dashv$$

Example 5A.2. The class of recursive partial functions is "uniformly" closed for composition, for example there is a primitive recursive function $u^n(e, m_1, m_2)$ such that for all $\vec{x} = (x_1, \dots , x_n)$,

$$\{u^n(e, m_1, m_2)\}(\vec{x}) = \{e\}(\{m_1\}(\vec{x}), \{m_2\}(\vec{x})).$$

Proof. The partial function

$$f(e, m_1, m_2, \vec{x}) = \{e\}(\{m_1\}(\vec{x}), \{m_2\}(\vec{x}))$$

is recursive, and so for some number $\widehat{f}$ and by Theorem 5A.1,

$$\begin{aligned} f(e, m_1, m_2, \vec{x}) &= \{\widehat{f}\}(e, m_1, m_2, \vec{x}) \\ &= \{S_n^3(\widehat{f}, e, m_1, m_2)\}(\vec{x}), \end{aligned}$$

and it is enough to set

$$u^n(e, m_1, m_2) = S_n^3(\widehat{f}, e, m_1, m_2). \qquad \dashv$$

This is, obviously, a special case of a general fact which follows from the S_n^m-Theorem, in slogan form: *if the class of recursive partial function is closed for some operation, it is then closed uniformly* (in the codes) *for the same operation.*

To simplify the statements of several definitions and results in the sequel, we recall here and name the basic, "logical" operations on relations:

$(\neg)$	$P(\vec{x}) \iff \neg Q(\vec{x})$
$(\&)$	$P(\vec{x}) \iff Q(\vec{x})\ \&\ R(\vec{x})$
$(\vee)$	$P(\vec{x}) \iff Q(\vec{x}) \vee R(\vec{x})$
$(\Rightarrow)$	$P(\vec{x}) \iff Q(\vec{x}) \Longrightarrow R(\vec{x})$
$(\exists^{\mathbb{N}})$	$P(\vec{x}) \iff (\exists y)Q(\vec{x}, y)$
$(\exists_{\leq})$	$P(z, \vec{x}) \iff (\exists i \leq z)Q(\vec{x}, i)$
$(\forall^{\mathbb{N}})$	$P(\vec{x}) \iff (\forall y)Q(\vec{x}, y)$
$(\forall_{\leq})$	$P(z, \vec{x}) \iff (\forall i \leq z)Q(\vec{x}, i)$
(replacement)	$P(\vec{x}) \iff Q(f_1(\vec{x}), \dots, f_m(\vec{x}))$

For example, we have already shown that the class of primitive recursive relations is closed under all these operations (with primitive recursive $f_i(\vec{x})$), except for the (unbounded) quantifiers $\exists^{\mathbb{N}}, \forall^{\mathbb{N}}$, under which it is not closed by Theorem 4F.2.

Proposition 5A.3. *The class of recursive relations is closed under the propositional operations* $\neg$, $\&$, $\vee$, $\Rightarrow$, *the bounded quantifiers* $\exists_{\leq}, \forall_{\leq}$, *and substitution of* (total) *recursive functions, but it is not closed under the* (unbounded) *quantifiers* $\exists, \forall$.

Definition 5A.4. (1) A relation $P(\vec{x})$ is **semirecursive** if it is the domain of some recursive partial function $f(\vec{x})$, i.e.,

$$P(\vec{x}) \iff f(\vec{x})\downarrow .$$

(2) A relation $P(\vec{x})$ is Σ_1^0 if there is some recursive relation $Q(\vec{x}, y)$, such that

$$P(\vec{x}) \iff (\exists y)Q(\vec{x}, y).$$

Proposition 5A.5. *The following are equivalent, for an arbitrary relation* $P(\vec{x})$:

(1) $P(\vec{x})$ *is semirecursive.*

(2) $P(\vec{x})$ *is* Σ_1^0.

(3) *$P(\vec{x})$ satisfies the equivalence*

$$P(\vec{x}) \iff (\exists y)Q(\vec{x}, y)$$

with some primitive recursive $Q(\vec{x}, y)$.

Proof. (1) $\Longrightarrow$ (3) by the Normal Form Theorem; (3) $\Longrightarrow$ (2) trivially; and for (2) $\Longrightarrow$ (1) we set

$$f(\vec{x}) = \mu y Q(\vec{x}, y),$$

so that

$$(\exists y)Q(\vec{x}, y) \iff f(\vec{x})\downarrow . \qquad \dashv$$

Proposition 5A.6 (Kleene's Theorem)**.** *A relation $P(\vec{x})$ is recursive if and only if both $P(\vec{x})$ and its negation $\neg P(\vec{x})$ are semirecursive.*

Proof. If $P(\vec{x})$ is recursive, then the relations

$$Q(\vec{x}, y) \iff P(\vec{x}), \qquad R(\vec{x}, y) \iff \neg P(\vec{x})$$

are both recursive, and (trivially)

$$\begin{aligned} P(\vec{x}) &\iff (\exists y)Q(\vec{x}, y) \\ \neg P(\vec{x}) &\iff (\exists y)R(\vec{x}, y). \end{aligned}$$

For the other direction, if

$$\begin{aligned} P(\vec{x}) &\iff (\exists y)Q(\vec{x}, y) \\ \neg P(\vec{x}) &\iff (\exists y)R(\vec{x}, y) \end{aligned}$$

with recursive Q and R, then the function

$$f(\vec{x}) = \mu y[P(\vec{x}, y) \vee Q(\vec{x}, y)]$$

is total and recursive, and

$$P(\vec{x}) \iff Q(\vec{x}, f(\vec{x})). \qquad \dashv$$

Proposition 5A.7. *The class of semirecursive relations is closed under the "positive" propositional operations $\&, \vee$, under the bounded quantifiers $\exists_{\leq}$, $\forall_{\leq}$, and under the existential quantifier $\exists^{\mathbb{N}}$; it is not closed under negation $\neg$ and under the universal quantifier $\forall^{\mathbb{N}}$.*

Proof. Closure under (total) recursive substitutions is trivial, and the following transformations show the remaining positive claims of the proposition:

$$\begin{aligned}
(\exists y)Q(\vec{x},y) \vee (\exists y)R(\vec{x},y) &\iff (\exists u)[Q(\vec{x},u) \vee R(\vec{x},u)]\\
(\exists y)Q(\vec{x},y) \;\&\; (\exists y)R(\vec{x},y) &\iff (\exists u)[Q(\vec{x},(u)_0) \;\&\; R(\vec{x},(u)_1)]\\
(\exists z)(\exists y)Q(\vec{x},y,z) &\iff (\exists u)R(\vec{x},(u)_0,(u)_1)\\
(\exists i \le z)(\exists y)Q(\vec{x},y,i) &\iff (\exists y)(\exists i \le z)Q(\vec{x},y,i)\\
(\forall i \le z)(\exists y)Q(\vec{x},y,i) &\iff (\exists u)(\forall i \le z)Q(\vec{x},(u)_i,i).
\end{aligned}$$

On the other hand, the class of semirecursive relations is not closed under $\neg$ or $\forall^{\mathbb{N}}$, otherwise the basic Halting relation

$$H(e,x) \iff (\exists y)T_1(e,x,y)$$

would have a semirecursive negation and so would be recursive by 5A.6, which it is not. $\dashv$

The *graph* of a partial function $f(\vec{x})$ is the relation

(113) $$G_f(\vec{x},w) \iff f(\vec{x}) = w,$$

and the next restatement of Theorem 4E.10 often gives (with the closure properties of Σ^0_1) simple proofs of recursiveness for partial functions:

Proposition 5A.8 (The Σ^0_1-Graph Lemma). *A partial function $f(\vec{x})$ is recursive if and only if its graph $G_f(\vec{x},w)$ is a semirecursive relation.*

Proof. If $f(\vec{x})$ is recursive with code $\widehat{f}$, then

$$G_f(\vec{x},w) \iff (\exists y)[T_n(\widehat{f},\vec{x},y) \;\&\; U(y) = w],$$

so that $G_f(\vec{x},w)$ is semirecursive; and if

$$f(\vec{x}) = w \iff (\exists u)R(\vec{x},w,u)$$

with some recursive $R(\vec{x},w,u)$, then

$$f(\vec{x}) = \Big(\mu u R(\vec{x},(u)_0,(u)_1)\Big)_0,$$

so that $f(\vec{x})$ is recursive. $\dashv$

The next Lemma is also very simple, but it simplifies many proofs.

Proposition 5A.9 (The Σ^0_1-Selection Lemma). *For each semirecursive relation $R(\vec{x},w)$, there is a recursive partial function*

$$f(\vec{x}) = \nu w R(\vec{x},w)$$

such that for all $\vec{x}$,

$$\begin{aligned}
(\exists w)R(\vec{x},w) &\iff f(\vec{x})\downarrow\\
(\exists w)R(\vec{x},w) &\implies R(\vec{x},f(\vec{x})).
\end{aligned}$$

Proof. By the hypothesis, there is a recursive relation $P(\vec{x}, w, y)$ such that

$$R(\vec{x}, w) \iff (\exists y)P(\vec{x}, w, y),$$

and the conclusion of the lemma follows if we just set

$$f(\vec{x}) = \Big(\mu u P(\vec{x}, (u)_0, (u)_1)\Big)_0. \qquad \dashv$$

5B. Recursively enumerable sets

Some of the properties of semirecursive relations are easier to identify when we view unary relations as sets:

Definition 5B.1 (R.e. sets)**.** A set $A \subseteq \mathbb{N}$ is **recursively** or **computably enumerable** if either $A = \emptyset$, or some total, recursive function enumerates it, i.e.,

$$A = \{f(0), f(1), \dots, \}. \tag{114}$$

The term “recursively enumerable” is unwieldy and it is always abbreviated by the initials “r.e.” or ”c.e.”.

Proposition 5B.2. *The following are equivalent for any $A \subseteq \mathbb{N}$:*

(1) *A is r.e.*

(2) *The relation $x \in A$ is semirecursive.*

(3) *A is finite, or there exists a one-to-one recursive function $f : \mathbb{N} \rightarrowtail \mathbb{N}$ which enumerates it.*

Proof. The implication (3) $\Longrightarrow$ (1) is trivial, and (1) $\Longrightarrow$ (2) follows from the equivalence

$$x \in A \iff (\exists n)[f(n) = x]$$

which holds for all non-empty r.e. sets A. To show (2) $\Longrightarrow$ (3), we suppose that A is infinite and

$$x \in A \iff (\exists y)R(x, y)$$

with a recursive $R(x, y)$, and set

$$B = \{u \mid R((u)_0, (u)_1) \ \& \ (\forall v < u)[R((v)_0, (v)_1) \Longrightarrow (v)_0 \neq (u)_0]\}.$$

It is clear that B is a recursive set, that

$$u \in B \Longrightarrow (u)_0 \in A,$$

and that if $x \in A$ and we let

$$t = (\mu u)[R((u)_0, (u)_1) \ \& \ (u)_0 = x],$$

then (directly from the definition of B),

$$t \in B \ \& \ (\forall u)[(u \in B \ \& \ (u)_0 = x) \iff u = t];$$

it follows that the projection

$$\pi(u) = (u)_0$$

is a one-to-one correspondence of B with A, and hence B is infinite. Now B is enumerated without repetitions by the recursive function

$$\begin{aligned} g(0) &= (\mu u)[u \in B] \\ g(n+1) &= (\mu u)[u > g(n) \ \& \ u \in B], \end{aligned}$$

and the composition

$$f(n) = (g(n))_0$$

enumerates A without repetitions. ⊣

The next fact shows that we cannot go any further in producing "nice" enumerations of arbitrary r.e. sets.

Proposition 5B.3. *A set $A \subseteq \mathbb{N}$ is recursive if and only if it is finite, or there exists an increasing, total recursive function which enumerates it,*

$$A = \{f(0) < f(1) < \dots, \}.$$

Proof. A function $f : \mathbb{N} \to \mathbb{N}$ is *increasing* if

$$f(n) < f(n+1) \qquad (n \in \mathbb{N}),$$

from which it follows (by an easy induction) that for all n

$$n \le f(n);$$

thus, if some increasing, recursive f enumerates A, then

$$x \in A \iff (\exists n \le x)[x = f(n)],$$

and A is recursive. For the opposite direction, if A is recursive and infinite, then the function

$$\begin{aligned} f(0) &= (\mu x)[x \in A] \\ f(n+1) &= (\mu x)[x > f(n) \ \& \ x \in A] \end{aligned}$$

is recursive, increasing and enumerates A. ⊣

The simplest example of an r.e. non-recursive set is the "diagonal" set

(115) $$K = \{x \mid (\exists y)T_1(x, x, y)\} = \{x \mid \{x\}(x)\!\downarrow\},$$

and the next Proposition shows that (in some sense) K is the "most complex" r.e. set.

Proposition 5B.4. *For each r.e. set A, there is a one-to-one recursive function $f : \mathbb{N} \rightarrowtail \mathbb{N}$ such that*

$$x \in A \iff f(x) \in K. \tag{116}$$

PROOF. By hypothesis, $A = \{x \mid g(x)\downarrow\}$ for some recursive partial function $g(x)$. We set

$$h(x, y) = g(x)$$

and we choose some code $\widehat{h}$ of h, so that for any y,

$$\begin{aligned} x \in A &\iff h(x,y)\downarrow \\ &\iff \{\widehat{h}\}(x,y)\downarrow \\ &\iff \{S^1_1(\widehat{h},x)\}(y)\downarrow; \end{aligned}$$

in particular, this holds for $y = S^1_1(\widehat{h}, x)$ and it yields in that case

$$\begin{aligned} x \in A &\iff \{S^1_1(\widehat{h},x)\}(S^1_1(\widehat{h},x))\downarrow \\ &\iff S^1_1(\widehat{h},x) \in K, \end{aligned}$$

so that (116) holds with $f(x) = S^1_1(\widehat{h}, x)$. ⊣

Definition 5B.5 (Reducibilities)**.** A **reduction** of a set A to another set B is any (total) recursive function f, such that

$$x \in A \iff f(x) \in B, \tag{117}$$

and we set:

$$\begin{aligned} A \leq_m B &\iff \text{there exists a reduction of } A \text{ to } B, \\ A \leq_1 B &\iff \text{there exists a one-to-one reduction of } A \text{ to } B, \\ A \equiv B &\iff \text{there exists a reduction } f \text{ of } A \text{ to } B \\ &\qquad \text{which is a permutation,} \end{aligned}$$

where a permutation $f : \mathbb{N} \rightarrowtail\!\!\!\!\rightarrow \mathbb{N}$ is any one-to-one correspondence of $\mathbb{N}$ onto $\mathbb{N}$. Clearly

$$A \equiv B \Longrightarrow A \leq_1 B \Longrightarrow A \leq_m B.$$

Proposition 5B.6. *For all sets A, B, C,*

$$A \leq_m A \textit{ and } [A \leq_m B \;\&\; B \leq_m C] \Longrightarrow A \leq_m C,$$

and the same holds for the stronger reductions $\leq_1$ and $\equiv$; in addition, the relation $\equiv$ of recursive isomorphism is symmetric,

$$A \equiv B \iff B \equiv A.$$

Definition 5B.7. A set B is **r.e. complete** if it is r.e., and every r.e. set A is one-one reducible to B, $A \leq_1 B$.

Proposition 5B.4 expresses precisely the r.e. completeness of K, and the next, basic result shows that up to recursive isomorphism, there is only one r.e. complete set.

Theorem 5B.8 (John Myhill)**.** *For any two sets A and B,*

$$A \leq_1 B \;\&\; B \leq_1 A \Longrightarrow A \equiv B.$$

Proof. The argument is s constructive version of the classical Schröder-Bernstein in set theory, and it is based on the next Lemma, in which a sequence of pairs

$$W = (x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n) \tag{118}$$

is called *good* (as an approximation to an isomorphism) for A and B if

$$i \neq j \Longrightarrow [x_i \neq x_j \text{ and } y_i \neq y_j], \qquad x_i \in A \iff y_i \in B \qquad (i \leq n).$$

For any good sequence, we set

$$X = \{x_0, x_1, \ldots, x_n\}, \quad Y = \{y_0, y_1, \ldots, y_n\}.$$

Lemma X. *If there is a recursive one-to-one function $f : \mathbb{N} \rightarrowtail \mathbb{N}$ such that*

$$x \in A \iff f(x) \in B,$$

then for every good sequence (118) *and each $x \notin X$, we can find some $y \notin Y$ such that the extension*

$$W' = (x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n), (x, y) \tag{119}$$

is also good, i.e.,

$$x \in A \iff y \in B,$$

Prof of Lemma X. We set

$$z_0 = f(x)$$
$$z_{i+1} = \begin{cases} z_i & \text{if } z_i \notin Y, \\ f(x_j) & \text{otherwise, if } z_i = y_j, \end{cases}$$

and we verify two basic properties of the sequence $z_0, z_1, \ldots$.

(1) For each i, $x \in A \iff z_i \in B$.

Proof. For $i = 0$, $x \in A \iff f(x) = z_0 \in B$, by the hypothesis on f. Inductively, if $z_i \notin Y$, then

$$x \in A \iff z_{i+1} = z_i \in B$$

by the induction hypothesis, and if $z_i \in Y$, then

$$\begin{aligned} x \in A &\iff z_i = y_j \in B && \text{(by the induction hypothesis)}\\ &\iff x_j \in A && \text{(because the given sequence is good)}\\ &\iff f(x_j) = z_{i+1} \in B. \end{aligned}$$

(2) For every i, $z_i \in Y \Longrightarrow (\forall k < i)[z_i \neq z_k]$.

Proof. The proposition is trivially true if $z_0 = f(x) \notin Y$, since, in this case, $z_i = f(x) \notin Y$ for every i, by the definition. The proposition is also trivially true for $i = 0$, and, inductively, we assume that it holds for i and that $z_{i+1} \in Y$. Notice that $z_i \in Y$, otherwise (by the definition) $z_{i+1} = z_i \notin Y$; hence, by the definition again, for some j,

$$z_i = y_j, \quad z_{i+1} = f(x_j). \tag{120}$$

Towards a contradiction, let k be the least counterexample for z_{i+1}, i.e.,

$$z_{i+1} = z_k \ \& \ (\forall l < k)[z_{i+1} \neq z_l].$$

Notice that $k \neq 0$, since $z_0 = f(x)$, $z_{i+1} = f(x_j)$, and hence,

$$z_{i+1} = z_0 \Longrightarrow f(x_j) = f(x) \Longrightarrow x_j = x,$$

which is absurd, since $x \notin X$ while $x_j \in X$; hence $k = t+1$ for some $t < i$, and by the selection of k, $z_t \in Y$ (otherwise $z_{t+1} = z_t$ and $t+1$ would not be a counterexample), and hence, for some s,

$$z_t = y_s, \quad z_{t+1} = f(x_s). \tag{121}$$

We compute:

$$\begin{aligned} z_{i+1} = z_{t+1} &\Longrightarrow f(x_j) = f(x_s) && \text{(from (120) and (121))}\\ &\Longrightarrow x_j = x_s && \text{(because } f \text{ is one-to-one)}\\ &\Longrightarrow y_j = y_s && \text{(because the sequence is good)}\\ &\Longrightarrow z_i = z_t && \text{(by (120) and (121)).} \end{aligned}$$

It follows from the inductive hypothesis that $t \geq i$, hence $t+1 \geq i+1$, and this contradicts the assumption $t+1 < i+1$.

Now (2) implies that for some $j < n+2$, $z_j \notin Y$ (since Y has $n+1$ members), and the Lemma holds if we choose $y = z_j$, $W' = W, (x, y)$. ⊣ (Lemma X)

The symmetric Lemma Y gives us for each good sequence W and each $y \notin Y$ some $x \notin X$ such that the extension (119) $W' = W, (x, y)$ is good, and the construction of the required recursive permutation proceeds by successive application of these two Lemmas starting with the good sequence

$$W_0 = \langle 0, f(0) \rangle, \quad X_0 = \{0\}, Y_0 = \{f(0)\}.$$

Odd step $2n+1$. Let $y = \min(\mathbb{N} \setminus Y_{2n})$ and extend W_{2n} by applying Lemma Y, so that $y \in Y_{2n+1}$.

Even step $2n+2$. Let $x = \min(\mathbb{N} \setminus X_{2n+1})$ and extend W_{2n+1} by applying Lemma X so that $x \in X_{2n+2}$.

In the end, the union $\bigcup_n W_n$ is the graph of a permutation $h : \mathbb{N} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbb{N}$ which reduces A to B,

$$x \in A \iff h(x) \in B.$$

The recursiveness of h follows from the construction and completes the proof that $A \equiv B$. ⊣

Definition 5B.9 (Codes for r.e. sets)**.** For each $e \in \mathbb{N}$, let

$$W_e = \{x \mid \phi_e(x)\downarrow\},$$

so that the relation $x \in W_e$ is semirecursive and the sequence

$$W_0, W_1, \dots$$

enumerates all the r.e. sets.

Proposition 5B.10. *If $A \le_m B$ and B is recursive, then A is also recursive; hence, if $A \le_m B$ and A is not recursive, then B is not recursive either.*

With the r.e. completeness of K, this simple fact is the basic tool for proving non-recursiveness for sets and relations: because if we verify that $K \le_m B$, then B is not recursive.

Example 5B.11. The set

$$A = \{e \mid W_e \neq \emptyset\}$$

is r.e. but not recursive.

Proof. The set A is r.e. because the relation

$$e \in A \iff (\exists x)[x \in W_e]$$

is Σ^0_1. To show that $K \le_m A$, we let

$$g(e, x) = \mu y T_1(e, e, y),$$

so that the value $g(e, x)$ is independent of x, i.e.,

$$g(e,x) = \begin{cases} \mu y T_1(e,e,y) & \text{if } (\exists y) T_1(e,e,y) \\ \text{undefined} & \text{otherwise.} \end{cases}$$

It follows that for all e and x,

$$e \in K \iff g(e,x)\downarrow,$$

so that

$$e \in K \iff (\exists x) g(e,x)\downarrow;$$

and so, if $\widehat{g}$ is any code of $g(x, y)$,

$$\begin{aligned} e \in K &\iff (\exists x)[\{\widehat{g}\}(e, x)\downarrow] \\ &\iff (\exists x)[\{S^1_1(\widehat{g}, e)\}(x)\downarrow] \\ &\iff W_{S^1_1(\widehat{g},e)} \neq \emptyset \\ &\iff S^1_1(\widehat{g}, e) \in A, \end{aligned}$$

so that $K \leq_1 A$ and A is not recursive. ⊣

Notice that with this construction,

$$\begin{aligned} e \in K &\iff W_{S^1_1(\widehat{g},e)} = \mathbb{N} \\ &\iff W_{S^1_1(\widehat{g},e)} \text{ has at least 2 members,} \end{aligned}$$

so that the sets

$$B = \{e \mid W_e = \mathbb{N}\}, \quad C = \{e \mid W_e \text{ has at least 2 members}\}$$

are also not recursive.

5C. Productive, creative and simple sets

Up until now, the only r.e non-recursive sets we have seen are r.e. complete, and the question arises whether that is all there is. The next sequence of definitions and results (due to Emil Post) shows that this simplistic picture of the class of r.e. sets is far from the truth.

Definition 5C.1. A function $p : \mathbb{N} \rightarrowtail \mathbb{N}$ is a **productive function** for a set B if it is recursive, one-to-one, and such that

$$W_e \subseteq B \Longrightarrow p(e) \in B \setminus W_e;$$

and a set B is **productive** if it has a productive function.

A set A is **creative** if it is r.e. and its complement

$$A^c = \{x \in \mathbb{N} \mid x \notin A\}$$

is productive.

Proposition 5C.2. *The complete set K is creative, with productive function for its complement the identity $p(e) = e$.*

Proof. We must show that

$$W_e \subseteq K^c \Longrightarrow e \in K^c \setminus W_e,$$

i.e.,

$$(\forall t)[t \in W_e \Longrightarrow t \notin K] \Longrightarrow [e \notin W_e \ \& \ e \notin K].$$

Spelling out the hypothesis of the required implication:

$$(\forall t)[\{e\}(t)\downarrow \ \Longrightarrow \{t\}(t)\uparrow];$$

and the conclusion simply says that

$$\{e\}(e)\uparrow,$$

because

$$e \notin W_e \iff e \notin K \iff \{e\}(e)\uparrow .$$

Finally, the hypothesis implies the conclusion because if $\{e\}(e)\downarrow$, then, setting $t = e$ in the hypothesis we get $\{e\}(e)\uparrow$, which is contradictory. ⊣

Corollary 5C.3. *Every r.e. complete is creative.*

Proof. It is enough to show that if A is productive and $A \leq_1 B$, then B is also productive, and then apply this to the complement X^c of the given, r.e. complete set X for which we have $K^c \leq_1 X^c$ (because $K \leq_1 X$). So suppose that

$$x \in A \iff f(x) \in B$$

with $f(x)$ recursive and 1 - 1, and that $p(e)$ is a productive function for A. Choose $u(e)$ (by appealing to the S^m_n-Theorem) such that it is recursive, 1 - 1, and for each e,

$$W_{u(e)} = f^{-1}[W_e],$$

and let

$$q(e) = f(p(u(e))).$$

To verify that $q(e)$ is a productive function for B, we compute:

$$\begin{aligned} W_e \subseteq B &\Longrightarrow W_{u(e)} = f^{-1}[W_e] \subseteq A \\ &\Longrightarrow p(u(e)) \in A \setminus f^{-1}[W_e] \\ &\Longrightarrow q(e) = f(p(u(e))) \in B \setminus W_e. \end{aligned}$$

⊣

Proposition 5C.4. *Every productive set B has an infinite r.e. subset.*

Proof. The idea is to define a function $f : \mathbb{N} \to \mathbb{N}$ by the recursion

$$\begin{aligned} f(0) &= e_0, \text{ where } W_{e_0} = \emptyset \\ f(x+1) &= \text{some code of } W_{f(x)} \cup \{p(f(x))\}, \end{aligned}$$

where $p(e)$ is a given productive function for B. If we manage this, then a simple induction will show that, for every x,

$$W_{f(x)} \subsetneq W_{f(x+1)} \subseteq B,$$

so that the set

$$A = W_{f(0)} \cup W_{f(1)} \cup \ldots = \{y \mid (\exists x)[y \in W_{f(x)}\}$$

is an infinite, r.e. subset of B. For the computation of the required function $h(w, x)$ such that

$$f(x+1) = h(f(x), x),$$

let first

$$R(e,y,x) \iff x \in W_e \vee x = y$$

and notice that this is a semirecursive relation, so that for some $\widehat{g}$,

$$\begin{aligned} x \in W_e \cup \{y\} &\iff \{\widehat{g}\}(e,y,x)\downarrow \\ &\iff \{S^2_1(\widehat{g},e,y)\}(x)\downarrow . \end{aligned}$$

This means that if we set

$$u(e,y) = S^2_1(\widehat{g},e,y),$$

then

$$W_{u(e,y)} = W_e \cup \{y\}.$$

Finally, set

$$h(w,x) = u(w,p(w)),$$

and in the definition of f,

$$f(x+1) = h(f(x),x) = u(f(x),p(f(x))),$$

so that

$$W_{f(x+1)} = W_{f(x)} \cup \{p(f(x))\}$$

as required. ⊣

Definition 5C.5. A set A is **simple** if it is r.e., and its complement A^c is infinite and has no infinite r.e. subset, i.e.,

$$W_e \cap A = \emptyset \Longrightarrow W_e \text{ is finite.}$$

Theorem 5C.6 (Emil Post)**.** *There exists a simple set.*

Proof. The relation

$$R(x,y) \iff y \in W_x \ \&\ y > 2x$$

is semirecursive, so that by the Σ^0_1-Selection Lemma 5A.9, there is a recursive partial function $f(x)$ such that

$$\begin{aligned} (\exists y)[y \in W_x \ \&\ y > 2x] &\iff f(x)\downarrow \\ &\iff f(x)\downarrow \ \&\ f(x) \in W_x \ \&\ f(x) > 2x. \end{aligned}$$

The required set is the image of f,

$$\begin{aligned} A &= \{f(x) \mid f(x)\downarrow\} \\ &= \{y \mid (\exists x)[f(x) = y]\} \\ &= \{y \mid (\exists x)[f(x) = y \ \&\ 2x < y]\}, \end{aligned} \tag{122}$$

where the last, basic equality follows from the definition of the relation $R(x,y)$.

(1) A is r.e., from its definition, because the graph of $f(x)$ is Σ^0_1.

(2) The complement A^c of A is infinite, because

$$\begin{aligned} y \in A \ \&\ y \le 2z &\implies (\exists x)[y = f(x) \ \&\ 2x < y \le 2z] \\ &\implies (\exists x)[y = f(x) \ \&\ x < z], \end{aligned}$$

so that *at most* z *of the* $2z+1$ *numbers* $\le 2z$ *belong to* A; it follows that some $y \ge z$ belongs to the complement A^c, and since this holds for every z, the set A^c is infinite.

(3) For every infinite W_e, $W_e \cap A \neq \emptyset$, because

$$\begin{aligned} W_e \text{ is infinite} &\implies (\exists y)[y \in W_e \ \&\ y > 2e] \\ &\implies f(e)\downarrow \ \ \&\ f(e) \in W_e \\ &\implies f(e) \in W_e \cap A. \end{aligned} \qquad \dashv$$

Corollary 5C.7. *Simple sets are neither recursive nor r.e. complete, and so there exists an r.e., non-recursive set which is not r.e. complete.*

Proof. A simple set cannot be recursive, because its (infinite, by definition) complement is a witness against its simplicity; and it cannot be r.e. complete, because it is not creative by Proposition 5C.4. $\dashv$

5D. The Second Recursion Theorem

In this section we will prove a very simple result of Kleene, which has surprisingly strong and unexpected consequences in many parts of definability theory, and even in analysis and set theory. Here we will prove just one, substantial application of the Second Recursion Theorem, but we will also use it later in the theory of *recursive functionals* and *effective operations*.

Theorem 5D.1 (Kleene)**.** *For each recursive partial function* $f(z, \vec{x})$*, there is a number* z^**, such that for all* $\vec{x}$*,*

$$\varphi_{z^*}(\vec{x}) = \{z^*\}(\vec{x}) = f(z^*, \vec{x}). \tag{123}$$

In fact, for each n*, there is a primitive recursive function* $h_n(e)$*, such that if* $f = \varphi_e^{n+1}$*, is* $n+1$*-ary, then equation* (123) *holds with* $z^* = h_n(e)$*, i.e.,*

$$\varphi_{h_n(e)}(\vec{x}) = \{h_n(e)\}(\vec{x}) = \varphi_e(h_n(e), \vec{x}). \tag{124}$$

The theorem gives immediately several simple propositions which show that the coding of recursive partial functions has many unexpected (and even weird) properties.

Example 5D.2. There exist numbers $z_1 - z_4$, such that

$$\begin{aligned}\varphi_{z_1}(x) &= z_1\\ \varphi_{z_2}(x) &= z_2 + x\\ W_{z_3} &= \{z_3\}\\ W_{z_4} &= \{0, \ldots, z_4\}.\end{aligned}$$

Proof. For z_1, we apply the Second Recursion Theorem to the function

$$f(z, x) = z$$

and we set $z_1 = z^*$; it follows that

$$\varphi_{z_1}(x) = f(z_1, x) = z_1.$$

The rest are similar and equally easy. ⊣

Proof of the Second Recursion Theorem 5D.1. The partial function

$$g(z, \vec{x}) = f(S^1_n(z, z), \vec{x})$$

is recursive, and so there some number $\widehat{g}$ such that

$$\{S^1_n(\widehat{g}, z)\}(\vec{x}) = \{\widehat{g}\}(z, \vec{x}) = f(S^1_n(z, z), \vec{x});$$

the result follows from this equation if we set

$$z^* = S^1_n(\widehat{g}, \widehat{g}).$$

For the stronger (uniform) version (124), let d be a number such that

$$\varphi_d(e, z, \vec{x}) = \varphi_e(S^1_n(z, z), \vec{x});$$

it follows that

$$\widehat{g} = S^1_{n+1}(d, e)$$

is a code of $\varphi_e(S^1_n(z, z), \vec{x})$, and the required function is

$$h(e) = S^1_n(\widehat{g}, \widehat{g}) = S^1_n(S^1_{n+1}(d, e), S^1_{n+1}(d, e)).$$ ⊣

For a (much more significant) example of the strength of the Second Recursion Theorem, we show here the converse of 5C.3, that every creative set is r.e. complete (and a bit more).

Theorem 5D.3 (John Myhill)**.** *The following are equivalent for every r.e. set A.*

(1) *There is a recursive partial function $p(e)$ such that*

$$W_e \cap A = \emptyset \Longrightarrow [p(e)\downarrow \ \& \ p(e) \in A^c \setminus W_e].$$

(2) *There is a total recursive function $q(e)$ such that*

$$W_e \cap A = \emptyset \Longrightarrow q(e) \in A^c \setminus W_e. \tag{125}$$

(3) *A is creative, i.e.,* (125) *holds with a one-to-one recursive function* $q(e)$.

(4) *A is r.e. complete.*

In particular, an r.e. set is complete if and only if it is creative.

Proof. (1) $\Rightarrow$ (2). For the given, recursive partial function $p(e)$, there exists (by the Second Recursion Theorem) some number z such that

$$\{S^1_1(z,e)\}(t) = \varphi_z(e,t) = \begin{cases} \varphi_e(t), & \text{if } p(S^1_1(z,e))\downarrow, \\ \uparrow, & \text{otherwise.} \end{cases}$$

We set $q(e) = p(S^1_1(z,e))$ with this z, and we observe that $q(e)$ is a total function, because

$$\begin{aligned} q(e) = p(S^1_1(z,e))\uparrow &\Longrightarrow W_{S^1_1(z,e)} = \emptyset \text{ by the definition} \\ &\Longrightarrow p(S^1_1(z,e))\downarrow . \end{aligned}$$

In addition, since $q(e)\downarrow$, $W_{S^1_1(z,e)} = W_e$, and hence

$$W_e \cap A = \emptyset \Longrightarrow q(e) = p(S^1_1(z,e)) \in A^c \setminus W_{S^1_1(z,e)} = A^c \setminus W_e$$

which is what we needed to show.

(2) $\Rightarrow$ (3) (This implication does not use the Second recursion Theorem, and could have been given in Section 5A.) For the given $q(e)$ which satisfies (125), we observe first that there is a recursive partial function $h(e)$ such that

$$W_{h(e)} = W_e \cup \{q(e)\};$$

and then we set, by primitive recursion,

$$\begin{aligned} g(0,e) &= e \\ g(i+1,e) &= h(g(i,e)), \end{aligned}$$

so that (easily, by induction on i),

$$W_{g(i+1,e)} = W_e \cup \{q(g(0,e)), q(g(1,e)), \dots , q(g(i,e))\}.$$

It follows that for each $i > 0$,

$$\begin{aligned} (126) \quad & W_e \cap A = \emptyset \\ & \Longrightarrow q(g(i,e)) \in A^c \setminus (W_e \cup \{q(g(0,e)), q(g(1,e)), \dots , q(g(i-1,e))\}), \end{aligned}$$

and, more specifically,

$$(127) \qquad W_e \cap A = \emptyset \Longrightarrow (\forall j < i)[q(g(i,e)) \neq q(g(j,e))].$$

Finally, we set

$$f(0) = q(0),$$

and for the (recursive) definition of $f(e+1)$, we compute first, in sequence, the values $q(g(0,e+1)), \dots , q(g(e+1,e+1))$ and we distinguish two cases.

Case 1. If these values are all distinct, then one of them is different from the values $f(0), \dots, f(e)$, and we just set

$$\begin{aligned} j &= (\mu i \le (e+1))(\forall y \le e)[q(g(i, e+1)) \neq f(y)] \\ f(e+1) &= q(g(j, e+1)). \end{aligned}$$

Case 2. There exist $i, j \le e+1$, $i \neq j$, such that $q(g(i, e+1)) = q(g(j, e+1))$. In this case we set

$$f(e+1) = \max\{f(0), \dots, f(e)\} + 1.$$

It is clear that $f(e)$ is recursive and one-to-one, and that it is a productive function for A^c follows immediately from (127) and (126).

(3) $\Rightarrow$ (4). If $q(e)$ is a productive function for the complement A^c and B is any r.e. set, then (by the Second Recursion Theorem) there is some number z such that

$$\varphi_z(x, t) = \begin{cases} 1 & \text{if } x \in B \ \&\ t = q(S^1_1(z, x)) \\ \uparrow & \text{otherwise;} \end{cases}$$

the function

$$f(x) = q(S^1_1(z, x))$$

is one-to-one (as a composition of one-to-one functions), and it reduces B to A, as follows.

If $x \in B$, then $W_{S^1_1(z,x)} = \{q(S^1_1(z, x)\} = \{f(x)\}$, and

$$\begin{aligned} f(x) \notin A &\Longrightarrow W_{S^1_1(z,x)} \cap A = \emptyset \\ &\Longrightarrow q(S^1_1(z, x)) \in A^c \setminus W_{S^1_1(z,x)} \\ &\Longrightarrow f(x) \in A^c \setminus \{f(x)\}, \end{aligned}$$

which is a contradiction; hence $f(x) \in A$. On the other hand, if $x \notin B$, then $W_{S^1_1(z,x)} = \emptyset \subseteq A^c$, hence $f(x) = q(S^1_1(z, x)) \in A^c$. $\dashv$

5E. The arithmetical hierarchy

The semirecursive (Σ^0_1) relations are of the form

$$(\exists y)Q(\vec{x}, y)$$

where $Q(\vec{x}, y)$ is recursive, and so they are just one *existential quantifier* "away" from the recursive relations in complexity. The next definition gives us a useful tool for the classification of complex, undecidable relations.

Definition 5E.1. The classes (sets) of relations Σ^0_k, Π^0_k, Δ^0_k are defined recursively, as follows:

$$\begin{aligned}
\Sigma^0_1 &: \text{the semirecursive relations}\\
\Pi^0_k = \neg\Sigma^0_k &: \text{the negations (complements) of relations in } \Sigma^0_k\\
\Sigma^0_{k+1} = \exists^{\mathbb{N}}\Pi^0_k &: \text{the relations which satisfy an equivalence}\\
&\quad P(\vec{x}) \iff (\exists y)Q(\vec{x}, y), \text{where } Q(\vec{x}, y) \text{ is } \Pi^0_k\\
\Delta^0_k = \Sigma^0_k \cap \Pi^0_k &: \text{ the relations which are both } \Sigma^0_k \text{ and } \Pi^0_k.
\end{aligned}$$

A set A is in one of these classes Γ if the relation $x \in A$ is in Γ.

5E.2. Canonical forms. These classes of the *arithmetical hierarchy* are (obviously) characterized by the following "canonical forms", in the sense that a given relation $P(\vec{x})$ is in a class Γ if it is equivalent with the canonical form for Γ, with some recursive Q:

$$\begin{array}{lcr}
\Sigma^0_1 & : & (\exists y)Q(\vec{x}, y)\\
\Pi^0_1 & : & (\forall y)Q(\vec{x}, y)\\
\Sigma^0_2 & : & (\exists y_1)(\forall y_2)Q(\vec{x}, y_1, y_2)\\
\Pi^0_2 & : & (\forall y_1)(\exists y_2)Q(\vec{x}, y_1, y_2)\\
\Sigma^0_3 & : & (\exists y_1)(\forall y_2)(\exists y_3)Q(\vec{x}, y_1, y_2, y_3)\\
 & \vdots &
\end{array}$$

A trivial corollary of these canonical forms is that:

Proposition 5E.3. *The relations which belong to some Σ^0_k or some Π^0_k are precisely the arithmetical relations.*

Proof. Each primitive recursive relation is arithmetical, by Theorem 4B.13 and Lemma 4B.2, and then (inductively) every Σ^0_k and every Π^0_k relation is arithmetical, because the class of arithmetical relations is closed under negation and quantification on $\mathbb{N}$. For the other direction, we notice that relations defined by quantifier-free formulas are (trivially) recursive, and that every arithmetical relation is defined by some formula in prenex form with quantifier-free matrix; and by introducing dummy quantifiers, if necessary, we may assume that the quantifiers in the prefix are alternating and start with an $\exists$, so that the relation defined by each formula is in some Σ^0_k. ⊣

Theorem 5E.4. (1) *For each $k \geq 1$, the classes Σ^0_k, Π^0_k, and Δ^0_k are closed for (total) recursive substitutions and for the operations &, $\vee$, $\exists_\leq$ and $\forall_\leq$. In addition*:

- *Each Δ^0_k is closed for negation $\neg$.*
- *Each Σ^0_k is closed for $\exists^{\mathbb{N}}$, existential quantification over $\mathbb{N}$.*

- *Each* Π^0_k *is closed for* $\forall^{\mathbb{N}}$, *universal quantification over* $\mathbb{N}$.

(2) *For each* $k \geq 1$,

$$\Sigma^0_k \subseteq \Delta^0_{k+1}, \tag{128}$$

and hence the arithmetical classes satisfy the following diagram of inclusions:

$$\begin{array}{ccccccccccccc}
 & & \Sigma^0_1 & & & & \Sigma^0_2 & & & & \Sigma^0_3 & & \\
 & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & \\
\Delta^0_1 & & & & \Delta^0_2 & & & & \Delta^0_3 & & & & \cdots \\
 & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & \\
 & & \Pi^0_1 & & & & \Pi^0_2 & & & & \Pi^0_3 & &
\end{array}$$

Proof. First we verify the closure of all the arithmetical classes for recursive substitutions, by induction on k; the proposition is known for $k = 1$ by 5A.7, and (inductively), for the case of Σ^0_{k+1}, we compute:

$$\begin{aligned}
P(\vec{x}) &\iff R(f_1(\vec{x}), \dots, f_n(\vec{x})) \\
&\iff (\exists y)Q(f_1(\vec{x}), \dots, f_n(\vec{x}), y) \\
&\qquad \text{where } Q \in \Pi^0_k, \text{ by definition} \\
&\iff (\exists y)Q'(\vec{x}, y) \\
&\qquad \text{where } Q' \in \Pi^0_k \text{ by the induction hypothesis.}
\end{aligned}$$

The remaining parts of (1) are shown directly (with no induction) using the transformations in the proof of 5A.7.

We show (2) by induction on k, where, in the basis, if

$$P(\vec{x}) \iff (\exists y)Q(\vec{x}, y)$$

with a recursive Q, then P is surely Σ^0_2, since each recursive relation is Π^0_1; but a semirecursive relation is also Π^0_2, since, obviously,

$$P(\vec{x}) \iff (\forall z)(\exists y)Q(\vec{x}, y)$$

and the relation

$$Q_1(\vec{x}, z, y) \iff Q(\vec{x}, y)$$

is recursive. The induction step of the proof is practically identical, and the inclusions in the diagram follow easily from (128) and simple computations. ⊣

More interesting is the next theorem which justifies the appellation "hierarchy" for the classes Σ^0_k, Π^0_k:

Theorem 5E.5 (Kleene).

(1) (Enumeration for Σ^0_k) *For each $k \geq 1$ and each $n \geq 1$, there is an $n+1$-ary relation $\widetilde{S}^0_{k,n}(e, \vec{x})$ in the class Σ^0_k which enumerates all the n-ary, Σ^0_k relations, i.e., $P(\vec{x})$ is Σ^0_k if and only if for some e,*

$$P(\vec{x}) \iff \widetilde{S}^0_{k,n}(e, \vec{x}).$$

(2) (Enumeration for Π^0_k) *For each $k \geq 1$ and each $n \geq 1$, there is an $n+1$-ary relation $\widetilde{P}^0_{k,n}(e, \vec{x})$ in Π^0_k which enumerates all the n-ary, Π^0_k relations, i.e., $P(\vec{x})$ is Π^0_k if and only if, for some e,*

$$P(\vec{x}) \iff \widetilde{P}^0_{k,n}(e, \vec{x}).$$

(3) (Hierarchy Theorem) *The inclusions in the Diagram of Proposition* 5E.4 *are all strict, i.e.,*

$$\begin{array}{ccccccccccccc}
 & & \Sigma^0_1 & & & & \Sigma^0_2 & & & & \Sigma^0_3 & & \\
 & \subsetneq & & \supsetneq & & \subsetneq & & \supsetneq & & \subsetneq & & \supsetneq & \\
\Delta^0_1 & & & & \Delta^0_2 & & & & \Delta^0_3 & & & & \cdots \\
 & \supsetneq & & \subsetneq & & \supsetneq & & \subsetneq & & \supsetneq & & \subsetneq & \\
 & & \Pi^0_1 & & & & \Pi^0_2 & & & & \Pi^0_3 & &
\end{array}$$

Proof. For (1) and (2) we set, recursively,

$$\begin{aligned}
\widetilde{S}^0_{1,n}(e, \vec{x}) &\iff (\exists y) T_n(e, \vec{x}, y) \\
\widetilde{P}^0_{k,n}(e, \vec{x}) &\iff \neg \widetilde{S}^0_{k,n}(e, \vec{x}) \\
\widetilde{S}^0_{k+1,n}(e, \vec{x}) &\iff (\exists y) \widetilde{P}^0_{k,n+1}(e, \vec{x}, y),
\end{aligned}$$

and the proofs are easy, with induction on k. For (3), we observe that the "diagonal" relation

$$D_k(x) \iff \widetilde{S}^0_{k,1}(x, x)$$

is Σ^0_k but cannot be Π^0_k, because, if it were, then for some e we would have

$$\neg \widetilde{S}^0_{k,1}(x, x,) \iff \widetilde{S}^0_{k,1}(e, x)$$

which is absurd when $x = e$. It follows that for each k, there exist relations which are Σ^0_k but not Π^0_k, and from this follows easily the strictness of all the inclusions in the diagram. $\dashv$

Theorem 5E.5 gives an alternative proof—and a better understanding—of Tarski's Theorem 4A.5, that the truth set of arithmetic $\mathrm{Truth}^{\mathbf{N}}$ is not arithmetical, cf. Problem x5.30.

Definition 5E.6 (Classifications)**.** A (complete) **classification** of a relation $P(\vec{x})$ (in the arithmetical hierarchy) is the determination of "the least" arithmetical class to which $P(\vec{x})$ belongs, i.e., the proof of a proposition of the form

$$P \in \Sigma^0_k \setminus \Pi^0_k, \quad P \in \Pi^0_k \setminus \Sigma^0_k, \quad \text{or } P \in \Delta^0_{k+1} \setminus (\Sigma^0_k \cup \Pi^0_k);$$

for example, in 5B.11 we showed that

$$\{e \mid W_e \neq \emptyset\} \in \Sigma^0_1 \setminus \Pi^0_1.$$

The complete classification of a relation P is sometimes very difficult, and we are often satisfied with the computation of some "upper bound", i.e., some k such that $P \in \Sigma^0_k$ or $P \in \Pi^0_k$. The basic method for the computation of a "lower bound," when this can be done, is to show that the given relation is *complete* in some class Σ^0_k or Π^0_k as in the next result.

Proposition 5E.7. (1) *The set* $F = \{e \mid \varphi_e$ *is total* $\}$ *is* Π^0_2 *but it is not* Σ^0_2.

(2) *The set* $\mathrm{Fin} = \{e \mid W_e$ *is finite*$\}$ *is* $\Sigma^0_2 \setminus \Pi^0_2$.

Proof. (1) The upper bound is obvious, since

$$e \in F \iff (\forall x)(\exists y)T_1(e, x, y).$$

To show (by contradiction) that F is not Σ^0_2, suppose $P(x)$ is any Π^0_2 relation, so that

$$P(x) \iff (\forall u)(\exists v)Q(x, u, v)$$

with a recursive $Q(x, u, v)$, and set

$$f(x, u) = \mu v Q(x, u, v).$$

If $\widehat{f}$ is a code of this (recursive) partial function $f(x, u)$, then

$$\begin{aligned} P(x) &\iff (\forall u)[f(x, u)\downarrow] \\ &\iff (\forall u)[\{S^1_1(\widehat{f}, x)\}(u)\downarrow] \\ &\iff S^1_1(\widehat{f}, x) \in F; \end{aligned}$$

it follows that if F were Σ^0_2, then every Π^0_2 would be Σ^0_2, which contradicts the Hierarchy Theorem 5E.5 (3).

(2) The upper bound is again trivial,

$$e \in \mathrm{Fin} \iff (\exists k)(\forall x)[x \in W_e \Longrightarrow x \leq k].$$

For the lower bound, let $P(x)$ be any Σ^0_2 relation, so that

$$P(x) \iff (\exists u)(\forall v)Q(x, u, v)$$

with a recursive Q. We set

$$g(x, u) = \mu y(\forall i \leq u)\neg Q(x, i, (y)_i),$$

so that if $\widehat{g}$ is a code of g, then

$$\begin{aligned} (\exists u)(\forall v)Q(x, u, v) &\iff \{u \mid g(x, u)\downarrow\} \text{ is finite} \\ &\iff \{u \mid \{\widehat{g}\}(x, u)\downarrow\} \text{ is finite} \\ &\iff \{u \mid \{S^1_1(\widehat{g}, x)\}(u)\downarrow\} \text{ is finite,} \end{aligned}$$

i.e.,

$$P(x) \iff S_1^1(\widehat{g}, x) \in \text{Fin};$$

but this implies that Fin is not Π_2^0, because, if it were, then every Σ_2^0 relation would be Π_2^0, which it is not. ⊣

5F. Relativization

The notions of μ-recursiveness in 4E.5 and reckonability in 4E.9 "relativize" naturally to a "given" partial function as follows.

Definition 5F.1. For a fixed partial function $p : \mathbb{N}^m \rightharpoonup \mathbb{N}$:

(1) A **μ-recursive derivation from** (or *relative to*) p is a sequence of partial functions on $\mathbb{N}$

$$f_1, f_2, \ldots, f_k,$$

where each f_i is S, or a constant C_q^n or a projection P_i^n, *or* p, or is defined by composition, primitive recursion or minimalization from functions before it in the sequence; and a partial function $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ is **μ-recursive in** p if it occurs in a μ-recursive derivation from p.

(2) For each partial function p, let Q_p be Robinson's system in the extension of the language of arithmetic with a single m-ary function symbol p and with the additional axioms

$$D_p = \{\mathsf{p}(\Delta x_1, \ldots, \Delta x_m) = \Delta w \mid p(x_1, \ldots, x_m) = w\},$$

which express formally the graph of p. A partial function f is **reckonable in** p, if there is a formula $\mathbf{F}(v_1, \ldots, v_n, y, \mathsf{p})$ of Q_p, such that for all $\vec{x}, w$,

$$f(\vec{x}) = w \iff Q_p \vdash \mathbf{F}(\Delta x_1, \ldots, \Delta x_n, \Delta w, \mathsf{p}).$$

These notions express two different ways in which we can compute a function f *given access to the values of* p, and they behave best when the "given" p is total, in which case they coincide:

Proposition 5F.2. *If* $p : \mathbb{N}^m \to \mathbb{N}$ *is a total function, then, for every* (possibly partial) f,

$$f \text{ is } \mu\text{-recursive in } p \iff f \text{ is reckonable in } p.$$

Proof is a simple modification of the proof of 4E.10. ⊣

We will just say

$$f \text{ is recursive in } p \quad \text{or} \quad f \text{ is Turing-recursive in } p$$

for this notion of reduction of a partial function to a total one, the reference to "Turing" coming from a third equivalent definition which involves "Turing machines with oracles". The notion is cleanest and easiest to study on sets, via their characteristic functions.

5F.3. Turing reducibility and Turing degrees. For any two sets $A, B \subseteq \mathbb{N}$, we set

$$\begin{aligned} A \leq_T B &\iff A \text{ is } \textit{recursive} \text{ in (or } \textit{Turing reducible to}) \ B \\ &\iff \chi_A \text{ is recursive in } \chi_B, \end{aligned}$$

where χ_A, χ_B are the (total) characteristic functions of A and B. We also set

$$A \equiv_T B \iff A \leq_T B \ \& \ B \leq_T A,$$

and we assign to each set A its *degree* (of unsolvability)

$$\deg(A) = \{B \mid B \equiv_T A\}.$$

Proposition 5F.4. (1) *$A \leq_m B \Longrightarrow A \leq_T B$, but the converse is not always true.*

(2) *If $A \leq_T B$ and $B \leq_T C$, then $A \leq_T C$.*

(3) *If B is recursive, then, for every A,*

$$A \leq_T B \iff A \text{ is recursive},$$

and so

$$\deg(\emptyset) = \deg(\mathbb{N}) = \{A \mid A \text{ is recursive}\}.$$

Less trivial are the following three properties, with which the serious study of degrees of unsolvability starts:

(1) *There is no maximal Turing degree*, i.e., for each A, there is some B such that $A <_T B$. (For example, if A is recursive, then $A <_T K$, since $A \leq_1 K$, but we can't have $K \leq_T A$ since this would imply that K is recursive.)

(2) (The Kleene-Post Theorem). *There exist Turing-incomparable sets A and B, i.e.,*

$$A \not\leq_T B \text{ and } B \not\leq_T A. \tag{129}$$

(3) (The Friedberg-Mucnik Theorem, strengthening (2) and resolving *Post's Problem*). *There exist Turing-incomparable, r.e. sets A, and B.*

We will not pursue here the theory of degrees of unsolvability, which is a separate (intricate and difficult) research area in the mathematical theory of computability. We turn instead to another use of the relativization process, which yields natural notions of computability for operations which take partial function arguments.

Definition 5F.5 (Functionals). A (partial) *functional* is any partial function $\alpha(x_1, \dots, x_n, p_1, \dots, p_m)$ of n number arguments and m partial function arguments, such that for $i = 1, \dots, m$, p_i ranges over the k_i-ary partial functions on $\mathbb{N}$, and such that (when it takes a value), $\alpha(x_1, \dots, x_n, p_1, \dots, p_m) \in$

$\mathbb{N}$. We view every partial function $f(\vec{x})$ as a functional 0 partial function arguments. More interesting examples include:

$$\alpha_1(x, p) = p(x + 1)$$
$$\alpha_2(x, p, q) = \mathit{if}\ x = 0\ \mathit{then}\ p(x)\ \mathit{else}\ q(x, p(x - 1))$$
$$\alpha_3(p) = \begin{cases} 1 & \text{if } p(0)\downarrow \text{ or } p(1)\downarrow \\ \uparrow & \text{otherwise} \end{cases}$$
$$\alpha_4(p) = \begin{cases} 1 & \text{if } p(0)\downarrow \\ 0 & \text{otherwise} \end{cases}$$
$$\alpha_5(p) = \begin{cases} 1 & \text{if } (\forall x)[p(x)\downarrow] \\ \uparrow & \text{otherwise} \end{cases}$$

From these examples, we might say that α_1 and α_2 are "recursive", in the sense that we can see a direct method for computing their values if we have access to a "oracles" who can respond to questions of the form

What is $p(x)$? What is $q(x, y)$?

for specific x. To compute $\alpha_2(x, p)$, for example, if $x = 0$ we request of the oracle the value $p(0, x)$ and give it as output, while, if $x > 0$, then we first request the value $v = p(x - 1, 0)$, and then we request and give as output the value $p(x, v)$. On the other hand, there is no obvious way to compute the values of α_4 and α_5 in this way, unless we can ask the oracle questions about the domain of convergence of p, a conception which does not yield a natural and useful notion of computability. Finally, $\alpha_3(p)$ is a borderline case, which appears to be recursive if we can ask the oracle "non-deterministic" questions of the form

what is $p(0)$ or $p(1)$?,

which looks iffy—or, at the least, suggests on a different notion of "non-deterministic computability" for functionals.

Definition 5F.6 (Recursive functionals)**.** We make these two notions of functional computability precise, using the relativization process.

(1) A μ-**recursive** (functional) **derivation** (in one, m-ary partial function variable) is a sequence of functionals

$$\alpha_1(\vec{x}_1, p), \dots, \alpha_m(\vec{x}_m, p)$$

in which each α_i is S, C^n_q or P^n_j (not depending on p); an *evaluation functional*

$$\text{ev}^m(x_1, \dots, x_m, p) = p(x_1, \dots, x_m) \tag{130}$$

which introduces dependence on p; or it is defined from previously listed functionals by composition, primitive recursion or minimalization, which are defined as before, e.g,

$$\alpha_i(\vec{x}, p) = \mu y[\alpha_j(\vec{x}, y, p) = 0] \quad (j < i).$$

A functional is **μ-recursive**, or just **recursive**, if it occurs in some μ-recursive derivation.

(2) A functional $\alpha(\vec{x}, p)$ is **reckonable** (or *non-deterministically recursive*) if there is a formula $\mathbf{F}(v_1, \dots, v_n, y, \mathsf{p})$ in the system Q_p introduced in (2) of 5F.1, such that for all $\vec{x}, w$ and p,

$$\alpha(\vec{x}, p) = w \iff Q_p \vdash \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w, \mathsf{p}). \tag{131}$$

5F.7. Remark. There is no formula $\mathbf{F}(v_1, \dots, v_n, y, \mathsf{p})$ such that, for all $\vec{x}$, w and p

$$p(\vec{x}) = w \iff \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w) \tag{A}$$

$$Q_p \vdash (\exists! y)\mathbf{F}(\Delta x_1, \dots, \Delta x_n, y), \tag{B}$$

simply because if (A) holds for all p, then the formula on the right of (B) is not true, whenever p is not a totally defined function. This means that the simplest evaluation functional (130) is not "numeralwise representable" in Q, in the most natural extension of this notion to functionals, which is why we have not introduced it.

Proposition 5F.8. *Every recursive functional is reckonable.*

Proof is a minor modification of the argument for (1) $\Longrightarrow$ (2) of Theorem 4E.10 (skipping the argument for the characteristic property of numeralwise representability which does not hold here), and we will skip it. $\dashv$

To separate recursiveness from reckonability for functionals, we need to introduce some basic notions, all of them depending on the following, partial ordering of partial functions of the same arity.

Definition 5F.9. For any two, m-ary partial functions p and q, we set

$$p \leq q \iff (\forall \vec{x}, w)[p(\vec{x}) = w \Longrightarrow q(\vec{x}) = w],$$

i.e., if the domain of convergence of p is a subset of the domain of convergence of q, and q agrees with p whenever they are both defined. For example, if $\emptyset$ is *the nowhere-defined* m-ary partial function, then, for every m-ary q, $\emptyset \leq q$; and, at the other extreme,

$$(\forall \vec{x})p(\vec{x})\downarrow \ \ \& \ p \leq q \Longrightarrow p = q.$$

Proposition 5F.10. *For each m, $\leq$ is a partial ordering of the set of all m-ary partial functions, i.e.,*

$$p \leq p, \quad [p \leq q \ \& \ q \leq r] \Longrightarrow p \leq r, \quad [p \leq q \ \& \ q \leq p] \Longrightarrow p = q.$$

Proof is simple and we will skip it. ⊣

Definition 5F.11. A functional $\alpha(\vec{x}, p)$ is:

1. **monotonic** (or monotone), if for all partial functions p, q, and all $\vec{x}$, w,
$$[\alpha(\vec{x}, p) = w \;\&\; p \leq q] \Longrightarrow \alpha(\vec{x}, q) = w;$$
2. **continuous**, if for each p and al $\vec{x}$, w,
$$\alpha(\vec{x}, p) = w \Longrightarrow (\exists r)[r \leq p \;\&\; \alpha(\vec{x}, r) = w \;\&\; r \text{ is finite}],$$
where a partial function is **finite** if its domain of convergence is finite; and
3. **deterministic**, if for each p and all $\vec{x}$, w,
$$\alpha(\vec{x}, p) = w \Longrightarrow (\exists! r \leq p)[\alpha(\vec{x}, r) = w \;\&\; (\forall r' \leq r)[\alpha(\vec{x}, r')\downarrow \;\Longrightarrow r' = r]].$$

5F.12. Exercise. Give counterexamples to show that no two of these properties imply the third.

Theorem 5F.13. (1) *Every reckonable functional is monotonic and continuous.*

(2) *Every recursive functional is monotonic, continuous and deterministic.*

(3) *There are reckonable functionals which are not deterministic.*

Proof. (1) is immediate, using the (corresponding) properties of proofs: for example, if
$$Q_p \vdash \mathbf{F}(\Delta x_1, \ldots, \Delta x_n, \Delta w, \mathsf{p})$$
for some p, $\vec{x}$ and w, then the proof can only use a finite number of the axioms in Q_p, which "fix" p only on a finite set of arguments—and if r is the (finite) restriction of p to this set, then
$$Q_r \vdash \mathbf{F}(\Delta x_1, \ldots, \Delta x_n, \Delta w, \mathsf{r}),$$
so that $\alpha(\vec{x}, r) = w$.

(2) is proved by induction on a given μ-recursive derivation. There are several cases to consider, but the arguments are simple and we will skip them.

(3) The standard example is
$$\alpha_3(p) = \begin{cases} 1 & \text{if } p(0)\downarrow \text{ or } p(1)\downarrow \\ \uparrow & \text{otherwise} \end{cases}$$
as above, which is not deterministic because if $p(0) = p(1) = 0$ and $p(x)\uparrow$ for all $x > 1$, then there is no *least* $r \leq p$ which determines the value $\alpha_3(p) = 1$. ⊣

Part (1) of this theorem yields a simple normal form for reckonable functionals which characterizes them without reference to any formal systems. We need another coding.

5F.14. Coding of finite partial functions and sets. For each $a \in \mathbb{N}$ and each $m \geq 1$,

$$\begin{aligned} d(a,x) &= \begin{cases} (a)_x \dot{-} 1 & \text{if } x < \mathrm{lh}(a) \ \&\ (a)_x > 0, \\ \uparrow & \text{otherwise} \end{cases} \\ d_a(x) &= d(a,x), \\ D_x &= \{i \mid d_x(i)\downarrow\} \\ d_a^m(\vec{x}) &= d^m(a,\vec{x}) = d(a,\langle\vec{x}\rangle) \quad (\vec{x} = x_1,\dots,x_m). \end{aligned}$$

Note that, easily, *each partial function $d^m(a,\vec{x})$ is primitive recursive*; *the sequence*

$$d_0^m, d_1^m, \dots$$

enumerates all finite partial functions of m arguments; and *the sequence*

$$D_0, D_1, \dots$$

enumerates all finite sets, so that the binary relation of membership

$$i \in D_x \iff i < \mathrm{lh}(x) \ \&\ (x)_i > 0,$$

is primitive recursive.

Theorem 5F.15 (Normal form for reckonable functionals)**.** *A functional $\alpha(\vec{x},p)$ is reckonable if and only if there exists a semirecursive relation $R(\vec{x},w,a)$, such that for all $\vec{x}$, w and p,*

$$\alpha(\vec{x},p) = w \iff (\exists a)[d_a^m \leq p \ \&\ R(\vec{x},w,a)]. \tag{132}$$

PROOF. Suppose first that $\alpha(\vec{x},p)$ is reckonable, and compute:

$$\begin{aligned} \alpha(\vec{x},p) = w &\iff (\exists \text{ finite } r \leq p)[\alpha(\vec{x},r) = w] \qquad \text{(by 5F.13)} \\ &\iff (\exists a)[d_a^m \leq p \ \&\ \alpha(\vec{x},d_a^m) = w)]. \end{aligned}$$

Thus, it is enough to prove that the relation

$$R(\vec{x},w,a) \iff \alpha(\vec{x},d_a^m) = w$$

is semirecursive; but if (131) holds with some formula $\mathbf{F}(v_1,\dots,v_m,y,\mathsf{p})$, then

$$\begin{aligned} R(\vec{x},w,a) &\iff Q_{d_a^m} \vdash \mathbf{F}(\Delta x_1,\dots,\Delta x_n,\Delta w,\mathsf{p}) \\ &\iff Q \vdash \sigma_{m,a,\mathsf{p}} \rightarrow \mathbf{F}(\Delta x_1,\dots,\Delta x_n,\Delta w,\mathsf{p}) \end{aligned}$$

where $\sigma_{m,a,\mathsf{p}}$ is the *finite* conjunction of equations

$$\mathsf{p}(\Delta u_1,\dots,\Delta u_m) = \Delta d_a^m(u_1,\dots,u_m),$$

one for each $u_1, \dots, u_m$ in the domain of d_a^m. A code of the sentence on the right can be computed primitive recursively from $\vec{x}, w, a$, so that $R(\vec{x}, w, a)$ is reducible to the relation of provability in Q and hence semirecursive.

For the converse, we observe that with the same $\sigma_{m,a,\mathsf{p}}$ we just used and for any m-ary p,

$$d_a^m \leq p \iff Q_p \vdash \sigma_{m,a,\mathsf{p}},$$

and that, with some care, this $\sigma_{m,a,\mathsf{p}}$ can be converted to a formula $\sigma^*(a, \mathsf{p})$ with the free variable a, in which bounded quantification replaces the blunt, finite conjunction so that

$$d_a^m \leq p \iff Q_p \vdash \sigma^*(\Delta a, \mathsf{p}). \tag{133}$$

Assume now that $\alpha(\vec{x}, p)$ satisfies (132), choose a primitive recursive $P(\vec{x}, w, a, z)$ such that

$$R(\vec{x}, w, a) \iff (\exists z) P(\vec{x}, w, a, z),$$

choose a formula $\mathbf{P}(v_1, \dots, v_n, v_{n+1}, v_{n+2}, z)$ which numeralwise expresses P in Q, and set

$$\mathbf{F}(v_1, \dots, v_n, v_{n+1}, v_{n+2})) \equiv (\exists a)[\sigma^*(a, \mathsf{p}) \ \&\ (\exists z)\mathbf{P}(v_1, \dots, v_n, v_{n+1}, a, z)]].$$

Now,

$$\begin{aligned} Q_p \vdash \mathbf{F}(\Delta x_1, \dots, \Delta x_n, \Delta w, \mathsf{p}) & \\ \iff Q_p \vdash (\exists a)[\sigma^*(a, \mathsf{p}) & \\ \&\ (\exists z)[\mathbf{P}(\Delta x_1, \dots, \Delta x_n, \Delta w, a, z)]] & \\ \iff \alpha(\vec{x}, p) = w, & \end{aligned}$$

with the last equivalence easy to verify, using the soundness of Q_p. ⊣

There is no simple normal form of this type for recursive functionals, because predicate logic is not well suitable for expressing "determinism".

5G. Effective operations

Intuitively, a functional $\alpha(\vec{x}, p)$ is *recursive* in either of the two ways that we made precise, if its values can be computed effectively and uniformly *for all partial functions* p, given access only to specific values of p—which simply means that the evaluation functional (130) is declared recursive. In many cases, however, we are interested in the values $\alpha(\vec{x}, p)$ only for *recursive partial functions* p, and then we might make available to the computation procedure some code of p, from which (perhaps) more than the values of p can be extracted.

Definition 5G.1. The *associate* of a functional $\alpha(\vec{x}, p)$ is the partial function

$$f_\alpha(\vec{x}, e) = \alpha(\vec{x}, \varphi_e), \tag{134}$$

and we call $\alpha(\vec{x}, p)$ an *effective operation* if its associate is recursive.

Note that this imposes no restriction on the values $\alpha(\vec{x}, p)$ for non-recursive p, and so, properly speaking, we should think of effective operations as (partial) functions on *recursive partial functions*, not on all partial functions—this is why the term "operation" is used. For purposes of comparison with recursive functionals, however, it is convenient to consider effective operations as functionals, with arbitrary values on non-recursive arguments, as we did in the precise definition.

Proposition 5G.2. *A recursive partial function $f(\vec{x}, e)$ is the associate of some effective operation if and only if it satisfies the invariance condition*

$$\varphi_e = \varphi_m \Longrightarrow f(\vec{x}, e) = f(\vec{x}, m); \tag{135}$$

and if f satisfies this condition, then it is the associate of the effective operation

$$\alpha(\vec{x}, \varphi_e) = f(\vec{x}, e),$$

(with $\alpha(\vec{x}, p)$ defined arbitrarily when p is not recursive).

Proof is immediate. ⊣

Theorem 5G.3. *Every reckonable functional* (and hence every recursive functional) *is an effective operation.*

Proof. This is immediate from the Normal Form Theorem for reckonable functionals 5F.15; because if $f(\vec{x}, e)$ is the associate of $\alpha(\vec{x}, p)$, then

$$f(\vec{x}, e) = w \iff (\exists a)[d_a^m \le \varphi_e \;\&\; R(\vec{x}, w, a)]$$

with a semirecursive $R(\vec{x}, w, a)$ by 5F.15, and so the graph of f is semirecursive and f is recursive. ⊣

Definition 5G.4. A functional $\alpha(\vec{x}, p)$ is *operative* if $\vec{x} = x_1, \dots, x_n$ varies over n-tuples and p over n-ary partial functions, for the same n, so that the *fixed point equation*

$$p(\vec{x}) = \alpha(\vec{x}, p) \tag{136}$$

makes sense. Solutions of this equation are called *fixed points* of α.

Theorem 5G.5 (The Fixed Point Lemma). *Every operative effective operation α has a recursive fixed point, i.e., there exists a recursive partial function p such that, for all $\vec{x}$,*

$$p(\vec{x}) = \alpha(\vec{x}, p).$$

Proof. The partial function

$$f(z,\vec{x}) = \alpha(\vec{x},\varphi_z)$$

is recursive, and so, by the Second Recursion Theorem, there is some z^* such that

$$\begin{aligned}\varphi_{z^*}(\vec{x}) &= f(z^*,\vec{x})\\ &= \alpha(\vec{x},\varphi_{z^*});\end{aligned}$$

and so $p = \varphi_{z^*}$ is a fixed point of α. $\dashv$

5G.6. Remark. By an elaboration of these methods (or different arguments), it can be shown that *every effective operation has a recursive least fixed point*: i.e., that for some recursive partial function p, the fixed point equation (136) holds, and in addition, for all q,

$$(\forall\vec{x})[q(\vec{x}) = \alpha(\vec{x},q)] \Longrightarrow p \le q.$$

The Fixed Point Lemma applies to all reckonable operative functionals, and it is a powerful tool for showing easily the recursiveness of partial functions defined by very general recursive definitions, for example by *double recursion*:

5G.7. Example. If g_1, g_2, g_3, π_1, π_2 are total recursive functions and $f(x,y,z)$ is defined by the *double recursion*

$$\begin{aligned}f(0,y,z) &= g_1(y,z)\\ f(x+1,0,z) &= g_2(f(x,\pi_1(x,y,z),z),x,y,z)\\ f(x+1,y+1) &= g_3(f(x+1,y,\pi_2(x,y,z)),x,y,z),\end{aligned}$$

then $f(x,y,z)$ is recursive.

Proof. The functional

$$h(x,y,z,p) = \begin{cases} g_1(y,z) & \text{if } x = 0\\ g_2(p(x \dot{-} 1,\pi_1(x \dot{-} 1,0,z),z),x \dot{-} 1,0,z) & \text{otherwise, if } y = 0\\ g_3(p(x,y \dot{-} 1,\Pi^0_2(x,y \dot{-} 1,z)),x,y \dot{-} 1,z) & \text{otherwise}\end{cases}$$

is recursive, and so it has a recursive fixed point $f(x,y,z)$, which, easily, satisfies the required equations. It remains to show that $f(x,y,z)$ is a total function, and we do this by showing by an induction on x that $(\forall x)f(x,y,z)\downarrow$; both the basis case and the induction step require separate inductions on y. $\dashv$

The converse of Theorem 5G.3 depends on the following, basic result.

Lemma 5G.8. *Every effective operation is monotonic and continuous on recursive partial arguments.*

Proof. To simplify the argument we consider only effective operations of the form $\alpha(p)$, with no numerical argument and a unary partial function argument, but the proof for the general case is only notationally more complex.

To show monotonicity, suppose $p \le q$, where

$$p = \varphi_e \text{ and } q = \varphi_m,$$

and let $\widehat{f}$ be a code of the associate of α, so that for every z,

$$\alpha(\varphi_z) = \{\widehat{f}\}(z).$$

Suppose also that

$$\alpha(\varphi_e) = w;$$

we must show that $\alpha(\varphi_m) = w$.

The relation

$$R(z, x, v) \iff \varphi_e(x) = v \text{ or } [\{\widehat{f}\}(z) = w \;\&\; \varphi_m(x) = v]$$

is semirecursive; the hypothesis $\varphi_e \le \varphi_m$ implies that

$$R(z, x, v) \Longrightarrow \varphi_m(x) = v;$$

hence $R(z, x, v)$ is the graph of some recursive partial function $g(z, x)$; and so, by the Second recursion Theorem, there is some number z^* such that $\varphi_{z^*}(x) = g(z^*, x)$, so that

$$\varphi_{z^*}(x) = v \iff \varphi_e(x) = v \text{ or } [\{\widehat{f}\}(z^*) = w \;\&\; \varphi_m(x) = v]. \tag{137}$$

We now observe that:

(1a) $\alpha(\varphi_{z^*}) = \{\widehat{f}\}(z^*) = w$; because, if not, then $\varphi_{z^*} = \varphi_e$ from (137), and so $\alpha(\varphi_{z^*}) = \alpha(\varphi_e) = w$.

(1b) $\varphi_{z^*} = \varphi_m$, directly from the hypothesis $\varphi_e \le \varphi_m$ and (1a).

It follows that $\alpha(\varphi_m) = \alpha(\varphi_{z^*}) = w$.

The construction for the proof of continuity is a small variation, as follows. First, we find using the Second recursion Theorem some z^* such that

(138)

$$\varphi_{z^*}(x) = v \iff (\forall u \le x)\neg[T_1(\widehat{f}, z^*, u) \;\&\; U(u) = w] \;\&\; \varphi_e(x) = v,$$

and we observe:

(2a) $\alpha(\varphi_{z^*}) = w$. Because, if not, then

$$(\forall u)\neg[T_1(\widehat{f}, z^*, u) \;\&\; U(u) = w],$$

and hence, for every x,

$$(\forall u \le x)\neg[T_1(\widehat{f}, z^*, u) \;\&\; U(u) = w],$$

and so, from (138), $\varphi_{z^*} = \varphi_e$ and $\alpha(\varphi_{z^*}) = \alpha(\varphi_e) = w$.

(2b) $\varphi_{z^*} \le \varphi_e$, directly from (138).

(2c) The partial function φ_{z^*} is finite, because it converges only when

(139) $$x < (\mu u)[T_1(\widehat{f}, z^*, u) \;\&\; U(u) = w]. \qquad \dashv$$

Theorem 5G.9 (Myhill-Shepherdson)**.** *For each effective operation $\alpha(\vec{x}, p)$, there is a reckonable functional $\alpha^*(\vec{x}, p)$ such that for all recursive partial functions p,*

(140) $$\alpha(\vec{x}, p) = \alpha^*(\vec{x}, p).$$

Proof. By the Lemma,

$$\alpha(\vec{x}, \varphi_e) = w \iff (\exists a)[d^m_a \le \varphi_e \;\&\; \alpha(\vec{x}, d^m_a) = w],$$

and so (140) holds with

(141) $$\alpha^*(\vec{x}, p) = w \iff (\exists a)[d^m_a \le p \;\&\; \alpha(\vec{x}, d^m_a) = w].$$

To show that this α^* is reckonable, note that (by an easy application of the S^m_n-Theorem) there is a primitive recursive $u(a)$ such that

$$d^m_a = \varphi_{u(a)},$$

and so the partial function

$$\alpha(\vec{x}, d^m_a) = f_\alpha(\vec{x}, u(a))$$

is recursive, its graph is semirecursive, and (141) with Theorem 5F.15 imply that α^* is reckonable. $\dashv$

5G.10. Remark. It is natural to think of a functional $\alpha(\vec{x}, p)$ as interpreting a program A, which computes some function $f(\vec{x})$ but requires for the computations some unspecified partial function p—and hence, A must be "given" p in addition to the arguments $\vec{x}$. Now if p could be any partial function whatsoever, then the only reasonable way by which A can be "given" p is *through its values*: we imagine that A can look up a table or ask an "oracle" for $p(u)$, for any specific u, during the computation. We generally refer to this manner of "accessing" a partial function by a program as *call-by-value*, and it is modeled mathematically by recursive or reckonable functionals, depending on whether the program A is deterministic or not. On the other hand, if it is known that $p = \varphi_e$ is a recursive partial function, then some code e of it may be given to A, at the start of the computation, so that A can compute any $p(u)$ that it wishes, but also (perhaps) infer general properties of p from e, and use these properties in its computations; this manner of accessing a recursive partial function is (one version of) *call-by-name*, and it is modeled mathematically by effective operations.

One might suspect that given access to a code of p, one might be able to compute effectively partial functions (depending on p) which cannot be computed when access to p is restricted in call-by-value fashion. The Myhill-Shepherdson Theorem tells us that, for non-deterministic programs, this cannot happen—knowledge of a code of p does not enlarge the class of partial functions which can be non-deterministically computed from it. Note that this is certainly false for deterministic computations, because of the basic example $\alpha_3(p)$ in 5F.5, which is reckonable but not recursive.

5H. Computability on Baire space

We will extend here the basic results about recursive partial functions and relations on $\mathbb{N}$, to partial functions and relations which can also take arguments in *Baire space*, the set

$$\mathcal{N} = (\mathbb{N} \to \mathbb{N}) = \{\alpha \mid \alpha : \mathbb{N} \to \mathbb{N}\}$$

of all total, unary functions on the natural numbers. For example, the total functions

$$f(\alpha) = \alpha(0), \quad g(x, \alpha, \beta, y) = \alpha(\beta(x)) + y,$$

will be deemed recursive (recursive) by the definitions we will give, and so will the partial function

$$h(\alpha) = \mu t[\alpha(t) = 0],$$

which is defined only if $\alpha(t) = 0$ for some t. The relation

$$R(\alpha) \iff (\exists t)[\alpha(t) = 0]$$

will be semirecursive but not recursive.

5H.1. Notation. More precisely, in this section we will study partial functions

$$f : \mathbb{N}^n \times \mathcal{N}^\nu \rightharpoonup \mathbb{N},$$

with $n = 0$ or $\nu = 0$ allowed, so that the partial functions on $\mathbb{N}$ we have been studying are included. To avoid "too many dots", we set once and for all boldface abbreviations for vectors,

$$\boldsymbol{x} = (x_1, \dots, x_n),\ \boldsymbol{y} = (y_1, \dots, y_m),\ \boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_\nu),\ \boldsymbol{\beta} = (\beta_1, \dots, \beta_\mu),$$

so that the values of our partial functions will be denoted compactly by expression like

$$f(\boldsymbol{x}, \boldsymbol{\alpha}),\ g(t, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{\alpha}, \gamma, \boldsymbol{\beta}),\ \text{etc.}$$

In defining specific functions we will sometimes mix the number with the Baire arguments, as above, the "official" reading always being the one in which all number arguments precede all the Baire ones, e.g.,

$$g(x, \alpha, \beta, y) = g(x, y, \alpha, \beta).$$

Codings of initial segments. Recall from Lemma 3I.13 the following notation, which will now be very useful:

$$\overline{\alpha}(0) = 1, \quad \overline{\alpha}(t) = \langle \alpha(0), \alpha(1), \dots, \alpha(t \dot{-} 1)\rangle \in \mathbb{N}$$

and for vectors of Baire points,

$$\overline{\boldsymbol{\alpha}}(t) = (\overline{\alpha}_1(t), \dots, \overline{\alpha}_\nu(t)) \in \mathbb{N}^\nu.$$

For any sequence code u and any s, put

$$u \restriction s = \begin{cases} \langle (u)_0, \dots, (u)_{s-1}\rangle, & \text{if } s \leq \mathrm{lh}(u),\\ u, & \text{otherwise,}\end{cases}$$

so that

$$\mathrm{lh}(u \restriction s) = \min\{\mathrm{lh}(u), s\}, \quad \text{and} \quad s \leq t \Longrightarrow \overline{\alpha}(s) = \overline{\alpha}(t) \restriction s.$$

Similarly, for any tuple of sequence codes $\vec{u} = (u_1, \dots, u_\nu)$ and any s, put

$$\vec{u} \restriction s = (u_1 \restriction s, \dots, u_\nu \restriction s),$$

so that

$$\text{if } s \leq t, \text{ then } \overline{\boldsymbol{\alpha}}(s) = \overline{\boldsymbol{\alpha}}(t) \restriction s.$$

A relation $R(\boldsymbol{x}, \vec{u})$ is **monotone in** $\vec{u}$ if, for every $\boldsymbol{\alpha}$ and every s,

$$\text{if } R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s)) \text{ and } s \leq t, \text{ then } R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)).$$

λ-abstraction. We will also find useful Church's λ operation, by which, for any partial function $f : \mathbb{N}^{n+1} \times \mathcal{N}^\nu \rightharpoonup \mathbb{N}$,

$$\lambda(t) f(\boldsymbol{x}, t, \boldsymbol{\alpha}) = g_{\boldsymbol{x},\boldsymbol{\alpha}} : \mathbb{N} \rightharpoonup \mathbb{N} \text{ where } g_{\boldsymbol{x},\boldsymbol{\alpha}}(t) = f(\boldsymbol{x}, t, \boldsymbol{\alpha}),$$

For example, $\lambda(t)(xt + t^2)$ is that function $g_x : \mathbb{N} \to \mathbb{N}$ such that for all t, $g_x(t) = xt + t^2$, and (closer to the way we will use this),

$$\lambda(x) U(\mu y T_1(e, x, y)) = \varphi_e. \tag{142}$$

Definition 5H.2 (Semirecursive relations on $\mathcal{N}$)**.** A relation

$$P(\boldsymbol{x}, \boldsymbol{\alpha}) \iff P(x_1, \dots, x_n, \alpha_1, \dots, \alpha_\nu)$$

is *semirecursive* or Σ^0_1, if there is a semirecursive relation

$$R(\boldsymbol{x}, \vec{u}) \iff R(x_1, \dots, x_n, u_1, \dots, u_\nu)$$

on $\mathbb{N}$, such that

$$P(\boldsymbol{x}, \boldsymbol{\alpha}) \iff (\exists t) R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)). \tag{143}$$

A relation $P(\boldsymbol{x}, \boldsymbol{\alpha})$ is *recursive* or Δ^0_1 if both $P(\boldsymbol{x}, \boldsymbol{\alpha})$ and its negation $\neg P(\boldsymbol{x}, \boldsymbol{\alpha})$ are semirecursive.

Notice that these definitions agree with the old ones for relations $R(\boldsymbol{x})$ which have no Baire arguments.

Lemma 5H.3. *The class of semirecursive relations with arguments in* $\mathbb{N}$ *and* $\mathcal{N}$ *is closed under permutations and identifications of variables: i.e., if*

$$\pi : \{1, \dots , n\} \to \{1, \dots , m\}, \quad \rho : \{1, \dots , \nu\} \to \{1, \dots , \mu\}$$

are any functions and $P(y_1, \dots , y_m, \beta_1, \dots , \beta_\mu)$ *is semirecursive, then so is the relation*

$$P'(x_1, \dots , x_n, \alpha_1, \dots , \alpha_\nu) \iff P(x_{\pi(1)}, \dots , x_{\pi(n)}, \alpha_{\rho(1)}, \dots , \alpha_{\rho(n)})$$

This justifies "explicit" definitions of the form

$$P'(x, y, \alpha, \beta) \iff P(y, x, x, \beta, \beta, \beta)$$

within Σ^0_1, and it is immediate from the definition.

Lemma 5H.4. (1) *If* $P(\boldsymbol{x}, \boldsymbol{\alpha}) \iff (\exists t)R(\boldsymbol{x}, t, \boldsymbol{\alpha})$ *with a semirecursive* $R(\boldsymbol{x}, t, \vec{u})$*, then* $P(\boldsymbol{x}, \boldsymbol{\alpha})$ *is semirecursive.*

(2) *If* $P(\boldsymbol{x}, \boldsymbol{\alpha})$ *is semirecursive and* $\nu \geq 1$*, then it satisfies* (143) *with some recursive relation* $R(\boldsymbol{x}, \vec{u})$ *which is monotone in* $\vec{u}$*.*

Proof. (1) The claim is obvious when $\nu = 0$, since the assumed equivalence implies immediately that $R(\boldsymbol{x})$ is a semirecursive relation on $\mathbb{N}$.

If $\nu \geq 1$, so that $P(\boldsymbol{x}, \boldsymbol{\alpha})$ has at least one Baire argument, we set

$$R'(\boldsymbol{x}, \vec{u}) \iff (\exists s \leq \mathrm{lh}(u_1))R(\boldsymbol{x}, s, \vec{u} \restriction s),$$

and compute:

$$\begin{aligned} P(\boldsymbol{x}, \boldsymbol{\alpha}) &\iff (\exists t)R(\boldsymbol{x}, t, \overline{\boldsymbol{\alpha}}(t)) \\ &\iff (\exists t)(\exists s \leq t)R(\boldsymbol{x}, s, \overline{\boldsymbol{\alpha}}(s)) \\ &\iff (\exists t)(\exists s \leq \mathrm{lh}(\overline{\alpha}_1(t)))R(\boldsymbol{x}, s, \overline{\boldsymbol{\alpha}}(t) \restriction s) \\ &\iff (\exists t)R'(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)). \end{aligned}$$

(2) Assume that (143) holds with

$$R(\boldsymbol{x}, \vec{u}) \iff (\exists y)Q(\boldsymbol{x}, \vec{u}, y)$$

where $Q(\boldsymbol{x}, \vec{u}, y)$ is recursive, and let

$$\begin{aligned} R'(\boldsymbol{x}, \vec{u}) \iff &(\text{for } i = 1, \dots , \nu)[\mathrm{lh}(u_i) = \mathrm{lh}(u_1)] \\ &\& \ (\exists s \leq \mathrm{lh}(u_1))(\exists y \leq \mathrm{lh}(u_1))Q(\boldsymbol{x}, \vec{u} \restriction s, y). \end{aligned}$$

Now $R'(\boldsymbol{x}, \vec{u})$ is clearly recursive and monotone in $\vec{u}$, and

$$\begin{aligned} P(\boldsymbol{x}, \boldsymbol{\alpha}) &\iff (\exists s)R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s)) \\ &\iff (\exists s)(\exists y)Q(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s), y) \\ &\iff (\exists t)(\exists s \leq t)(\exists y \leq t)Q(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s), y) \\ &\iff (\exists t)R'(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)). \end{aligned}$$

⊣

Lemma 5H.5 (Closure properties of Σ^0_1 and Δ^0_1). (1) *The class of semirecursive relations with arguments in* $\mathbb{N}$ *and* $\mathcal{N}$ *is closed under substitutions of total, recursive functions* $f : \mathbb{N}^n \to \mathbb{N}$*; the positive propositional operations* & *and* $\vee$*; bounded number quantification of both kinds; existential number quantification* $(\exists x)$*; and also existential quantification over* $\mathcal{N}$*,* $(\exists\alpha)$*.*

(2) *The class of recursive relations with arguments in* $\mathbb{N}$ *and* $\mathcal{N}$ *is closed under substitutions of total, recursive functions* $f : \mathbb{N}^n \to \mathbb{N}$*; the propositional operations* $\neg$*,* & *and* $\vee$*; and bounded number quantification of both kinds.*

Proof. We may assume in the proofs that $\nu \geq 1$ (i.e., Baire arguments are present), since otherwise these results are known.

For conjunction, assume that P_1 and P_2 satisfy (143) with a recursive, monotone matrix, by (2) of Lemma 5H.4, and compute:

$$\begin{aligned} P_1(\boldsymbol{x},\boldsymbol{\alpha}) \ \&\ P_2(\boldsymbol{x},\boldsymbol{\alpha}) &\iff (\exists t)R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t)) \ \&\ (\exists t)R_2(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t)) \\ &\iff (\exists t)[R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t)) \ \&\ R_2(\boldsymbol{x},t,\overline{\boldsymbol{\alpha}}(t))], \end{aligned}$$

the last equivalence by the monotonicity.

For existential quantification over $\mathcal{N}$:

$$\begin{aligned} P(\boldsymbol{x},\boldsymbol{\alpha}) &\iff (\exists\beta)P_1(\boldsymbol{x},\boldsymbol{\alpha},\beta) \\ &\iff (\exists\beta)(\exists t)R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t),\overline{\beta}(t)) \\ &\iff (\exists t)(\exists\beta)R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t),\overline{\beta}(t)) \\ &\iff (\exists t)(\exists v)[\mathrm{Seq}(v) \ \&\ \mathrm{lh}(v) = t \ \&\ R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t),v)]; \end{aligned}$$

the crucial "quantifier-drop" equivalence

$$(\exists\beta)R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t),\overline{\beta}(t)) \iff (\exists v)[\mathrm{Seq}(v) \ \&\ \mathrm{lh}(v) = t \ \&\ R_1(\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t),v)]$$

is proved from left-to-right by setting $v = \overline{\beta}(t)$, and from right-to-left by taking β to be an arbitrary, infinite extension of the sequence v. Now set

$$R'(\boldsymbol{x},t,\vec{u}) \iff (\exists v)[\mathrm{Seq}(v) \ \&\ \mathrm{lh}(v) = t \ \&\ R(\boldsymbol{x},\vec{u},v)];$$

this is a semirecursive relation,

$$P(\boldsymbol{x},\boldsymbol{\alpha}) \iff (\exists\beta)P_1(\boldsymbol{x},\boldsymbol{\alpha},\beta) \iff (\exists t)R'(\boldsymbol{x},t,\overline{\boldsymbol{\alpha}}(t)),$$

and so $P(\boldsymbol{x},\boldsymbol{\alpha})$ is semirecursive by (1) of Lemma 5H.4.

The remaining arguments are similar. $\dashv$

Theorem 5H.6. (1) *For every* n *and every* ν*, there exists a* Σ^0_1 *relation*

$$\widetilde{S}^0_{n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}) \iff \widetilde{S}^0_{n,\nu}(e,x_1,\dots,x_n,\alpha_1,\dots,\alpha_\nu)$$

such that an arbitrary relation $R(\boldsymbol{x},\boldsymbol{\alpha})$ *is semirecursive if and only if there is some number* e *such that*

$$R(\boldsymbol{x},\boldsymbol{\alpha}) \iff \widetilde{S}^0_{n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}).$$

In fact, if $\nu \geq 1$, then

$$\widetilde{S}^0_{n,\nu}(e, \boldsymbol{x}, \boldsymbol{\alpha}) \iff (\exists t) T^r_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)), \tag{144}$$

where $T^r_{n,\mu}(e, \boldsymbol{x}, \vec{u})$ is a primitive recursive and monotone in $\vec{u}$ relation on $\mathbb{N}$.

(2) *If $n+\nu > 0$, then there exists a semirecursive relation $P(\boldsymbol{x}, \overline{\boldsymbol{\alpha}})$ which is not recursive.*

(3) *For every m, every n and every ν, there exists a primitive recursive function $S^{r,m}_{n,\nu}(e, \boldsymbol{y})$ such that for all $\boldsymbol{y}, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}$,*

$$\widetilde{S}^0_{m+n,\nu}(e, \boldsymbol{y}, \boldsymbol{x}, \boldsymbol{\alpha}) \iff \widetilde{S}^0_{n,\nu}(S^{r,m}_{n,\nu}(e, \boldsymbol{y}), \boldsymbol{x}, \boldsymbol{\alpha}).$$

Proof. (1) The result is known when $\nu = 0$, so we assume $\nu \geq 1$, and with the notation of the Normal Form and Enumeration Theorem 4F.1, we let

$$\begin{aligned} T^r_{n,\nu}(e, \boldsymbol{x}, \vec{u}) \iff & (\text{for } i = 1, \ldots, \nu)[\mathrm{Seq}(u_i) \ \& \ \mathrm{lh}(u_i) = \mathrm{lh}(u_1)] \\ & \& \ (\exists s \leq \mathrm{lh}(u_1))(\exists y \leq \mathrm{lh}(u_1)) T_{n+\nu}(e, \boldsymbol{x}, \vec{u} \restriction s, y). \end{aligned}$$

This is clearly primitive recursive and monotone in $\vec{u}$, and if $\widetilde{S}^0_{n,\nu}$ is defined from it by (144), then it is semirecursive. For the converse, suppose $P(\boldsymbol{x}, \boldsymbol{\alpha})$ satisfies (143) with a semirecursive $R(\boldsymbol{x}, \vec{u})$. By the Enumeration Theorem 4F.1, there is some e such that

$$R(\boldsymbol{x}, \vec{u}) \iff (\exists y) T_{n+\nu}(e, \boldsymbol{x}, \vec{u}, y),$$

and then we compute:

$$\begin{aligned} P(\boldsymbol{x}, \boldsymbol{\alpha}) &\iff (\exists t) R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)) \\ &\iff (\exists t)(\exists s \leq t) R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s)) \\ &\iff (\exists t)(\exists s \leq t)(\exists y) T_{n+\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s), y) \\ &\iff (\exists t)(\exists y \leq t)(\exists s \leq t) T_{n+\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(s), y) \\ &\iff (\exists t) T^r_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)). \end{aligned}$$

(2) follows from (1) by the usual, diagonal method, and (3) follows from the S^m_n theorem for recursive partial functions on $\mathbb{N}$ by setting

$$S^{r,m}_{n,\nu}(e, \boldsymbol{y}) = S^m_{n+\nu}(e, \boldsymbol{y})$$

and chasing the definitions. ⊣

Definition 5H.7 (Recursive partial functions on $\mathcal{N}$ to $\mathbb{N}$)**.** A partial function $f(\boldsymbol{x}, \boldsymbol{\alpha})$ with values in $\mathbb{N}$ is *recursive* if its graph

$$G_f(\boldsymbol{x}, \boldsymbol{\alpha}, w) \iff f(\boldsymbol{x}, \boldsymbol{\alpha}) = w$$

is semirecursive. For example, the (total) *evaluation function*

$$\mathrm{ev}(x, \alpha) = \alpha(x)$$

is recursive, because

$$\alpha(x) = w \iff (\exists t)[t > x \ \&\ (\overline{\alpha}(t))_x = w].$$

Lemma 5H.8 (Closure properties for recursive partial functions into $\mathbb{N}$)**.** *The class of recursive partial functions on Baire space with values in $\mathbb{N}$ contains all recursive partial functions $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$; it is closed under permutations and identifications of variables, i.e., if*

$$f(x_1, \dots, x_n, \alpha_1, \dots, \alpha_\nu) = g(x_{\pi(1)}, \dots, x_{\pi(n)}, \alpha_{\rho(1)}, \dots, \alpha_{\rho(n)})$$

with π, ρ as in Lemma 5H.3 and $g(\boldsymbol{y}, \boldsymbol{\beta})$ is recursive, then so is $f(\boldsymbol{x}, \boldsymbol{\alpha})$; and it is also closed under substitution (in its number arguments), primitive recursion, and minimalization.

PROOF. These claims all follow easily from the closure properties of the class of semirecursive relations, and we will consider just two of them, as examples.

For substitution (in a simple case), we are given that

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = g(h_1(\boldsymbol{x}, \boldsymbol{\alpha}), \boldsymbol{x}, \boldsymbol{\alpha}),$$

where $g(y, \boldsymbol{x}, \boldsymbol{\alpha})$ and $h(\boldsymbol{x}, \boldsymbol{\alpha})$ are recursive, and we compute the graph of $f(\boldsymbol{x}, \boldsymbol{\alpha})$:

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = w \iff (\exists y)[h_1(\boldsymbol{x}, \boldsymbol{\alpha}) = y \ \&\ g(y, \boldsymbol{x}, \boldsymbol{\alpha}) = w];$$

the result follows from the closure properties of Σ^0_1 in Lemma 5H.5.

For primitive recursion, we are given that

$$f(0, \boldsymbol{x}, \boldsymbol{\alpha}) = g(\boldsymbol{x}, \boldsymbol{\alpha}), \quad f(y + 1, \boldsymbol{x}, \boldsymbol{\alpha}) = h(f(y, \boldsymbol{x}, \boldsymbol{\alpha}), y, \boldsymbol{x}, \boldsymbol{\alpha}).$$

Hence,

$$\begin{aligned} &f(y, \boldsymbol{x}, \boldsymbol{\alpha}) = w \iff \\ &\quad (\exists u)[(u)_0 = g(\boldsymbol{x}, \boldsymbol{\alpha}) \ \&\ (\forall i \leq y)[(u)_{i+1} = h((u)_i, \boldsymbol{x}, \boldsymbol{\alpha})] \ \&\ (u)_y = w, \end{aligned}$$

and so the graph of $f(y, \underline{\mathrm{x}}, \boldsymbol{\alpha})$ is semirecursive. $\dashv$

Theorem 5H.9 (Normal Form and Enumeration)**.** (1) *For every n and every $\nu \geq 1$, there is a* (primitive) *recursive and monotone in $\vec{u}$ relation $T^1_{n,\nu}(e, \boldsymbol{x}, \vec{u})$ on $\mathbb{N}$, such that a partial function $f(\boldsymbol{x}, \boldsymbol{\alpha})$ into $\mathbb{N}$ is recursive if and only if there is a number e such that*

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = \{e\}(\boldsymbol{x}, \boldsymbol{\alpha}) = U(\mu t T^1_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t))), \tag{145}$$

with $U(t) = (t)_0$.

(2) *For every m, every n and every ν, there exists a primitive recursive function $S^m_{n,\nu}(e, \boldsymbol{y})$ such that for all $\boldsymbol{y}, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}$,*

$$\{e\}(\boldsymbol{y}, \boldsymbol{x}, \boldsymbol{\alpha}) = \{(S^m_{n,\nu}(e, \boldsymbol{y})\}(\boldsymbol{x}, \boldsymbol{\alpha}).$$

PROOF. (1) Every partial function defined by (145) with a recursive $T^1_{n,\nu}$ is recursive, by the closure properties. To define a suitable $T^1_{n,\nu}$, we note that by the definitions and Theorem 5H.6, for each recursive $f(\boldsymbol{x}, \boldsymbol{\alpha}) = w$, there is some e such that

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = w \iff (\exists t) T^r_{n+1,\nu}(e, \boldsymbol{x}, w, \overline{\boldsymbol{\alpha}}(t)). \tag{146}$$

We set

$$T^1_{n,\nu}(e, \boldsymbol{x}, \vec{u}) \iff (\text{for } i = 1, \dots, \nu)[\mathrm{Seq}(u_i) \;\&\; \mathrm{lh}(u_i) = \mathrm{lh}(u_1)] \\ \& \; (\exists s \le \mathrm{lh}(u_1)) T^r_{n+1,\nu}(e, \boldsymbol{x}, (s)_0, \vec{u} \restriction s).$$

This is obviously primitive recursive and monotone in $\vec{u}$, and to complete the proof, we need only show that if (146) holds for some e, then

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = \Big(\mu t T^1_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t))\Big)_0. \tag{147}$$

So fix $\boldsymbol{x}, \boldsymbol{\alpha}$, and first check that

$$s = \mu t T^1_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t)) \Longrightarrow f(\boldsymbol{x}, \boldsymbol{\alpha}) = (s)_0; \tag{148}$$

this holds because the hypothesis implies $T^r_{n+1,\nu}(e, \boldsymbol{x}, (s)_0, \overline{\boldsymbol{\alpha}}(s))$, which by (146) yields the conclusion. Conversely, if $f(\boldsymbol{x}, \boldsymbol{\alpha}) = w$, then

$$T^r_{n+1,\nu}(e, \boldsymbol{x}, w, \overline{\boldsymbol{\alpha}}(t))$$

holds for some t, and then taking $s = \langle w, t\rangle > t$ and using the monotonicity of $T^r_{n+1,\nu}(e, \boldsymbol{x}, w, \vec{u})$, we have

$$T^r_{n+1,\nu}(e, \boldsymbol{x}, (s)_0, \overline{\boldsymbol{\alpha}}(s));$$

so $(\exists t) T^1_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t))$, and then (148) gives

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = w \Longrightarrow \Big(\mu t T^1_{n,\nu}(e, \boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t))\Big)_0 = w, \tag{149}$$

which together with (148) yield (147).

(2) follows from (3) of Theorem 5H.6 by setting

$$S^m_{n,\nu}(e, \boldsymbol{y}) = S^{r,m}_{n+1,\nu}(e, \boldsymbol{y})$$

and chasing the definitions. $\dashv$

Definition 5H.10 (Recursive partial functions with values in $\mathcal{N}$)**.** A partial function $f : \mathbb{N}^n \times \mathcal{N}^\nu \rightharpoonup \mathcal{N}$ is recursive, if the following, associated, *unfolding* partial function $f^* : \mathbb{N}^{n+1} \times \mathcal{N} \rightharpoonup \mathbb{N}$ is recursive:

$$f^*(\boldsymbol{x}, \boldsymbol{\alpha}, t) = f(\boldsymbol{x}, \boldsymbol{\alpha})(t);$$

or, equivalently, if

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = \lambda(t) f^*(\boldsymbol{x}, \boldsymbol{\alpha}, t),$$

with some recursive $f^* : \mathbb{N}^{n+1} \times \mathcal{N}^\nu \rightharpoonup \mathbb{N}$. Thus

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = \beta \iff (\forall t)[f^*(\boldsymbol{x}, \boldsymbol{\alpha}, t) = \beta(t)],$$
$$f(\boldsymbol{x}, \boldsymbol{\alpha})\downarrow \iff (\forall t)[f^*(\boldsymbol{x}, \boldsymbol{\alpha}, t)\downarrow],$$

which suggests that *neither the graph nor the domain of convergence of a recursive partial functions with values in* $\mathcal{N}$ *need be semirecursive.* In fact, if we view (142) as a definition of a partial function $h : \mathbb{N} \rightharpoonup \mathcal{N}$, then

$$h(e) = \lambda(x)U(\mu y T_1(e, x, y))\downarrow \iff (\forall x)(\exists y)T_1(e, x, y),$$

so that by Proposition 5E.7, the domain of convergence of h is $\Pi^0_2 \setminus \Sigma^0_2$.

Lemma 5H.11. *The class of recursive partial functions with arguments in* $\mathcal{N}$ *is not closed under substitution.*

Proof. If $g(\alpha) = 0$, $h(e) = \lambda(x)U(\mu y T_1(e, x, y))$, and $f(e) = g(h(e))$, then $f : \mathbb{N} \rightharpoonup \mathbb{N}$,

$$f(e) = w \iff (\forall t)[\{e\}(t)\downarrow] \ \&\ w = 0,$$

and the graph of f is not semirecursive, so that f is not recursive. ⊣

However, $f(e)$ agrees with a recursive partial function (the constant 0) for values of e for which $h(e)\downarrow$; this is a general and useful fact:

Theorem 5H.12. (1) *Suppose* $g : \mathbb{N}^n \times \mathcal{N} \times \mathcal{N}^\nu \rightharpoonup \mathbb{N}$ *and* $h : \mathbb{N}^n \times \mathcal{N}^\nu \rightharpoonup \mathcal{N}$ *are recursive partial functions, and let*

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = g(\boldsymbol{x}, h(\boldsymbol{x}, \boldsymbol{\alpha}), \boldsymbol{\alpha});$$

then there exists a recursive partial function $\widetilde{f} : \mathbb{N}^n \times \mathcal{N}^\nu \rightharpoonup \mathbb{N}$ *such that*

$$\text{if } h(\boldsymbol{x}, \boldsymbol{\alpha})\downarrow, \text{ then } f(\boldsymbol{x}, \boldsymbol{\alpha}) = \widetilde{f}(\boldsymbol{x}, \boldsymbol{\alpha}).$$

(2) *If* $g(z_1, \dots, z_m), h_1(\boldsymbol{x}, \boldsymbol{\alpha}), \dots, h_m(\boldsymbol{x}, \boldsymbol{\alpha})$ *are recursive partial functions such that for* $i = 1, \dots, m$, *if* $h_i : \mathbb{N}^n \times \mathcal{N}^\nu \rightharpoonup \mathcal{N}$ *then* h_i *is total, then the substitution*

$$f(\boldsymbol{x}, \boldsymbol{\alpha}) = g(h_1(\boldsymbol{x}, \boldsymbol{\alpha}), \dots, h_m(\boldsymbol{x}, \boldsymbol{\alpha}))$$

is a recursive partial function.

Proof. (1) By the Normal Form Theorem 5H.9,

$$g(\boldsymbol{x}, \beta, \boldsymbol{\alpha}) = U(\mu t R(\boldsymbol{x}, \overline{\beta}(t), \overline{\boldsymbol{\alpha}}(t)))$$

with a recursive relation $R(\boldsymbol{x}, v, \vec{u})$. Let also

$$\widetilde{h}(t, \boldsymbol{x}, \boldsymbol{\alpha}) = \langle h(\boldsymbol{x}, \boldsymbol{\alpha})(0), \dots, h(\boldsymbol{x}, \boldsymbol{\alpha})(t-1)\rangle;$$

this is a recursive partial function, such that

$$\text{if } h(\boldsymbol{x}, \boldsymbol{\alpha}) = \beta, \text{ then } \widetilde{h}(t, \boldsymbol{x}, \boldsymbol{\alpha}) = \overline{\beta}(t).$$

Finally, put

$$\widetilde{f}(\boldsymbol{x}, \boldsymbol{\alpha}) = U(\mu t R(\boldsymbol{x}, \widetilde{h}(t, \boldsymbol{x}, \boldsymbol{\alpha}), \boldsymbol{x}, \boldsymbol{\alpha})), \overline{\boldsymbol{\alpha}}(t))).$$

Now this is a recursive partial function, and if $h(\boldsymbol{x}, \boldsymbol{\alpha}) = \beta$, then

$$\widetilde{f}(\boldsymbol{x}, \boldsymbol{\alpha}) = U(\mu t R(\boldsymbol{x}, \overline{\beta}(t), \boldsymbol{x}, \boldsymbol{\alpha})) = g(\boldsymbol{x}, h(\boldsymbol{x}, \boldsymbol{\alpha}), \boldsymbol{\alpha}),$$

as claimed.

(2) follows immediately from (1). ⊣

Corollary 5H.13. *The classes of semirecursive and recursive relations with arguments in Baire space are closed under substitution of total, recursive functions with values in $\mathcal{N}$.*

Among the most useful such substitutions are those which use the following codings of finite and infinite tuples of Baire points:

Definition 5H.14 (Sequence codings for Baire space)**.** We set

$$\langle \alpha_0, \dots, \alpha_{\nu-1} \rangle = \lambda(t) \begin{cases} \alpha_i(s), & \text{if } t = \langle i, s \rangle \text{ for some } i < \nu \text{ and some } s, \\ 0, & \text{otherwise,} \end{cases}$$

and similarly for an infinite sequence of Baire points,

$$\langle \alpha_0, \alpha_1, \dots \rangle = \lambda(t) \begin{cases} \alpha_i(s), & \text{if } t = \langle i, s \rangle \text{ for some } i \text{ and some } s, \\ 0, & \text{otherwise.} \end{cases}$$

We also set,

$$(\alpha)_i = \lambda(s)\alpha(\langle i, s \rangle).$$

Lemma 5H.15. (1) *The function*

$$(\alpha_0, \dots, \alpha_{\nu-1}) \mapsto \langle \alpha_0, \dots, \alpha_{\nu-1} \rangle,$$

is recursive and one-to-one on $\mathcal{N}^\nu \to \mathcal{N}$; and the function

$$(\alpha, i) \mapsto (\alpha)_i$$

is recursive and an inverse of the tuple functions, in the sense that

$$(\langle \alpha_0, \dots, \alpha_{n-1} \rangle)_i = \alpha_i \quad (i < n).$$

(2) *The function*

$$(\alpha_0, \alpha_1, \dots) \mapsto \langle \alpha_0, \alpha_1, \dots \rangle$$

is one-to-one on $\mathcal{N}^\infty \to \mathcal{N}$.

5H.16. The arithmetical hierarchy with arguments in Baire space. We can now define and establish the basic properties of the arithmetical hierarchy for relations with arguments in Baire space, exactly as we did for relations with arguments in $\mathbb{N}$ in Section 5E, starting with the Σ^0_1 relations on Baire space and using recursive functions with arguments and values in Baire space. We comment briefly on the changes that must be made, which involve only the results needed to justify the theorems.

The basic definition of the classes Σ^0_k, Π^0_k and Δ^0_k is exactly that in 5E.1, starting with the definition 5H.2 of semirecursive relations on Baire space. The canonical forms of these classes are those in 5E.2, whose Table we repeat to emphasize the form of the dependence on the Baire arguments when these are present, i.e., with $\nu \geq 1$:

$$\begin{array}{lcr}
\Sigma^0_1 & : & (\exists y)Q(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(y)) \\
\Pi^0_1 & : & (\forall y)Q(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(y)) \\
\Sigma^0_2 & : & (\exists y_1)(\forall y_2)Q(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(y_2), y_1) \\
\Pi^0_2 & : & (\forall y_1)(\exists y_2)Q(\boldsymbol{x}, , \overline{\boldsymbol{\alpha}}(y_2), y_1) \\
\Sigma^0_3 & : & (\exists y_1)(\forall y_2)(\exists y_3)Q(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(y_3), y_2, y_3) \\
 & \vdots &
\end{array}$$

The closure properties are again those in Theorem 5A.7, with the closure under substitutions of total recursive functions with values either in $\mathbb{N}$ or in $\mathcal{N}$ depending on Corollary 5H.13, and the quantifier contractions justified by the sequence codings in 5H.14 and 5H.15. Finally, the Enumeration and Hierarchy Theorems 5E.5 are proved as before, starting with Theorem 5H.6 now, and the proper inclusions diagram in that theorem still holds, with the "properness" witnessed by the same relations on $\mathbb{N}$.

5H.17. Baire codes of subsets of $\mathbb{N}$ and relations on $\mathbb{N}$. With each Baire point γ, we associate the set of natural numbers

(150) $$A_\gamma = \{s \in \mathbb{N} \mid \gamma(s) = 1\},$$

and for each $n \geq 2$, the n-ary relation

(151) $$R^n_\gamma(x_1, \dots, x_n) \iff \gamma(\langle x_1, \dots, x_n\rangle) = 1;$$

we say that γ *is a code of* A if $A_\gamma = A$, and *a code of* $R \subseteq \mathbb{N}^n$ if $R = R^n_\gamma$. If $n = 2$, we often use "infix notation",

$$xR_\gamma y \iff R_\gamma(x, y) \iff \gamma(\langle x, y\rangle) = 1.$$

These trivial codings allow us to classify subsets of $\mathcal{N}$ and relations on $\mathcal{N}$ in the arithmetical hierarchy, as in the following, simple example.

Lemma 5H.18. *The set of codes of linear orderings*

(152) $$\mathrm{LO} = \{\gamma \mid \gamma \textit{ is a code of a linear ordering (of a subset of } \mathbb{N})\}$$

is $\Pi^0_1 \setminus \Sigma^0_1$.

Proof. To simplify notation, set

$$x \leq_\gamma y \iff \gamma(\langle x, y\rangle) = 1, \quad x \in D_\gamma \iff x \leq_\gamma x,$$

and compute:

$$\begin{aligned}\gamma \in \mathrm{LO} \iff & \leq_\gamma \text{ is a linear ordering of } D_\gamma \\ \iff & (\forall x, y)[x \leq_\gamma y \Longrightarrow [x \in D_\gamma \;\&\; y \in D_\gamma]] \\ & \quad \& \; (\forall x, y)[[x \leq_\gamma y \;\&\; y \leq_\gamma x] \Longrightarrow x = y] \\ & \quad \& \; (\forall x, y, z)[[x \leq_\gamma y \;\&\; y \leq_\gamma z] \Longrightarrow x \leq_\gamma z] \\ & \quad \& \; (\forall x, y)[[x \in D_\gamma \;\&\; y \in D_\gamma] \Longrightarrow x \leq_\gamma y \vee y \leq_\gamma x].\end{aligned}$$

For the converse, suppose that

$$P(x) \iff (\forall u)R(x, u)$$

with $R(x, u)$ recursive, and let

$$f^*(x, t) = \begin{cases} 1, & \text{if } R(x, \min((t)_0, (t)_1)) \;\&\; (t)_0 \leq (t)_1, \\ 0, & \text{if } R(x, \min((t)_0, (t)_1)) \;\&\; (t)_0 > (t)_1, \\ 1, & \text{if } \neg R(x, \min((t)_0, (t)_1)). \end{cases}$$

The function $f^*(x, t)$ is recursive and total, and hence so is the function

$$f(x) = \lambda(t) f^*(x, t);$$

moreover, if $(\forall t)R(x, t)$, then

$$f(x)(\langle u, v\rangle) = f^*(x, \langle u, v\rangle) = \begin{cases} 1, & \text{if } u \leq v, \\ 0, & \text{otherwise,} \end{cases}$$

so that $f(x) \in \mathrm{LO}$, in fact $f(x)$ is a code of the natural ordering on $\mathbb{N}$. On the other hand, if, for some t, $\neg R(x, t)$, then

$$f(x)(\langle t, t+1\rangle) = f(x)(\langle t+1, t\rangle) = 1, \qquad \text{i.e., } t \leq_{f(x)} (t+1) \;\&\; (t+1) \leq_{f(x)} t,$$

so that $f(x) \notin \mathrm{LO}$. This establishes the reduction.

$$P(x) \iff (\forall u)R(x, u) \iff f(x) \in \mathrm{LO}.$$

It follows that if LO were Σ^0_1, then every Π^0_1 relation on $\mathbb{N}$ would be in Σ^0_1, which it is not, and hence LO is not Σ^0_1. ⊣

5I. The analytical hierarchy

Once we have relations with arguments in Baire space, we can apply quantification over $\mathcal{N}$ on them to define more complex (and more interesting) relations. The resulting *analytical hierarchy* resembles in structure the arithmetical structure, which it extends, but it contains many of the fundamental relations of analysis and set theory.

Definition 5I.1. The *Kleene classes* of relations Σ^1_k, Π^1_k, Δ^1_k with arguments in $\mathbb{N}$ and $\mathcal{N}$ are defined recursively, for $k \geq 0$, as follows:

$$\Pi^1_0 = \Pi^0_1 : \text{the negations of semirecursive relations}$$

$$\Sigma^1_{k+1} = \exists^{\mathcal{N}}\Pi^1_k : \text{the relations which satisfy an equivalence of the form}$$

$$P(\boldsymbol{x}, \boldsymbol{\alpha}) \iff (\exists\beta)Q(\boldsymbol{x}, \boldsymbol{\alpha}, \beta),$$

$$\text{where } Q(\boldsymbol{x}, \boldsymbol{\alpha}, \beta) \text{ is } \Pi^1_k$$

$$\Pi^1_k = \neg\Sigma^1_k : \text{the negations (complements) of relations in } \Sigma^1_k$$

$$\Delta^1_k = \Sigma^1_k \cap \Pi^1_k : \text{ the relations which are both } \Sigma^1_k \text{ and } \Pi^1_k.$$

A set of numbers $A \subseteq \mathbb{N}$ or of Baire points $A \subseteq \mathcal{N}$ is in one of these classes Γ if the relation $x \in A$ or $\alpha \in A$ is in Γ.

5I.2. Canonical forms. Using the canonical form for Σ^0_1 relations in (2) of Lemma 5H.4, we obtain immediately the following canonical forms for the Kleene classes, (with $k \geq 1$), where $R(\boldsymbol{x}, \vec{u}, v)$ is recursive on $\mathbb{N}$ and monotone in $\vec{u}, v$:

$$\begin{array}{ll}
\Pi^1_1 & : \quad (\forall\beta)(\exists t)R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t), \overline{\beta}(t)) \\
\Sigma^1_1 & : \quad (\exists\beta)(\forall t)R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t), \overline{\beta}(t)) \\
\Pi^1_2 & : \quad (\forall\beta_1)(\exists\beta_2)(\forall t)R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t), \overline{\beta}_1(t), \overline{\beta}_2(t)) \\
\Sigma^1_2 & : \quad (\exists\beta_1)(\forall\beta_2)(\exists t)R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t), \overline{\beta}_1(t), \overline{\beta}_2(t)) \\
\Pi^1_3 & : \quad (\forall\beta_1)(\exists\beta_2)(\forall\beta_3)(\exists t)R(\boldsymbol{x}, \overline{\boldsymbol{\alpha}}(t), \overline{\beta}_1(t), \overline{\beta}_2(t), \overline{\beta}_3(t)) \\
 & \vdots
\end{array}$$

It is worth singling out the form of Π^1_1 subsets of $\mathbb{N}$ and $\mathcal{N}$ which include some of the most interesting examples:

$$(\Pi^1_1) \quad x \in A \iff (\forall\beta)(\exists t)R(x, \overline{\beta}(t)),$$

$$\alpha \in A \iff (\forall\beta)(\exists t)R(\overline{\alpha}(t), \overline{\beta}(t)),$$

Theorem 5I.3. (1) *For each $k \geq 1$, the classes Σ^1_k, Π^1_k, and Δ^1_k are closed for (total) recursive substitutions with values in $\mathbb{N}$ or $\mathcal{N}$, and for the operations &, $\vee$, $\exists_\leq$, $\forall_\leq$, $\exists^{\mathbb{N}}$ and $\forall^{\mathbb{N}}$. In addition*:

- *Each Δ^1_k is closed for negation $\neg$.*
- *Each Σ^1_k is closed for $\exists^{\mathcal{N}}$, existential quantification over $\mathcal{N}$.*
- *Each Π^1_k is closed for $\forall^{\mathcal{N}}$, universal quantification over $\mathcal{N}$.*

(2) *Every arithmetical relation is Δ^1_1.*

(3) *For each $k \geq 1$,*

$$\Sigma^1_k \subsetneq \Delta^1_{k+1}, \tag{153}$$

and hence the Kleene classes satisfy the following diagram of proper inclusions:

$$\begin{array}{ccccccccccccc}
 & & \Sigma^1_1 & & & & \Sigma^1_2 & & & & \Sigma^1_3 & & \\
 & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & \\
\bigcup_k \Sigma^0_k \subseteq \Delta^1_1 & & & & \Delta^1_2 & & & & \Delta^1_3 & & & & \cdots \\
 & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & & \subsetneq & \\
 & & \Pi^1_1 & & & & \Pi^1_2 & & & & \Pi^1_3 & &
\end{array}$$

Proof. (1) The closure of all Kleene classes under total, recursive substitutions follows from the canonical forms and the closure of Σ^0_1 and Π^0_1 under total recursive substitutions, Corollary 5H.13. The remaining closure properties are proved by induction on $k \geq 1$, using the recursiveness of the projection functions and the function

$$\gamma \mapsto \gamma' = \lambda(t)\gamma(t);$$

the known closure properties of Π^0_1; and, to contract quantifiers, the following equivalences and their duals, where we abbreviate $\boldsymbol{z} = \boldsymbol{x}, \boldsymbol{\alpha}$.

(E1) $(\exists\beta)P(\boldsymbol{z},\beta) \vee (\exists\beta)Q(\boldsymbol{z},\beta) \iff (\exists\beta)[P(\boldsymbol{z},\beta) \vee Q(\boldsymbol{z},\beta)]$

(E2) $(\exists\beta)P(\boldsymbol{z},\beta)\ \&\ (\exists\beta)Q(\boldsymbol{z},\beta) \iff (\exists\gamma)[P(\boldsymbol{z},(\gamma)_0)\ \&\ Q(\boldsymbol{z},(\gamma)_1)]$

(E3) $(\exists s \leq t)(\exists\beta)P(\boldsymbol{z},s,\beta) \iff (\exists\beta)(\exists s \leq t)P(\boldsymbol{z},s,\beta)$

(E4) $(\forall s \leq t)(\exists\beta)P(\boldsymbol{z},s,\beta) \iff (\exists\gamma)(\forall s \leq t)P(\boldsymbol{z},s,(\gamma)_s)$

(E5) $(\exists s)(\exists\beta)P(\boldsymbol{z},s,\beta) \iff (\exists\beta)(\exists s)P(\boldsymbol{z},s,\beta)$

(E6) $(\forall s)(\exists\beta)P(\boldsymbol{z},s,\beta) \iff (\exists\gamma)(\forall s)P(\boldsymbol{z},s,(\gamma)_s)$

(E7) $(\exists\delta)(\exists\beta)P(\boldsymbol{z},\delta,\beta) \iff (\exists\gamma)P(\boldsymbol{z},(\gamma)_0,(\gamma)_1)$

These are all either trivial, or direct expressions of the countable Axiom of Choice for Baire space (E6).

In some more detail:

(1a) The closure properties of Σ^1_1 follow from those of Π^0_1 and (E1)-(E7). To show closure under $\forall^{\mathbb{N}}$, for example, suppose

$$P(\boldsymbol{z},t) \iff (\exists\beta)Q(\boldsymbol{z},\beta,t) \quad \text{with } Q \in \Pi^0_1,$$

and compute:

$$\begin{aligned}(\forall t)P(\boldsymbol{z},t) &\iff (\forall t)(\exists\beta)Q(\boldsymbol{z},\beta,t)\\ &\iff (\exists\gamma)(\forall t)Q(\boldsymbol{z},(\gamma)_t,t) \text{by (E6)}.\end{aligned}$$

This is enough, because $Q(\boldsymbol{z},(\gamma)_t,t)$ is Π^0_1 by the closure of this class under recursive substitutions.

(1b) The closure properties of Π^1_k follow from those of Σ^1_k taking negations and pushing the negation operator through the quantifier prefix.

(1c) The closure properties of Σ^1_{k+1} follow from those of Π^1_k using (E1)-(E7).

(2) follows from (1), since $\Delta^0_1 \subseteq \Delta^1_1$ and Δ^1_1 is closed under both number quantifiers. (And we will see in 5I.5 that the arithmetical relations are contained properly in Δ^1_1.)

(3) We notice first that the non-strict version of the diagram (with $\subseteq$ in place of $\subsetneq$) is trivial, using dummy quantification, and closure under recursive substitutions, e.g.,

$$(\exists\beta)P(\boldsymbol{z},\beta) \iff (\exists\beta)(\forall\alpha)P(\boldsymbol{z},\beta) \iff (\forall\alpha)(\exists\beta)P(\boldsymbol{z},\beta).$$

To show that the inclusions are strict, we need to define enumerating (universal) sets

$$\widetilde{S}^1_{k,n,\nu} \text{ for } \Sigma^1_k \text{ and } \widetilde{P}^1_{k,n,\nu} \text{ for } \Pi^1_k.$$

We start with the fact that the relation

$$\widetilde{P}^0_{n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}) \iff (\forall t)\neg T^r_{n,\nu}(e,\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t)) \tag{154}$$

enumerates all Π^0_1 relations with arguments $\boldsymbol{x},\boldsymbol{\alpha}$, by (144) in Theorem 5H.6, and set recursively:

$$\begin{aligned}
\widetilde{S}^1_{1,n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}) &\iff (\exists\beta)(\forall t)\neg T^r_{n,\nu+1}(e,\boldsymbol{x},\overline{\boldsymbol{\alpha}}(t),\overline{\beta}(t)),\\
\widetilde{P}^1_{k,n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}) &\iff \neg\widetilde{S}^1_{k,n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha})\\
\widetilde{S}^1_{k+1,n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}) &\iff (\exists\beta)\widetilde{P}^1_{k,n,\nu+1}(e,\boldsymbol{x},\boldsymbol{\alpha},\beta).
\end{aligned}$$

It is easy to verify (chasing the definitions) that a relation $R(\boldsymbol{x},\boldsymbol{\alpha})$ is Σ^1_k if and only if there is some e such that

$$R(\boldsymbol{x},\boldsymbol{\alpha}) \iff \widetilde{S}^1_{k,n,\nu}(e,\boldsymbol{x},\boldsymbol{\alpha}),$$

and then, as usual, the diagonal relation

$$D(x) \iff \widetilde{S}^1_{k,1,0}(x,x)$$

is in $\Sigma^1_k \setminus \Pi^1_k$. ⊣

We now place in the analytical hierarchy some important relations on Baire space, starting with the basic *satisfaction relation* on (codes of) structures.

5I.4. Codes of structures. Consider (for simplicity) $\mathbb{FOL}(\tau)$, where the signature τ has K relation symbols $P_1,\dots,P_K$ where P_i is n_i-ary. We code τ by its *characteristic*

$$u = \langle n_1,\dots,n_K\rangle.$$

With each $\alpha \in \mathcal{N}$ and each u, we associate the tuple

$$\mathbf{A}(u,\alpha) = (A_\alpha, R_{1,\alpha},\dots,R_{K,\alpha}),$$

where

$$A_\alpha = \{n \in \mathbb{N} \mid (\alpha)_0(n) = 1\},$$
$$R_{i,\alpha}(x_1, \dots, x_{n_i}) \iff x_1, \dots, x_{n_i} \in A \;\&\; (\alpha)_i(\langle x_1, \dots, x_{n_i}\rangle) = 1.$$

This is a structure when $A_\alpha \neq \emptyset$, and it is convenient to insure this by demanding that $0 \in A_\alpha$; and so the semirecursive relation

$$\mathrm{Str}(u, \alpha) \iff 0 \in A_\alpha \iff (\alpha)_0(0) = 1$$

determines which Baire points code structures. Let

$$\begin{aligned}\mathrm{Assgn}(u, x, \alpha) &\iff x \text{ codes an (ultimately 0) assignment into } A_\alpha\\ &\iff \mathrm{Str}(u, \alpha) \;\&\; (\forall i < \mathrm{lh}(x))[(x)_i \in A_\alpha];\end{aligned}$$

this, too, is a semirecursive relation. Finally, using the codings of Section 4A, we set

$$\begin{aligned}\text{(155)}\qquad \mathrm{Sat}(u, \alpha, m, x) \iff\ & \mathrm{Str}(u, \alpha) \;\&\; \mathrm{Assgn}(u, x, \alpha)\\ &\& \; m \text{ codes a formula } \phi \text{ of } \mathbb{FOL}(\tau)\\ &\& \; \mathbf{A}(u, \alpha), (x)_0, (x)_1, \dots \models \phi,\end{aligned}$$

This relation codes the basic satisfaction relation between structures (on subsets of $\mathbb{N}$), assignments and formulas.

Theorem 5I.5. (1) *The relation* $\mathrm{Sat}(u, \alpha, m, x)$ *is* Δ^1_1.

(2) *The set* Truth *of codes of true arithmetical sentences is* Δ^1_1, *and so the arithmetical relations are properly contained in* Δ^1_1.

Proof. (1) Let

$$\begin{aligned}&P(u, \alpha, \beta)\\ &\quad\iff (\forall m, x)[\beta(\langle m, x\rangle) \leq 1 \;\&\; \beta(\langle m, x\rangle) = 1 \iff \mathrm{Sat}(u, \alpha, m, x)];\end{aligned}$$

the equivalence determines β completely, once u and α are fixed, and so

$$\begin{aligned}\mathrm{Sat}(u, \alpha, m, x) &\iff (\exists \beta)[P(u, \alpha, \beta) \;\&\; \beta(\langle m, x\rangle) = 1]\\ &\iff (\forall \beta)[P(u, \alpha, \beta) \Longrightarrow \beta(\langle m, x\rangle) = 1].\end{aligned}$$

Thus the proof will be complete once we show that $P(u, \alpha, \beta)$ is arithmetical, which is not too hard to do, since for it to hold, β must satisfy the "Tarski conditions" for satisfaction: $\beta(\langle m, x\rangle)$ must give the correct value when m codes a prime formula, and for complex formulas, the correct value of $\beta(\langle m, x\rangle)$ can be computed in terms of $\beta(\langle s, y\rangle)$ for codes s of shorter formulas.

(2) follows by first translating the formulas of number theory to $\mathbb{FOL}(\tau)$ with a signature τ which has only relation symbols (for the graphs of $0, S, +$ and $\cdot$), and then reformulating questions of truth to quries about satisfaction—which for sentences are one and the same thing.) ⊣

Next we turn to the classification of relation on countable ordinal numbers via their Baire codes. We set

(156) $$\mathrm{WO} = \{\alpha \in \mathrm{LO} \mid \leq_\alpha \text{ is a wellordering}\},$$

where the set LO of codes of linear orderings is defined in (152), and for each $\alpha \in \mathrm{WO}$, we set

(157) $$|\alpha| = \text{the ordinal similar with } \leq_\alpha \quad (\alpha \in \mathrm{WO}).$$

Each $|\alpha|$ is a countable ordinal, and each countable ordinal is $|\alpha|$ with some (in fact many) $\alpha \in \mathrm{WO}$.

Theorem 5I.6. *The set* WO *of ordinal codes is* Π^1_1*. Moreover, there are relations* $\leq_\Pi$, $\leq_\Sigma$ *in* Π^1_1 *and* Σ^1_1 *respectively, such that*

if $\beta \in \mathrm{WO}$, *then for all* α,

$$\alpha \leq_\Pi \beta \iff \alpha \leq_\Sigma \beta \iff [\alpha \in \mathrm{WO} \;\&\; |\alpha| \leq |\beta|].$$

Proof. To see that WO is Π^1_1, we compute:

$$\alpha \in \mathrm{WO} \iff \alpha \in \mathrm{LO}$$
$$\& \; (\forall\beta)\Big[(\forall t)[\beta(t+1) \leq_\alpha \beta(t)] \Longrightarrow (\exists t)[\beta(t+1) = \beta(t)]\Big].$$

To prove the second assertion, take first

$$\alpha \leq_\Sigma \beta \iff \alpha \in \mathrm{LO} \;\&\; (\exists\gamma)[\gamma \text{ maps } \leq_\alpha \text{ into } \leq_\beta \text{ in a one-to-one order-preserving manner}]$$
$$\iff \alpha \in \mathrm{LO} \;\&\; (\exists\gamma)(\forall n)(\forall m)[n <_\alpha m \Longrightarrow \gamma(n) <_\beta \gamma(m)].$$

It is immediate that $\leq_\Sigma$ is Σ^1_1 and for $\beta \in \mathrm{WO}$,

$$\alpha \leq_\Sigma \beta \iff [\alpha \in \mathrm{WO} \;\&\; |\alpha| \leq |\beta|].$$

For the relation $\leq_\Pi$, take

$$\alpha \leq_\Pi \beta \iff \alpha \in \mathrm{WO} \;\&\; \text{there is no order-preserving map of } \leq_\beta \text{ onto a proper initial segment of } \leq_\alpha$$
$$\iff \alpha \in \mathrm{WO}$$
$$\& \; (\forall\gamma)\neg(\exists k)(\forall n)(\forall m)\big[n \leq_\beta m \iff [\gamma(n) \leq_\alpha \gamma(m) <_\alpha k]\big],$$

where of course we abbreviate

$$s <_\alpha t \iff s \leq_\alpha t \;\&\; s \neq t. \qquad \dashv$$

That WO is not Σ^1_1 is a consequence of the following, basic result of definability theory, established (in various forms) by Lusin-Sierpinski and Kleene.

Theorem 5I.7 (The Basic Representation Theorem for Π^1_1). *If $P(\boldsymbol{x}, \boldsymbol{\alpha})$ is Π^1_1, then there exists a total recursive function $f : \mathbb{N}^n \times \mathcal{N}^\nu \to \mathcal{N}$, that for all $\boldsymbol{x}, \boldsymbol{\alpha}$, $f(\boldsymbol{x}, \boldsymbol{\alpha}) \in \mathrm{LO}$, and*

$$P(\boldsymbol{x}, \boldsymbol{\alpha}) \iff f(\boldsymbol{x}, \boldsymbol{\alpha}) \in \mathrm{WO}. \tag{158}$$

Proof. We set $\boldsymbol{z} = \boldsymbol{x}, \boldsymbol{\beta}$ to save some typing, and by 5I.2 we choose a recursive and monotone in u relation $R(\boldsymbol{z}, u)$ such that

$$P(\boldsymbol{z}) \iff (\forall \beta)(\exists t) R\big(\boldsymbol{z}, \overline{\beta}(t)\big).$$

For each $\boldsymbol{z}$, put

$$T(\boldsymbol{z}) = \{(u_0, \dots, u_{t-1}) \mid \neg R(\boldsymbol{z}, \langle u_0, \dots, u_{t-1} \rangle)\}$$

so that $T(\boldsymbol{z})$ is a tree on $\mathbb{N}$ (by the monotonicity or R) and clearly

$$P(\boldsymbol{z}) \iff T(\boldsymbol{z}) \text{ is wellfounded.}$$

What we must do is replace $T(\boldsymbol{z})$ by a linear ordering on a subset of $\mathbb{N}$ which will be wellfounded precisely when $T(\boldsymbol{z})$ is. Put

$$\begin{aligned}
(v_0, \dots, &v_{s-1}) >^{\boldsymbol{z}} (u_0, \dots, u_{t-1}) \\
&\iff (v_0, \dots, v_{s-1}), (u_0, \dots, u_{t-1}) \in T(\boldsymbol{z}) \\
&\qquad \& \Big[v_0 > u_0 \vee [v_0 = u_0 \ \& \ v_1 > u_1] \\
&\qquad\quad \vee [v_0 = u_0 \ \& \ v_1 = u_1 \ \& \ v_2 > u_2] \\
&\qquad\quad \vee \cdots \\
&\qquad\quad \vee [v_0 = u_0 \ \& \ v_1 = u_1 \ \& \ \cdots \ \& \ v_{s-1} = u_{s-1} \ \& \ s < t] \Big]
\end{aligned}$$

where $>$ on the right is the usual "greater than" in $\mathbb{N}$.

It is immediate that if $(v_0, \dots, v_{s-1})$, $(u_0, \dots, u_{t-1})$ are both in $T(\boldsymbol{z})$ and $(v_0, \dots, v_{s-1})$ is an initial segment of $(u_0, \dots, u_{t-1})$, then $(v_0, \dots, v_{s-1}) >^{\boldsymbol{z}} (u_0, \dots, u_{t-1})$; thus if $T(\boldsymbol{z})$ has an infinite branch, then $>^{\boldsymbol{z}}$ has an infinite descending chain.

Assume now that $>^{\boldsymbol{z}}$ has an infinite descending chain, say

$$v^0 >^{\boldsymbol{z}} v^1 >^{\boldsymbol{z}} v^2 >^{\boldsymbol{z}} \cdots,$$

where

$$v^i = (v^i_0, v^i_1, \dots, v^i_{s_i - 1}),$$

and consider the following array:

$$\begin{aligned} v^0 &= (v^0_0, v^0_1, \dots, v^0_{s_0-1}) \\ v^1 &= (v^1_0, v^1_1, \dots, v^1_{s_1-1}) \\ \cdots & \quad \cdots \\ v^i &= (v^i_0, v^i_1, \dots, v^i_{s_i-1}) \\ \cdots & \quad \cdots \end{aligned}$$

The definition of $>^{\boldsymbol{z}}$ implies immediately that

$$v^0_0 \geq v^1_0 \geq v^2_0 \geq \cdots,$$

i.e., the first column is a non-increasing sequence of natural numbers. Hence after a while they all are the same, say

$$v^i_0 = k_0 \quad \text{for } i \geq i_0.$$

Now the second column is non-increasing below level i_0, so that for some pair i_1, k_1,

$$v^i_1 = k_1 \quad \text{for } i \geq i_1.$$

Proceeding in the same way we find an infinite sequence

$$k_0, k_1, \dots$$

such that for each s, $(k_0, \dots, k_{s-1}) \in T(\boldsymbol{z})$, so $T(\boldsymbol{z})$ is not wellfounded. Thus we have shown,

$$\begin{aligned} P(\boldsymbol{z}) &\iff T(\boldsymbol{z}) \text{ is wellfounded} \\ &\iff >^{\boldsymbol{z}} \text{ has no infinite descending chains.} \end{aligned}$$

Finally put

$$\begin{aligned} u \leq^{\boldsymbol{z}} v \iff (\exists t \leq u)(\exists s \leq v)\Big[&\mathrm{Seq}(u) \ \&\ \mathrm{lh}(u) = t \ \&\ \mathrm{Seq}(v) \ \&\ \mathrm{lh}(v) = s \\ &\&\ \big[u = v \vee \big((v)_0, \dots, (v)_{s-1}\big) >^{\boldsymbol{z}} \big((u)_0, \dots, (u)_{t-1}\big)\big]\Big] \end{aligned}$$

and notice that $\leq^{\boldsymbol{z}}$ is always a linear ordering, and

$$P(\boldsymbol{z}) \iff \leq^{\boldsymbol{z}} \text{ is a wellordering.}$$

Moreover, the relation

$$P(\boldsymbol{z}, u, v) \iff u \leq^{\boldsymbol{z}} v$$

is easily recursive. The proof is completed by taking

$$f(\boldsymbol{z})(n) = \begin{cases} 1, & \text{if } (n)_0 \leq^{\boldsymbol{z}} (n)_1, \\ 0, & \text{otherwise.} \end{cases} \qquad \dashv$$

Corollary 5I.8. *The set* WO *of ordinal codes is not* Σ^1_1.

5J. Problems for Chapter 5

Problem x5.1. Prove that if $R(x_1, \ldots, x_n)$ is a recursive relation, then there exists a formula $\mathbf{R}(v_1, \ldots, v_n)$ in the language of arithmetic such that

$$R(x_1, \ldots, x_n) \Longrightarrow \mathsf{Q} \vdash \mathbf{R}(\Delta x_1 \ldots, \Delta x_n)$$
$$\text{and } \neg R(x_1, \ldots, x_n) \Longrightarrow \mathsf{Q} \vdash \neg\mathbf{R}(\Delta x_1 \ldots, \Delta x_n).$$

Problem x5.2. Prove that every axiomatizable, complete theory is decidable.

Problem x5.3. Show that the class of recursive partial functions is *uniformly* closed under definition by primitive recursion in the following, precise sense: there is a primitive recursive function $u^n(e, m)$, such that if $f(y, \vec{x})$ is defined by the primitive recursion

$$f(0, \vec{x}) = \varphi_e(\vec{x}), \quad f(y + 1, \vec{x}) = \varphi_m(f(y, \vec{x}), y, \vec{x}),$$

then $f(y, \vec{x}) = \{u^n(e, m)\}(y, \vec{x})$.

Problem x5.4. Define a total, recursive, one-to-one function $u^n(e, i)$, such that for all $e, i, \vec{x}$,

$$\{u^n(e, i)\}(\vec{x}) = \{e\}(\vec{x}).$$

(In particular, each recursive partial function has, effectively, an infinite number of distinct codes.)

Problem x5.5. Show that the partial function

$$f(e, u) = \langle \varphi_e((u)_0), \varphi_e((u)_1), \ldots, \varphi_e((u)_{\mathrm{lh}(u) \dot{-} 1}) \rangle$$

is recursive.

Problem x5.6 (Craig's Lemma)**.** Show that a theory T has a primitive recursive set of axioms if and only if it has an r.e. set of axioms.

Problem x5.7*. Prove that there is a recursive relation $R(x)$ which is not primitive recursive.

Problem x5.8. Suppose $R(\vec{x}, w)$ is a semirecursive relation such that for each $\vec{x}$ there exist at least two distinct numbers $w_1 \neq w_2$ such that $R(\vec{x}, w_1)$ and $R(\vec{x}, w_2)$. Prove that there exist two, total recursive functions $g(\vec{x})$ and $h(\vec{x})$, such tht for all $\vec{x}$,

$$R(\vec{x}, g(\vec{x})) \ \& \ R(\vec{x}, h(\vec{x})) \ \& \ g(\vec{x} \neq h(\vec{x}).$$

Problem x5.9*. Suppose $R(\vec{x}, w)$ is a semirecursive relation such that for each $\vec{x}$, there exists at least one w such that $R(\vec{x}, w)$.

(a) Prove that there is a total recursive function $f(n, \vec{x})$ such that

$$(*) \qquad R(\vec{x}, w) \iff (\exists n)[w = f(n, \vec{x})].$$

(b) Prove that if (in addition), for each $\vec{x}$, there exist infinitely many w such that $R(\vec{x}, w)$, then there exists a total, recursive $f(n, \vec{x})$ which satisfies $(*)$ and which is one-to-one, i.e.,

$$m \neq n \Longrightarrow f(m, \vec{x}) \neq f(n, \vec{x}).$$

Problem x5.10. Prove that a relation $P(\vec{x})$ is Σ^0_1 if and only if it is definable by a Σ_1 formula, in the sense of Definition 4C.11.

Problem x5.11. Show that there is a recursive, partial function $f(e)$ such that

$$W_e \neq \emptyset \Longrightarrow [f(e)\downarrow \ \& \ f(e) \in W_e].$$

Problem x5.12. Prove or give a counterexample to each of the following propositions:

(a) There is a total recursive function $u_1(e, m)$ such that for all e, m,

$$W_{u_1(e,m)} = W_e \cup W_m.$$

(b) There is a total recursive function $u_2(e, m)$ such that for all e, m,

$$W_{u_2(e,m)} = W_e \cap W_m.$$

(c) There is a total recursive function $u_3(e, m)$ such that for all e, m,

$$W_{u_3(e,m)} = W_e \setminus W_m.$$

Problem x5.13. Prove or give a counterexample to each of the following propositions, where $f : \mathbb{N} \to \mathbb{N}$ is a total recursive function and

$$f[A] = \{f(x) \mid x \in A\}, \quad f^{-1}[A] = \{x \mid f(x) \in A\}.$$

(a) If A is recursive, then $f[A]$ is also recursive.
(b) If A is r.e., then $f[A]$ is also r.e.
(c) If A is recursive, then $f^{-1}[A]$ is also recursive.
(d) If A is r.e., then $f^{-1}[A]$ is also r.e.

Problem x5.14. Prove that there is a total recursive function $u(e, m)$ such that

$$W_{u(e,m)} = \{x + y \mid x \in W_e \ \& \ y \in W_m\}.$$

Problem x5.15. Prove that every infinite r.e. set A has an infinite recursive subset.

Problem x5.16. (The Reduction Property of r.e. sets.) Prove that for every two r.e. sets A, B, there exist r.e. sets A^*, B^* with the following properties:

$$A^* \subseteq A, \quad B^* \subseteq B, \quad A \cup B = A^* \cup B^*, \quad A^* \cap B^* = \emptyset.$$

Problem x5.17. (The Separation Property for r.,e. complements.) Prove that if A and B are disjoint sets whose complements are r.e., then there exists a recursive set C such that

$$A \subseteq C, \quad C \cap B = \emptyset.$$

Problem x5.18. (Recursively inseparable r.e. sets.) Prove that there exist two disjoint r.e. sets A and B such that there is no recursive set C satisfying

$$A \subseteq C, \quad C \cap B = \emptyset.$$

Problem x5.19. Prove that for every two r.e. sets A, B, there is a formula $\phi(x)$ so that *whenever* $x \in (A \cup B)$,

$$\mathsf{Q} \vdash \phi(\mathbf{x}) \implies x \in A, \tag{159}$$

$$\mathsf{Q} \vdash \neg\phi(\mathbf{x}) \implies x \in B, \tag{160}$$

$$\mathsf{Q} \vdash \phi(\mathbf{x}) \ \ \textit{or} \ \ \mathsf{Q} \vdash \neg\phi(\mathbf{x}) \tag{161}$$

Problem x5.20. Show that if A is simple and B is infinite r.e., then the intersection $A \cap B$ is infinite.

Problem x5.21*.** Show that the intersection of two simple sets is simple.

Problem x5.22. Prove or give a counterexample:

(a) For each infinite r.e. set A, there is a total, recursive function $f(x)$ such that for each x,

$$f(x) > x \ \& \ f(x) \in A.$$

(b) (a) For each r.e. set A with infinite complement, there is a total, recursive function $f(x)$ such that for each x,

$$f(x) > x \ \& \ f(x) \notin A.$$

Problem x5.23*.** Prove that if Q is interpretable in a consistent, axiomatizable theory T, then the set

$$\#T = \{\#\theta \mid \theta \text{ is a sentence and } T \vdash \theta\}$$

of (codes of) theorems of T is creative.

Problem x5.24. Prove that there is some number z such that

$$W_z = \{z, z+1, \dots\} = \{x \mid x \geq z\}.$$

Problem x5.25. Prove that for some number t and all x, $\varphi_t(x) = t + x$.

Problem x5.26. Prove that for each total, recursive function $f(x)$ one of the following holds:

(a) There is a number z such that $f(z)$ is odd and for all x,

$$\varphi_z(x) = f(z + x);$$

or

(b) there is a number w such that $f(w)$ is even and for all x,

$$\varphi_w(x) = f(2w + x + 1).$$

Problem x5.27. Prove or give a counterexample: for each total, recursive function $f(x)$, there is some z such that

$$W_{f(z)} = W_z.$$

Problem x5.28. Prove or give a counterexample: for every total, recursive function $f(x)$, there is a number z such that for all t,

$$\varphi_{f(z)}(t) = \varphi_z(t).$$

Problem x5.29. (a) Prove that for every total, recursive function $f(x)$, there is a number z such that

$$W_z = \{f(z)\}.$$

(b) Prove that there is some number z such that

$$\varphi_z(z)\!\downarrow \text{ and } W_z = \{\varphi_z(z)\}.$$

Problem x5.30. Prove that for every arithmetical relation $P(\vec{x})$, there is a 1-1, total recursive function $f : \mathbb{N}^n \to \mathbb{N}$ such that

$$P(\vec{x}) \iff f(\vec{x}) \in \mathrm{Truth}^{\mathbf{N}};$$

infer Tarski's Theorem 4A.5, that $\mathrm{Truth}^{\mathbf{N}}$ is not arithmetical.

Problem x5.31. Classify in the arithmetical hierarchy the set

$$A = \{e \mid W_e \subseteq \{0, 1\}\}.$$

Problem x5.32. Classify in the arithmetical hierarchy the set

$$A = \{e \mid W_e \text{ is finite and non-empty}\}.$$

Problem x5.33. Classify in the arithmetical hierarchy the set

$$B = \{x \mid \text{there are infinitely many twin primes } p \geq x\},$$

where p is a twin prime if both p and $p + 2$ are prime numbers.

Problem x5.34. Classify in the arithmetical hierarchy the relation

$$\begin{aligned} Q(e, m) &\iff \varphi_e \sqsubseteq \varphi_m \\ &\iff (\forall x)(\forall w)[\varphi_e(x) = w \Longrightarrow \varphi_m(x) = w]. \end{aligned}$$

Problem x5.35. Classify in the arithmetical hierarchy the set

$$A = \{e \mid W_e \text{ has at least } e \text{ members}\}.$$

Problem x5.36. Classify in the arithmetical hierarchy the set

$$B = \{e \mid \text{ for some } w \text{ and all } x, \text{ if } \varphi_e(x)\downarrow, \text{ then } \varphi_e(x) \leq w\}.$$

(This is the set of codes of bounded recursive partial functions.)

Problem x5.37. For a fixed, unary, total recursive function f, classify in the arithmetical hierarchy the set of all the codes of f,

$$C_f = \{e \mid \varphi_e = f\}.$$

Problem x5.38. Let A be some recursive set with non-empty complements, i.e., $A \subsetneq \mathbb{N}$. Classify in the arithmetical hierarchy the set

$$B = \{e \mid W_e \subseteq A\}.$$

Problem x5.39. Show that the graph

$$G_f(\vec{x}, w) \iff f(\vec{x}) = w$$

of a total function is Σ^0_k if and only if it is Δ^0_k.

Is this also true of partial functions?

Problem x5.40. A total function $f : \mathbb{N}^n \to \mathbb{N}$ is *limiting recursive* if there is a total, recursive function $g : \mathbb{N}^{n+1} \to \mathbb{N}$ such that for all $\vec{x}$,

$$f(\vec{x}) = \lim_{m\to\infty} g(m, \vec{x}).$$

Prove that a total $f(\vec{x})$ is limiting recursive if and only if the graph G_f of $f(\vec{x})$ is Δ^0_2.

Problem x5.41. Prove that the class of recursive partial functions on Baire space to $\mathbb{N}$ is closed under minimalization.

Problem x5.42. Prove that a relation $P(\boldsymbol{x}, \boldsymbol{\alpha})$ is Σ^0_1 if and only if it is the domain of some recursive $f : \mathbb{N}^n \times \mathcal{N}^\nu \rightharpoonup \mathbb{N}$,

$$P(\boldsymbol{x}, \boldsymbol{\alpha}) \iff f(\boldsymbol{x}, \boldsymbol{\alpha})\downarrow .$$

Problem x5.43. (Σ^0_1-Selection). Prove that for every semirecursive relation $P(\boldsymbol{x}, y, \boldsymbol{\alpha})$, there is a recursive partial function $f(\boldsymbol{x}, \boldsymbol{\alpha})$ such that:

(1) $f(\boldsymbol{x}, \boldsymbol{\alpha})\downarrow \iff (\exists y)P(\boldsymbol{x}, y, \boldsymbol{\alpha})$.
(2) If $(\exists y)P(\boldsymbol{x}, y, \boldsymbol{\alpha})$, then $P(\boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{\alpha}), \boldsymbol{\alpha})$.

Problem x5.44. Prove that a relation $P(\boldsymbol{x}, \boldsymbol{\alpha})$ is recursive if and only if its characteristic (total) function $\chi_R(\boldsymbol{x}, \boldsymbol{\alpha})$ is recursive.

Problem x5.45*. Prove that the set

$$A = \{\alpha \in \mathcal{N} \mid \text{ for infinitely many } x, \alpha(x) = 0\}$$

is in $\Pi^0_2 \setminus \Sigma^0_2$.

Problem x5.46. Prove that if T is an axiomatizable theory, then for any sentence θ,

$$\mathsf{PA} \vdash \overline{\text{Provable}}_{T\cup\{\neg\theta\}}(\ulcorner\theta\urcorner) \to \overline{\text{Provable}}_{T}(\ulcorner\theta\urcorner).$$

Problem x5.47*. Prove that if $\theta(v)$ is a full extended formula and

$$\mathsf{PA} \vdash (\forall x)\overline{\text{Provable}}_{\mathsf{PA}}(\ulcorner\theta(\Delta x)\urcorner) \to (\forall v)\theta(v),$$

then $\mathsf{PA} \vdash (\forall v)\theta(v)$.

Problem x5.48. A function f is **provably recursive** in PA if there is a number e such that

$$f(\vec{x}) = U(\mu y T(e, \vec{x}, y)) \text{ and } \mathsf{PA} \vdash (\forall\vec{x})(\exists y)\mathbf{T}(\Delta e, \vec{x}, y),$$

where $\mathbf{T}(e, \vec{x}, y)$ is a formula which numeralwise expresses the Kleene T predicate. Prove that there is a total recursive function which is not provably recursive in PA.

Problem x5.49. Classify the following sets in the arithmetical hierarchy:

(a) $A = \{e \mid W_e \text{ is a singleton}\}$.
(b) $B = \{e \mid W_e \text{ is infinite}\}$.
(c) $C = \{e \mid (\forall x)(\exists! y)\langle x, y\rangle \in W_e\}$.

CHAPTER 6

APPENDIX TO CHAPTERS 1 – 5

We collect here some basic mathematical results, primarily from set theory, which are used in the first five chapters of these notes.

Notations. The (cartesian) product of two sets A, B is the set of all ordered pairs from A and B,

$$A \times B = \{(x, y) \mid x \in A \;\&\; y \in B\};$$

for products of more than two factors, similarly,

$$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) \mid x_1 \in A_1, \ldots, x_n \in A_n\}.$$

We write W^n for $A_1 \times \cdots \times A_n$ with $A_1 = A_2 = \cdots = A_n = W$, and W^* for the set of all finite sequences (words) from W.

We write $f : A \to W$ to indicate that f is a function on A to W, i.e.,

$$f \subseteq A \times W \;\&\; (\forall x \in A)(\exists! w \in W)[(x, w) \in f].$$

We also write $f : A \rightarrowtail W$ to indicate that f is an *injection* (one-to-one); $f : A \twoheadrightarrow W$ to indicate that f is a *surjection* (onto W); and finally, we write $f : A \rightarrowtail\!\!\!\!\!\twoheadrightarrow W$ to indicate that f is a *bijection*, i.e., a one-to-one correspondence of A with W. If $f : A \to W$, $X \subseteq A$ and $Y \subseteq W$, we let

$$\begin{aligned} f[X] &= \{f(x) \mid x \in X\} \qquad \text{(the image of } X \text{ by } f) \\ f^{-1}[Y] &= \{x \in A \mid f(x) \in Y\} \text{(the inverse image of } Y \text{ by } f. \end{aligned}$$

Problem x6.1 (Definition by recursion)**.** For any two sets W, Y and any two functions $g : Y \to W$, $h : W \times Y \times \mathbb{N} \to W$, there is exactly one function $f : \mathbb{N} \times Y \to W$ which satisfies the following two equations, for all $n \in \mathbb{N}$ and $y \in Y$:

$$\begin{aligned} f(0, y) &= g(y), \\ f(n+1, y) &= h(f(n, y), y, n) \end{aligned} \tag{162}$$

HINT: To prove that such a function exists, define the relation

$$
\begin{aligned}
P(n, y, w) \iff &\text{(there exists a sequence } w_0 w_1 \cdots w_n \in W^*) \\
&\qquad \text{such that } \Big[w_0 = g(y) \\
&\qquad\qquad \& \text{ (for all } i < n)[w_{i+1} = h(w_i, y, i)]] \\
&\qquad\qquad\qquad \& \ w_n = w\Big],
\end{aligned}
$$

and prove by induction on n that for all $y \in Y$, there is exactly one $w \in W$ such that $P(n, y, w)$. We can then set

$$f(n, y) = \text{the unique } w \text{ such that } P(n, y, w).$$

To prove uniqueness, we assume that $f_1, f_2 : \mathbb{N} \times Y \to W$ both satisfy (162) and we show by induction that for all n, for all y, $f_1(n, y) = f_2(n, y)$.

Problem x6.2 (Definition by complete recursion)**.** For any set W, any point $w_0 \in W$ and any function $h : W^* \times \mathbb{N} \to W$, there is exactly one function $f : \mathbb{N} \to W$ such that for all n,

$$f(0) = w_0, \quad f(n + 1) = h(f(0)f(1) \cdots f(n), n).$$

Suppose $F : U^m \to U$ is an m-ary function on a set U and $X \subseteq U$; we say that X *is closed under* F if

$$x_1, \ldots, x_m \in X \Longrightarrow F(x_1, \ldots, x_m) \in X.$$

Problem x6.3 (Functional closure)**.** For any set U, any collection of functions $\mathcal{F}$ on U, of any arity, and any $A \subseteq U$, let

$$
\begin{aligned}
A^{(0)} = A, \quad A^{(n+1)} = A^{(n)} \cup \{F(w_1, \ldots, w_m) \mid w_1, \ldots, w_m \in A^{(n)},& \\
F \in \mathcal{F}, \text{arity}(F) = m\},&
\end{aligned}
$$

$$\overline{A}^{\mathcal{F}} = \bigcup_{n=0}^{\infty} A^{(n)}.$$

Prove that $\overline{A}^{\mathcal{F}}$ is the least subset of U which contains A and is closed under all the functions in $\mathcal{F}$, i.e.,

(1) $A \subseteq \overline{A}^{\mathcal{F}}$;
(2) $\overline{A}^{\mathcal{F}}$ is closed under every $F \in \mathcal{F}$;
(3) if $X \subseteq U$, $A \subseteq X$ and X is closed under every $F \in \mathcal{F}$, then $\overline{A}^{\mathcal{F}} \subseteq X$.

Note. We call $A^{\mathcal{F}}$ the set *generated by* A *and* $\mathcal{F}$. For a standard example, take U to be the set of all strings of symbols of $\mathbb{FOL}(\tau)$ for some signature

τ; let A be the set of all the variables and the constants (viewed as strings of length 1); for any m-ary function symbol f in τ let

$$F_f(\alpha_1, \dots, \alpha_m) \equiv f(\alpha_1, \dots, \alpha_m);$$

and take $\mathcal{F}$ to be the collection of all F_f, one for each function symbol f of τ. The set $A^{\mathcal{F}}$ is then the set of terms of $\mathbb{FOL}(\tau)$.

Problem x6.4 (Structural recursion)**.** Let $A, U, \mathcal{F}$ be as in Problem x6.3 and assume in addition:

1. Each $F : U^m \rightarrowtail U$ is one-to-one and never takes on a value in A, i.e., $F[U^m] \cap A = \emptyset$.
2. The functions in $\mathcal{F}$ have disjoint images, i.e., if $F_1, F_2 \in \mathcal{F}$, arity$(F_1) = m$, arity$(F_2) = n$ and $F_1 \neq F_2$, then for all $u_1, \dots, u_m, v_1 \dots, v_n \in U$,
$$F_1(u_1, \dots, u_m) \neq F_2(v_1, \dots, v_n).$$

Suppose W is any set, $G : W \to W$, and for each m-ary $F \in \mathcal{F}$, $H_F : W^m \to W$ is an m-ary function on W. Prove that there is a unique function

$$\phi : A^{\mathcal{F}} \to W$$

such that

$$\text{if } x \in A, \text{ then } \phi(x) = G(x),$$

and

$$\begin{aligned} &\text{if } x_1, \dots, x_m \in A^{\mathcal{F}} \text{ and } F \text{ is } m\text{-ary in } \mathcal{F}, \\ &\qquad\qquad \text{then } \phi(F(x_1, \dots, x_m)) = H_F(\phi(x_1), \dots, \phi(x_m)). \end{aligned}$$

Problem x6.5. Let U be the set of symbols of $\mathbb{FOL}(\tau)$, and specify $A \subseteq U$ and $\mathcal{F}$ so that the conditions in Problem x6.4 are satisfied and $A^{\mathcal{F}}$ is the set of formulas of $\mathbb{FOL}(\tau)$. Indicate how the definition of FO(χ) in Definition 1B.6 is justified by Problem x6.4.

A set A is **countable** if either A is empty, or A is the image of some function $f : \mathbb{N} \twoheadrightarrow A$, i.e.,

$$A = \{a_0, a_1, \dots\} \quad \text{with } a_i = f(i).$$

Problem x6.6 (Cantor)**.** If $A_0, A_1, A_2, \dots$ is a sequence of countable sets, then the union

$$\textstyle\bigcup_{i=0}^{\infty} A_i = A_0 \cup A_1 \cup \cdots$$

is also countable. It follows that:

1. The union $A \cup B$ and the product $A \times B$ of two countable sets are countable.
2. If A is countable, then so is each finite power A^n.

3. If A is countable, then so is the set of all words A^*.

Hint: Assume (without loss of generality) that no A_i is empty; suppose for each $i \in \mathbb{N}$, $f_i : \mathbb{N} \twoheadrightarrow A_i$ enumerates A_i; choose some fixed $a_0 \in A_0$; and define $f : \mathbb{N} \to \bigcup_{i=0}^{\infty} A_i$ by

$$f(n) = \begin{cases} f_i(j), & \text{if } n = 2^i 3^j, \text{ for some (necessarily) unique } i, j, \\ a_0, & \text{otherwise;} \end{cases}$$

now prove that f is onto $\bigcup_{i=0}^{\infty} A_i$.

The Corollary for the product $A \times B$ follows by noticing that

$$A \times B = \bigcup_{i=0}^{\infty} \{(a_i, x) \mid x \in B\},$$

with $A = \{a_0, a_1, \dots\}$.

Problem x6.7* (Cantor)**.** Prove that if $\mathbf{A} = (A, \leq_A)$ and $\mathbf{B} = (B, \leq_B)$ are both countable, dense in themselves linear orderings with no first or last element, then $\mathbf{A}$ and $\mathbf{B}$ are isomorphic. Hint: Let

$$A = \{a_0, a_1, \dots\}, \quad B = \{b_0, b_1, \dots\},$$

(with no repetitions) and construct by recursion a sequence of bijective mappings $\rho_n : A_n \rightarrowtail\!\!\!\!\rightarrow B_n$ such that:

(1) A_n, B_n are finite sets, $A_n \subseteq A, B_n \subseteq B$.
(2) $a_0, \dots, a_n \in A_n, b_0, \dots, b_n \in B_n$.
(3) $\rho_0 \subseteq \rho_1 \subseteq \cdots$.
(4) If $a, a' \in A_n$, then $a \leq_A a' \iff \rho_n(a) \leq_B \rho(a')$.

The required isomorphism is $\rho = \bigcup_n \rho_n$.

Problem x6.8. A binary relation $\sim$ on a set C is an equivalence relation if and only if there exists a surjection

$$\rho : C \twoheadrightarrow \overline{C} \tag{163}$$

of C onto a set $\overline{C}$, such that

$$x \sim y \iff \rho(x) = \rho(y) \qquad (x, y \in C). \tag{164}$$

When (163) and (164) hold we call $\overline{C}$ a *quotient* of C by $\sim$ and ρ a *determining homomorphism* of $\sim$.

Hint: For the non-trivial direction, define the *equivalence class* of each $x \in C$ by

$$\overline{x} = \{y \in C \mid y \sim x\} \subseteq \text{Powerset}(C),$$

let $\overline{C} = \{\overline{x} \mid x \in C\}$ and let $\rho(x) = \overline{x}$.

A **wellordering** or **well ordered set** is a linear ordering $(A, \leq)$ in which every non-empty subset X of A has a least element.

Problem x6.9. A linear ordering $(A, \leq)$ is a wellordering if and only if there is no infinite descending chain $x_0 > x_1 > \cdots$. Hint: This requires a mild form of the Axiom of Choice, the so-called *Axiom of Dependent Choices*. Use the fact that the image $\{x_0, x_1, \dots\}$ of an infinite descending chain is a non-empty set with no minimum.

CHAPTER 7

INTRODUCTION TO FORMAL SET THEORY

We summarize here briefly the basic facts about sets which can be proved in the standard axiomatic set theories, primarily to prepare the ground for the introduction to the metamathematics of these theories in the next chapter.

7A. The intended universe of sets

It may be useful to review at this point our intuitive conception of the standard model for set theory, the universe V of sets. This *does not* contain all "arbitrary collections of objects" in Cantor's eloquent phrase: it is well known that this naive approach leads to contradictions. Instead, we admit as "sets" only those collections which occur in the *complete (transfinite) cumulative sequence of types*—the hierarchy obtained by starting with the empty set and iterating "indefinitely" the "power operation."

To be just a little more precise—and using "intuitive set theory", as we have been doing all along—suppose we are given an operation P on sets which assigns to each set x a collection $P(x)$ of subsets of x

(165) $$y \in P(x) \Longrightarrow y \subseteq x.$$

Suppose we are also given a collection $\mathcal{S}$ of *stages*, wellordered by a relation $\leq_{\mathcal{S}}$, i.e., for ζ, η, ξ in $\mathcal{S}$,

(166) $$\zeta \leq_{\mathcal{S}} \zeta, \quad (\zeta \leq_{\mathcal{S}} \eta \,\&\, \eta \leq_{\mathcal{S}} \xi) \Longrightarrow \zeta \leq_{\mathcal{S}} \xi,$$
$$(\zeta \leq_{\mathcal{S}} \eta \,\&\, \eta \leq_{\mathcal{S}} \zeta) \Longrightarrow \zeta = \eta, \quad \zeta \leq_{\mathcal{S}} \eta \quad \text{or} \quad \eta \leq_{\mathcal{S}} \zeta$$

(167) if $A \subseteq \mathcal{S}$ is any collection of stages, $A \neq \emptyset$, then
there is some $\xi \in A$ such that for every $\eta \in A$, $\xi \leq_{\mathcal{S}} \eta$.

Call *the least stage* 0 and for $\xi \in \mathcal{S}$, let $\xi + 1$ be *the next stage*—the least stage which is greater than ξ. If λ is a stage $\neq 0$ and $\neq \xi + 1$ for every ξ, we call it a *limit stage*.

For fixed P, $\mathcal{S}$, $\leq_{\mathcal{S}}$ satisfying (165) – (167) we define the hierarchy

$$V_\xi = V_\xi(P, \mathcal{S}, \leq_{\mathcal{S}}) \qquad (\xi \in \mathcal{S})$$

by recursion on $\xi \in \mathcal{S}$:

$$\begin{aligned} V_0 &= \emptyset \\ V_{\xi+1} &= V_\xi \cup P(V_\xi), \\ V_\lambda &= \bigcup_{\xi<\lambda} V_\xi \quad \text{if } \lambda \text{ is a limit stage.} \end{aligned}$$

The collection of sets

$$V = V(P, \mathcal{S}, \leq_{\mathcal{S}}) = \bigcup_{\xi \in \mathcal{S}} V_\xi$$

is *the universe generated with P as the power operation, on the stages $\mathcal{S}$*. It is very easy to check that

$$\xi \leq_{\mathcal{S}} \eta \Longrightarrow V_\xi \subseteq V_\eta$$

and that each V_ξ is a *transitive set*, i.e.,

$$(x \in V_\xi \,\&\, y \in x) \Longrightarrow y \in V_\xi.$$

For example, suppose we take

$$P(x) = \mathcal{P}(x) = \{y : y \subseteq x\}$$

and

$$\mathcal{S} = \omega 2 = \{0, 1, 2, \dots, \omega, \omega+1, \omega+2, \dots\},$$

where the stages $0, 1, 2, \dots, \omega, \omega+1, \omega+2, \dots$ are all assumed distinct and ordered as we have enumerated them. In this case we obtain the universe

$$V^Z = V(\mathcal{P}, \omega 2, \leq_{\omega 2}) = V_0 \cup V_1 \cup V_2 \cup \cdots \cup V_\omega \cup V_{\omega+1} \cup \cdots,$$

often called the *universe of Zermelo*. It is well known that all the familiar structures of classical mathematics have *isomorphic copies* within V^Z—we can locate in V^Z (faithful representations of) the natural and real numbers, all functions on the reals to the reals, etc.

For a very different universe of sets, we might choose a small power operation, e.g.,

$$\mathbf{Def}(x) = \{y \subseteq x : y \text{ is elementary in the structure } (x, \in\restriction x, \{t\}_{t\in x})\}.$$

We may want to take $\mathcal{S}$ quite long this time, say

$$\mathcal{S} = \omega^\omega = \{0, 1, 2, , \dots, \omega, \omega+1, \dots, \omega 2, \omega 2+1, \dots, \omega n, \omega n+1, \dots, \dots\},$$

so that ω^ω is the union of infinitely many disjoint copies of $\mathbb{N}$ put side-by-side. Using notation we will justify later, set

$$L_{\omega^\omega} = V(\mathbf{Def}, \omega^\omega, \leq_{\omega^\omega}).$$

It is easy to see that $V^Z \not\subseteq L_{\omega^\omega}$, because V^Z is uncountable while L_{ω^ω} is a countable set. It is a little more difficult to show also that $L_{\omega^\omega} \not\subseteq V^Z$, so that these two constructions yield two incomparable *set universes*, in which we can interpret the axioms of axiomatic set theory and check out which are true for each of them.

It is clear that the universe $V(P, \mathcal{S}, \leq_{\mathcal{S}})$ does not depend on the particular objects that we have chosen to call *stages* but only on the *length* (the *order type*) of the ordering $\leq_{\mathcal{S}}$; i.e., if the structures $(\mathcal{S}, \leq_{\mathcal{S}})$ and $(\mathcal{S}', \leq'_{\mathcal{S}})$ are isomorphic, then

$$V(P, \mathcal{S}, \leq_{\mathcal{S}}) = V(P, \mathcal{S}', \leq'_{\mathcal{S}}).$$

This definition of the universes $V(P, \mathcal{S}, \leq_{\mathcal{S}})$ is admittedly vague, and the results about them that we have claimed are grounded on intuitive ideas about sets and wellorderings which we have not justified. It is clear that we cannot expect to give a precise, mathematical definition of the basic notions of set theory, unless we use notions of some richer theory which in turn would require interpretation. At this point, we claim only that the intuitive description of $V(P, \mathcal{S}, \leq_{\mathcal{S}})$ is sufficiently clear so we can formulate meaningful propositions about these set universes and argue rationally about their truth or falsity.

Most mathematicians accept that there is *a largest meaningful* operation P satisfying (165) above, *the true power operation* which takes x to the collection $\mathcal{P}(x)$ of *all* subsets of x. This is one of the cardinal assumptions of *realistic* (meaningful, not formal) set theory. Similarly, it is not unreasonable to assume that there is a *longest* collection of stages ON along which we can *meaningfully* iterate the power operation.

Our intended standard universe of sets is then

$$V = V(\mathcal{P}, \mathrm{ON}, \leq_{\mathrm{ON}}),$$

where $(\mathrm{ON}, \leq_{\mathrm{ON}})$ *is the longest meaningful collection of stages*—the wellordered class of *ordinal numbers*, as we will call it later. The axioms of the standard axiomatic set theory ZFC (Zermelo-Fraenkel set theory with Choice and Foundation) are justified by appealing to this intuitive understanding of what sets are. We will formulate it (again) carefully in the following sections and then derive its most basic consequences.

What is less obvious is that if we take $(\mathrm{ON}, \leq_{\mathrm{ON}})$ to be the same "largest, meaningful collection of stages", then the set universe

$$L = (\mathbf{Def}, \mathrm{ON}, \leq_{\mathrm{ON}})$$

is another plausible understanding of the notion of set, Gödel's *universe of constructible sets*: the central theorem of this and the next Chapter is that L *also satisfies all the axioms of* ZFC. Moreover, Gödel's proof of this surprising result does not depend on the Axiom of Choice, and so it also shows the consistency of ZFC relative to its choiceless fragment.

7B. ZFC and its subsystems

To simplify the formulation of the formal axioms of set theory, we state here a simple result of logic which could have been included in Chapter 1, right after Definition 1H.9:

Proposition 7B.1 (Eliminability of descriptions)**.** *Fix a signature τ, and suppose $\phi(\vec{v}, w) \equiv \phi(v_1, \dots, v_n, w)$ is a full extended τ-formula and F is an n-ary function symbol not in τ.*

(1) *With each full, extended (τ, F)-formula $\theta'(\vec{u})$ we can associate a full, extended τ-formula $\theta(\vec{u})$ such that*

$$(\forall \vec{v})(\exists! w)\phi(\vec{v}, w) \ \& \ (\forall \vec{v})\phi(\vec{v}, F(\vec{v})) \vdash \theta'(\vec{u}) \leftrightarrow \theta(\vec{u}).$$

(2) *Suppose T is a τ-theory axiomatized by schemes such that*

$$T \vdash (\forall \vec{v})(\exists! w)\phi(\vec{v}, w),$$

and let T' be the (τ, F)-theory whose axioms are those of T, the sentence $(\forall \vec{v})\phi(\vec{v}, F(\vec{v}))$, and all instances with (τ, F) formulas of the axiom schemes of T. Then T' is a conservative extension of T, i.e., for all τ-sentences θ,

$$T' \vdash \theta \iff T \vdash \theta.$$

There is also an analogous result where we add to the language a new n-ary relation symbol C and the axiom

$$(168) \qquad (\forall \vec{v})[R(\vec{v}) \leftrightarrow \phi(\vec{v})] \quad (\phi(\vec{v}) \text{ full extended}),$$

but it is simpler, and it can be avoided by treating (168) as an abbreviation. In applying these constructions we will refer to T' as an *extension of T by definitions.*

We leave the precise definition of "axiomatization by schemes" and the proof for Problem x7.2*. The thing to notice here is that all the set theories we will consider are axiomatized by schemes, and so the proposition allows us to introduce—and use with no restriction—names for constants and operations defined in them. If, for example,

$$T \vdash (\exists! z)(\forall t)[t \notin z],$$

as all the theories we are considering do, we can then extend T with a constant $\emptyset$ and the axiom

$$(\forall t)[t \notin \emptyset]$$

and we can use this constant in producing instances of the axiom schemes of T without adding any new theorems which do not involve $\emptyset$.

We now restate for easy reference (from Definitions 1A.5, 1G.12) the axioms of set theory and their formal versions in the language $\mathbb{FOL}(\in)$.

We will be using the common abbreviations for *restricted quantification*

$$(\exists x \in z)\phi :\equiv (\exists x)[x \in z \,\&\, \phi],$$
$$(\forall x \in z)\phi :\equiv (\forall x)[x \in z \rightarrow \phi],$$
$$(\exists! x \in z)\phi :\equiv (\exists y \in z)(\forall x \in z)[\phi \leftrightarrow y = x]$$

(1) *Extensionality Axiom*: two sets are equal exactly when they have the same members:

$$(\forall x, y)[x = y \leftrightarrow [(\forall u \in x)(u \in y) \;\&\; (\forall u \in y)(u \in x)]].$$

(2) *Emptyset and Pairing Axioms*: there exists a set with no members, and for any two sets x, y, there is a set z whose members are exactly x and y:

$$(\exists z)(\forall u)[u \notin z], \quad (\forall x, y)(\exists z)(\forall u)[u \in z \leftrightarrow (u = x \vee u = y)]$$

It follows by the Extensionality Axiom that there is exactly one empty set and one pairing operation, and we name them $\emptyset$ and $\{x, y\}$, as usual. (And in the sequel we will omit this ceremony of stating separately the unique existence condition before baptizing the relevant operation with its customary name.)

(3) *Unionset Axiom*: for each set x, there is exactly one set $z = \bigcup x$ whose members are the members of members of x, i.e.,

$$(\forall u)[u \in \bigcup x \leftrightarrow (\exists y \in x)[u \in y]].$$

(4) *Infinity Axiom*: there exists a set z such that $\emptyset \in z$ and z is closed under the *set successor operation* x',

$$(\exists z)(\forall x \in z)[x' \in z],$$

where $u \cup v = \bigcup\{u, v\}$ and $x' = x \cup \{x\}$.

(5) *Replacement Axiom Scheme*: For each extended formula $\phi(u, v)$ in which the variable z does not occur and $x \not\equiv u, v$, the universal closure of the following formula is an axiom:

$$(\forall u)(\exists! v)\phi(u, v) \rightarrow (\exists z)\Big[(\forall u \in x)(\exists v \in z)\phi(u, v) \\ \& \; (\forall v \in z)(\exists u \in x)\phi(u, v)\Big].$$

The instance of the Replacement Axiom for a full extended formula $\phi(\vec{y}, u, v)$ says that if for some tuple $\vec{y}$ the formula defines an operation

$$F_{\vec{y}}(u) = (\text{the unique } v)[\phi(\vec{y}, u, v)],$$

then the image

$$F_{\vec{y}}[x] = \{F_{\vec{y}}(u) : u \in x\}$$

of any set x by this operation is also a set. This is most commonly used to justify definitions of operations, in the form

$$G(\vec{y}, x) = \{F(\vec{y}, u) : u \in x\}. \tag{169}$$

(6) *Powerset Axiom*: for each set x there is exactly one set $\mathcal{P}(x)$ whose members are all the subsets of x, i.e.,

$$(\forall u)[u \in \mathcal{P}(x) \leftrightarrow (\forall v \in u)[v \in x]].$$

(7) *Axiom of Choice,* **AC**: for every set x whose members are all non-empty and pairwise disjoint, there exists a set z which intersects each member of x in exactly one point:

$$\begin{aligned}(\forall x)\Big(\Big[&(\forall u \in x)(u \neq \emptyset)\\ &\ \&\ (\forall u, v \in x)[u \neq v \to [(\forall t \in u)(t \notin v)\ \&\ (\forall t \in v)(t \notin u)]]\Big]\\ &\qquad\qquad \to (\exists z)(\forall u \in x)(\exists! t \in z)(t \in u)\Big).\end{aligned}$$

(8) *Foundation Axiom*: Every non-empty set x has a member z from which it is disjoint:

$$(\forall x)[x \neq \emptyset \to (\exists z \in x)(\forall t \in z)[t \notin x]]$$

The most important of the theories we will consider are

- $\mathsf{ZF}^- = (1) - (5)$, i.e., the axioms of extensionality, emptyset and pairing, unionset, infinity and the Axiom Scheme of Replacement,
- $\mathsf{ZF}^-_g = (1) - (5) + (8) = \mathsf{ZF}^- +$ Foundation,
- $\mathsf{ZF} = (1) - (6) = \mathsf{ZF}^- +$ Powerset $= \mathsf{ZFC} -$ Foundation $- \mathbf{AC}$,
- $\mathsf{ZF}_g = (1) - (6) + (8) = \mathsf{ZF} +$ Foundation $= \mathsf{ZFC} - \mathbf{AC}$.
- $\mathsf{ZFC} = (1) - (8) = \mathsf{ZF}_g + \mathbf{AC}$.

We have included the alternative, more commonly used names of ZF and ZF_g which specify them as subtheories of ZFC.

The *Zermelo-Fraenkel set theory with choice* ZFC is the most widely accepted standard in mathematical practice: if a mathematician claims to have proved some proposition P about sets, then she is expected to be able to supply (in principle) a proof of its formal version θ_P from the axioms of ZFC. (This, in fact, applies to propositions in any part of mathematics, as they can all be interpreted faithfully by set-theoretic statements using familiar methods—which we will not discuss in any detail here.)

The weaker theories will also be very important to us, however, primarily as technical tools: to show the consistency of ZFC relative to ZF, for example, we will need to verify that a great number of theorems can be established in ZF—without appealing to the Axiom of Foundation or **AC**.

Convention: *All results in this Chapter will be derived from the axioms of* ZF$^-$ (or extensions of ZF$^-$ by definitions) *unless otherwise specified*—most often by a discreet notation (ZF) or (ZFC) added to the statement.

We will assume that the theorems we prove are interpreted in a structure $(\mathcal{V}, \in)$, which may be very different from the intended interpretation $(V, \in)$ of ZFC we discussed in Section 7A, especially as $(\mathcal{V}, \in)$ need not satisfy the powerset, choice and foundation axioms.

Finally, there is the matter of *mathematical propositions and proofs* versus *formal sentences of* $\mathbb{FOL}(\in)$ *and formal proofs* in one of the theories above—which are, in practice, impossible to write down in full and not very informative. We will choose the former over the latter for statements (and certainly for proofs), although in some cases we will put down the formal version of the conclusion, or a reasonable misspelling of it, cf. 1B.7. The following terminology and conventions help.

A full extended formula

$$\varphi(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m) \equiv \varphi(\vec{\mathbf{x}}, \vec{\mathbf{y}})$$

together with an m-tuple $\vec{y} = y_1, \dots, y_m \in \mathcal{V}$ determines an n-ary (class) *condition* on the universe $\mathcal{V}$,

$$P(\vec{x}) \iff (\mathcal{V}, \in) \models \varphi[\vec{x}, \vec{y}],$$

and it is a *definable condition* if there are no parameters, i.e., $m = 0$. For example, $t \in y$ is a condition for each y, and $x \in y,\ x = y$ are definable conditions.

A *collection* of sets $M \subseteq \mathcal{V}$ is a *class* if membership in M is a unary condition, i.e., if there is some full extended formula $\varphi(\mathbf{s}, \vec{\mathbf{y}})$ of $\mathbb{FOL}(\in)$ and sets $\vec{y}$ such that

$$M = \{s : (\mathcal{V}, \in) \models \varphi[s, \vec{y}]\}, \text{ i.e., } s \in M \iff (\mathcal{V}, \in) \models \varphi[s, \vec{y}].$$

It is a *definable class*

$$M = \{s : (\mathcal{V}, \in) \models \varphi[s]\}$$

if no parameters are used in its definition.

If a class M has the same members as a set x, we then identify it with x, so that, in particular, every set x is a class; and x is a *definable set* if it is definable as a class, i.e., if the condition $t \in x$ is definable.

A class is *proper* if it is not a set.

Finally, of $M_1, \dots, M_n$ are classes, then a *class operation*

$$F : M_1 \times \cdots \times M_n \to \mathcal{V}$$

is any $F : \mathcal{V}^n \to \mathcal{V}$ such that

$$s_1 \notin M_1 \vee \cdots \vee s_n \notin M_n \Longrightarrow F(s_1, \dots, s_n) = \emptyset,$$

and for some full extended formula $\varphi(\mathbf{s}_1, \ldots, \mathbf{s}_n, \mathbf{w}, \vec{\mathbf{y}})$ and suitable $\vec{y}$,

$$F(s_1, \ldots, s_n) = w \iff (\mathcal{V}, \in) \models \varphi[s_1, \ldots, s_n, w, \vec{y}].$$

Such a class operation is then determined by its values $F(s_1, \ldots, s_n)$ for arguments $s_1 \in M_1, \ldots, s_n \in M_n$. A class operation is *definable* if it can be defined by a formula without parameters.

When there is any possibility of confusion, we will use capital letters for classes, conditions and operations to distinguish them from sets, relations and functions (sets of ordered pairs) which are members of our interpretation.

It is important to remember that theorems about classes, conditions and operations are expressed formally by theorem schemes.

It helps to do this explicitly for a while, as in the following

Proposition 7B.2 (The Comprehension Scheme). *If A is a class and z is a set, then the intersection*

$$A \cap z = \{t \in z : t \in A\} \tag{170}$$

is a set, i.e., for every full extended formula $\phi(s, \vec{x})$,

$$\mathsf{ZF}^- \vdash (\forall \vec{x})(\exists w)(\forall s)\Big[s \in w \leftrightarrow (\phi(s, \vec{x}) \ \&\ s \in z)\Big].$$

Proof. If $(\forall t \in z)[t \notin A]$, then $A \cap z = \emptyset$ and $\emptyset$ is a set. If there is some $t_0 \in A \cap z$, let

$$F(t) = \begin{cases} t, & \text{if } t \in z \ \&\ t \in A, \\ t_0, & \text{otherwise,} \end{cases}$$

and check easily that $F[z] = A \cap z$. ⊣

The Comprehension Scheme is also called the *Subset* or *Separation Property* and it is one of the basic axioms in Zermelo's first axiomatization of set theory,

- ZC = (1) − (4) + (6) + (7) + Comprehension.

It is most useful in showing that simple sets exist and defining class operations by setting

$$F(z, \vec{x}) = \{s \in z : P(z, \vec{x})\}$$

where $P(z, \vec{x})$ is a definable condition, e.g.,

$$x \cap y = \{t \in x : t \in y\}, \quad x \setminus y = \{t \in x : t \notin y\}.$$

In fact, almost all of classical mathematics can be developed in ZC, without using replacement, but it is not a strong enough theory for our purposes here and so we will not return to it.

7B.3. Note. Zermelo's formulation of the Axiom of Infinity (given in Definition 1A.5) was different from (4), and so the universe of sets that can be constructed by his axioms is not exactly the collection V^Z defined in Section 7A. Zermelo's Axiom of Infinity is equivalent (in ZF^- − Infinity) to (4), but the proof requires establishing first some basic facts in Zermelo's theory.

7C. Set theory without powersets, AC or foundation, ZF^-

Set theory is mostly about the size (cardinality) of sets, and not much about size can be established without the Powerset Axiom and the Axiom of Choice. It is perhaps rather surprising that all the basic results about wellfounded relations, wellorderings and ordinal numbers can be developed in this fairly weak system.

We start with a list of basic and useful definable sets, classes and operations, some of which we have already introduced and some new ones which will not be motivated until later. In verifying the parts of the next theorem, we will often appeal (without explicit mention) to the following lemma, whose proof we leave for Problem x7.4:

Lemma 7C.1. *If $H, G_1, \ldots, G_m$ are definable class operations, then their* (generalized) *composition*

$$F(\vec{x}) = H(G_1(\vec{x}), \ldots, G_m(\vec{x}))$$

is also definable.

Theorem 7C.2. *The following classes, conditions, operations and sets are definable, and the claims made about them hold:*

#1. $x \in y \iff x$ is a member of y.

#2. $x \subseteq y \iff (\forall t \in x)[t \in y]$.

#3. $x = y \iff x$ is equal to y.

#4. $\{x, y\}$ = the unordered pair of x and y;
$\{x, y\} = w \iff x \in w \,\&\, y \in w \,\&\, (\forall t \in w)[t = x \vee t = y]$.

#5. $\emptyset = 0$ = the empty set; $1 = \{\emptyset\}$;
$w = \emptyset \iff (\forall t \in w)[t \notin w]$.

#6. $\bigcup x = \{t : (\exists s \in x)[t \in s]\}$;
$\bigcup x = w \iff (\forall s \in x)(\forall t \in s)[t \in w] \,\&\, (\forall t \in w)(\exists s \in x)[t \in s]$.

#7. $x \cup y = \bigcup\{x, y\}$, $\quad x \cap y = \{t \in x : t \in y\}$, $\quad x \setminus y = \{t \in x : t \notin y\}$.

#8. $x' = x \cup \{x\}$.

#9. $\omega =$ the $\subseteq$-least set satisfying the Axiom of Infinity;
$t \in \omega \iff (\forall z)\Big([\emptyset \in z \;\&\; (\forall x \in z)(x' \in z)] \rightarrow t \in z\Big)$.

#10. $\langle x, y\rangle = \big\{\{x\}, \{x, y\}\big\}$,
$\langle x_1, \ldots, x_{n+1}\rangle = \big\langle \langle x_1, \ldots, x_n\rangle, x_{n+1}\big\rangle$.

Notice that for any x, y,

$$x, y \in \bigcup \langle x, y\rangle, \quad \langle x, y\rangle \in r \Longrightarrow x, y \in \bigcup\bigcup r.$$

#11. $u \times v = \{\langle x, y\rangle : x \in u \,\&\, y \in v\}$,
$u_1 \times \cdots \times u_{n+1} = (u_1 \times \cdots \times u_n) \times u_{n+1}$,
$u \uplus v = (\{0\} \times u) \cup (\{1\} \times v)$ *(*disjoint union*)*

#12. $\mathrm{OrdPair}(w) \iff w$ is an ordered pair
$\iff (\exists x \in \bigcup w)(\exists y \in \bigcup w)[w = \langle x, y\rangle]$.

#13. $\mathrm{Relation}(r) \iff r$ is a set of ordered pairs
$\iff (\forall w \in r)\mathrm{OrdPair}(w)$.

#14. $\mathrm{Domain}(r) = \{x \in \bigcup\bigcup r : (\exists y \in \bigcup\bigcup r)[\langle x, y\rangle \in r]\}$,
$\mathrm{Domain}(r) = w \iff (\forall x \in \bigcup\bigcup r)(\forall y \in \bigcup\bigcup r)$
$[\langle x, y\rangle \in r \Longrightarrow x \in w] \,\&\, (\forall x \in w)(\exists y \in \bigcup\bigcup r)[\langle x, y\rangle \in r]$.

#15. $\mathrm{Image}(r) = \{y \in \bigcup\bigcup r : (\exists x \in \bigcup\bigcup r)[\langle x, y\rangle \in r]\}$,
$\mathrm{Image}(r) = w \iff (\forall x \in \bigcup\bigcup r)(\forall y \in \bigcup\bigcup r)$
$[\langle x, y\rangle \in r \Longrightarrow y \in w] \,\&\, (\forall y \in w)(\exists x \in \bigcup\bigcup r)[\langle x, y\rangle \in r]$.

#16. $\mathrm{Field}(r) = \mathrm{Domain}(r) \cup \mathrm{Image}(r)$.

#17. $\mathrm{Function}(f) \iff f$ is a function (as a set of ordered pairs)
$\iff \mathrm{Relation}(f)$
$\& \big(\forall x \in \mathrm{Domain}(f)\big)\big(\forall y \in \mathrm{Image}(f)\big)$
$\big(\forall y' \in \mathrm{Image}(f)\big)$
$\big[[\langle x, y\rangle \in f \,\&\, \langle x, y'\rangle \in f] \rightarrow y = y'\big]$.

If f is a function, we put

$$f(x) = y \iff \langle x, y\rangle \in f.$$

#18. $f : a \rightarrow b \iff \mathrm{Function}(f) \;\&\; \mathrm{Domain}(f) = a \;\&\; \mathrm{Image}(f) \subseteq b$,
$f : a \rightarrowtail b \iff f$ is an injection from a to b,
$f : a \twoheadrightarrow b \iff f$ is a surjection from a to b,
$f : a \rightarrowtail\!\!\!\!\twoheadrightarrow b \iff f$ is a bijection from a to b
$f : a \rightarrow \mathcal{V} \iff (\exists b)[f : a \rightarrow b]$
(and similarly with all the other arrows).

#19. $F \restriction a =$ the restriction of the operation F to a
$= \{\langle x, w\rangle : x \in a \;\&\; F(x) = w\}$

#20. $r \upharpoonright u = \{w \in r : (\exists x \in u)(\exists y \in \text{Image}(r))[w = \langle x, y\rangle\}$.

$$\begin{aligned} r \upharpoonright u = w \iff\ & w \subseteq r \,\&\, \text{Relation}(w) \\ & \& \big(\forall x \in \text{Domain}(r)\big)\big(\forall y \in \text{Image}(r)\big) \\ & \qquad [\langle x, y\rangle \in w \leftrightarrow x \in u]. \end{aligned}$$

#21. $$\begin{aligned} \text{Iso}(f, r_1, r_2) \iff\ & f \text{ is an isomorphism of } r_1 \text{ and } r_2 \\ \iff\ & f : \text{Field}(r_1) \rightarrowtail\!\!\!\!\rightarrow \text{Field}(r_2) \\ & \& \ (\forall s, t \in \text{Field}(r_1))[\langle s, t\rangle \in r_1 \leftrightarrow \langle f(s), f(t)\rangle \in r_2]. \end{aligned}$$

#22. $$\begin{aligned} \text{WF}(r) \iff\ & r \text{ is a (strict) wellfounded relation} \\ \iff\ & \text{Relation}(r) \ \& \ (\forall x \neq \emptyset)(\exists y \in x)(\forall t \in x)[\langle t, y\rangle \notin r]. \end{aligned}$$

A point y is *r-minimal in x* if $y \in x$ & $(\forall t \in x)[\langle t, y\rangle \notin r]$

#23. $$\begin{aligned} x \le_r y \iff\ & \langle x, y\rangle \in r, \\ x <_r y \iff\ & \langle x, y\rangle \in r \ \& \ \langle y, x\rangle \notin r. \end{aligned}$$

These are notation conventions, to facilitate dealing with partial orderings and wellfounded relations. The second defines the *strict part* of the relation r, and $<_r = r$ if r is already strict, i.e., if we never have $\langle x, y\rangle$ & $\langle y, x\rangle$; this is true, in particular for wellfounded r, since

$$\langle s, t\rangle, \langle t, s\rangle \in r \Longrightarrow \{s, t\} \text{ has no } r\text{-minimal member.}$$

Notice that

$$\{x : x <_r y\} = \{x \in \bigcup\bigcup r : x <_r y\}$$

is a set, as is $\{x : x \le_r y\}$.

#24. $$\begin{aligned} \text{PO}(r) \iff\ & r \text{ is a partial ordering (or } \textit{poset}) \\ \iff\ & \text{Relation}(r) \\ & \& \ (\forall x \in \text{Field}(r)[x \le_r x] \\ & \& \ (\forall x, y, z \in \text{Field}(r))[[x \le_r y \ \& \ y \le_r z] \to x \le_r z] \\ & \& \ (\forall x, y \in \text{Field}(r)[[x \le_r y \ \& \ y \le_r x] \to x = y] \end{aligned}$$

In the terminology introduced by Definition 1A.2 and used in the preceding chapters, a partial ordering is a pair $(x, \le_x)$ where $\text{PO}(\le_x)$ and $x = \text{Field}(\le_x)$ by this notation. We will sometimes revert to the old notation when it helps clarify the discussion.

#25. $$\begin{aligned} \text{LUB}(c, r, w) \iff\ & w \text{ is a least upper bound of } c \subseteq \text{Field}(r) \\ \iff\ & \text{PO}(r) \ \& \ (\forall x \in c)(x \le_r w) \\ & \quad \& \ (\forall v \in \text{Field}(r))\Big((\forall x \in c)(x \le_r v) \to w \le_r v\Big). \end{aligned}$$

#26. $\sup_r(c) =$ the least upper bound of c in r, if it exists, otherwise $\emptyset$

$\sup_r(c) = w \iff \text{LUB}(c, r, w) \vee [(\forall v \in \text{Field}(r))\neg\text{LUB}(c, r, w) \ \& \ w = \emptyset]$

#27. $$\begin{aligned} \text{Chain}(c, r) \iff\ & c \text{ is a chain in the relation } r \\ \iff\ & (\forall x, y \in c)[x \le_r y \vee y \le_r x]. \end{aligned}$$

#28. $$\begin{aligned} \text{LO}(r) \iff\ & r \text{ is a linear ordering} \\ \iff\ & \text{PO}(r) \ \& \ \text{Chain}(\text{Field}(r), r). \end{aligned}$$

#29. $\mathrm{WO}(r) \iff r$ is a wellordering
$\iff \mathrm{LO}(r)\ \&\ \mathrm{WF}(<_r)$.

We will appeal repeatedly (and silently) to the easy fact that

$$\mathrm{WO}(r) \Longrightarrow (\forall x)\mathrm{WO}(r \cap (x \times x)). \tag{171}$$

#30. $r_1 =_o r_2 \iff r_1$ and r_2 are similar (isomorphic) wellorderings
$\iff \mathrm{WO}(r_1)\ \&\ \mathrm{WO}(r_2)\ \&\ (\exists f)[\mathrm{Iso}(f, r_1, r_2)]$

#31. $\mathrm{Transitive}(x) \iff x$ is a transitive set
$\iff \bigcup x \subseteq x$
$\iff (\forall s \in x)[s \subseteq x]$
$\iff (\forall s \in x)(\forall t \in s)[t \in x]$.

#32. A is a transitive class $\iff (\forall s \in A)(\forall t \in s)[t \in A]$.

#33. $\mathrm{Ordinal}(\xi) \iff \xi$ is an ordinal (number)
$\iff \mathrm{Transitive}(\xi)$
$\&\ \mathrm{WO}(\{\langle x, y\rangle : x, y \in \xi\ \&\ [x = y \vee x \in y]\})$.

#34. $\mathrm{ON} = \{\xi : \mathrm{Ordinal}(\xi)\} =$ the class of ordinals.

#35. $x \leq_\xi y \iff x, y \in \xi \in \mathrm{ON}\ \&\ (x = y \vee x \in y)$.

#36. $\eta \leq_{\mathrm{ON}} \xi \iff \eta, \xi \in \mathrm{ON}\ \&\ [\eta = \xi \vee \eta \in \xi]$,
$\eta <_{\mathrm{ON}} \xi \iff \eta \leq_{\mathrm{ON}} \xi\ \&\ \eta \neq \xi$.

Proof. All the parts of the theorem follow very easily from the axioms and the properties of elementary definability, except perhaps for the following three.

(#9) The Axiom of Infinity guarantees that there is a set z^* which satisfies it, and we set

$$\omega = \Big\{x \in z^* : (\forall z \subseteq z^*)\Big[[\emptyset \in z\ \&\ (\forall x \in z)[x' \in z]] \rightarrow x \in z\Big]\Big\}.$$

It is easy to verify that ω satisfies the Axiom of Infinity and is the least such.

(#11) The existence of cartesian products is proved by two applications of replacement in the form (169):

$$u \times v = \bigcup\Big\{\{\langle x, y\rangle : x \in u\} : y \in v\Big\}.$$

(#19) Let $G(x) = \langle x, F(x)\rangle$ and using replacement, set

$$F \restriction a = G[a] = \{\langle x, F(x)\rangle : x \in a\}. \qquad \dashv$$

Next we establish the basic properties of ω, which models the natural numbers. The first—and most fundamental—is immediate from its definition:

Proposition 7C.3 (The Induction Principle). *For every set x,*

$$\Big(0 \in x \subseteq \omega\ \&\ (\forall n)[n \in x \Longrightarrow n' = n \cup \{n\} \in x]\Big) \Longrightarrow x = \omega.$$

This justifies in ZF^- the usual method of *proof by induction* of claims of the form

$$(\forall n \in \omega)P(n, \vec{y})$$

for any condition $P(n, \vec{y})$, taking $x = \{n \in \omega : P(n, \vec{y})\}$.

For a first, trivial application of the induction principle, we observe that:

Proposition 7C.4. (1) *If $x \in \omega$, then either $x = 0$ or $x = k \cup \{k\}$ for some $k \in \omega$.*

(2) Transitive(ω).

Proof. (1) is immediate from the definition of ω, since the set

$$\{x \in \omega : x = 0 \vee (\exists k \in \omega)[x = k \cup \{k\}]\}$$

contains 0 and is closed under the successor operation $k \mapsto k \cup \{k\}$.

(2) We prove by induction that $(\forall n \in \omega)[n \subseteq \omega]$. The basis is trivial since $0 = \emptyset \subseteq \omega$. In the induction step, assuming that $n \subseteq \omega$, we get immediately that $n' = n \cup \{n\} \subseteq \omega$. ⊣

Anticipating the next result, we set

$$m \leq_\omega n \iff m = n \vee m \in n, \quad (m, n \in \omega).$$

The proof of the next theorem is quite simple, but it depends essentially on the identification of $<_\omega$ with $\in$,

$$m <_\omega n \iff m \in n \quad (m, n \in \omega)$$

which is not a very natural (and so confusing) definition of a strict ordering condition and takes some getting used-to. It implies that for any set x,

$$\begin{aligned} y \text{ is } \leq_\omega\text{-minimal in } x &\iff y \text{ is } \in\text{-minimal in } x \\ &\iff y \in x \ \&\ (\forall t \in y)(t \notin x) \iff y \in x \ \&\ y \cap x = \emptyset. \end{aligned}$$

Theorem 7C.5 (Basic properties of ω)**.** *The relation $\leq_\omega$ on ω is a wellordering.*

It follows that ω is an ordinal, and every $n \in \omega$ is an ordinal.

Proof. We verify successively a sequence of properties of ω and $\leq_\omega$ which then together imply the statements in the theorem.

(a) *$\leq_\omega$ is wellfounded.*

Suppose that $x \subseteq \omega$ has no $\in$-minimal member. It is enough to show that for all $n \in \omega$, $n \cap x = \emptyset$, since this implies that $(n \cup \{n\}) \cap x = \emptyset$ for every $n \in \omega$ and so $x = \emptyset$.

The claim is trivial for $n = 0$, which has no members. In the inductive step, suppose $n \cap x = \emptyset$ but $(n \cup \{n\}) \cap x \neq \emptyset$; this means that $n \in x$, and n then is $\in$-minimal in x since none of its members are in x—contradicting the hypothesis.

(b) $\leq_\omega$ *is transitive*, i.e., $\Big(k \leq_\omega n \;\&\; n \leq_\omega m\Big) \Longrightarrow k \leq_\omega m$.

The claim here is that *each* $m \in \omega$ *is a transitive set* and we prove it by contradiction, using (a): if m is $\in$-minimal among the assumed non-transitive members of ω, it can't be 0 (which is transitive), and so $m = k \cup \{k\}$ for some k. Now $k \subseteq m$, and by the choice of m, $t \in k \Longrightarrow t \subseteq k \subseteq m$; hence $t \in m \Longrightarrow t \subseteq m$, which contradicts the assumption that m is not transitive.

(c) $\leq_\omega$ *is a partial ordering.*

We only need to show antisymmetry, so suppose that $m \leq_\omega n \leq_\omega m$. If $m \neq n$, this gives $m \in n \in m$ which contradicts (a), since it implies that the set $\{m, n\}$ has no $\in$-minimal element.

(d) $\leq_\omega$ *is a linear ordering.*

Notice first that by (a),

$$0 \neq m \in \omega \Longrightarrow 0 \in m;$$

because if m is not 0 and $\in$-least so that $0 \notin m$, then $m = k \cup \{k\}$ for some k by (a) of Proposition 7C.4, and then the choice of m yields an immediate contradiction.

Suppose now that the trichotomy law fails, and

(i) choose an $\in$-minimal n such that for some m

$$(*) \qquad m \notin n \;\&\; m \neq n \;\&\; n \notin m;$$

(ii) for this n, choose an $\in$-minimal m so that (*) holds.

By the first observation, $m, n \neq 0$, so for suitable k, l,

$$n = k \cup \{k\}, \quad m = l \cup \{l\}.$$

By (*), $m \notin k \cup \{k\}$, and so $m \notin k, m \neq k$; but then the choice of n means that

$$k \in m = l \cup \{l\}.$$

By (*) again, $n \notin m = l \cup \{l\}$, so $n \notin l, n \neq l$; but then the choice of m means that

$$l \in n = k \cup \{k\}.$$

Since $k \neq l$ (otherwise $n = m$), the last two displayed formulas imply that

$$k \in l \;\&\; l \in k,$$

which in turn implies that the set $\{k, l\} \subseteq \omega$ has no $\in$-minimal element, contradicting (a).

Now (a) and (d) together with (2) of Proposition 7C.4 mean exactly that ω is an ordinal. Moreover, since each $n \in \omega$ is a subset of ω, the restriction of $\in$ to n is a wellordering; and n is a transitive set by the transitivity of $\leq_\omega$, since

$$k \in m \in n \Longrightarrow k \leq_\omega m \leq_\omega n \Longrightarrow k \leq_\omega n \Longrightarrow k \in n,$$

the last because the alternative by (d) would produce a subset of ω with no $\in$-minimal element, as above. $\dashv$

Theorem 7C.6 (Definition by recursion on ω)**.** *From any two, given operations $G(\vec{x}), H(s, n, \vec{x})$, we can define an operation $F(n, \vec{x})$ such that*

$$\begin{aligned} F(0, \vec{x}) &= G(\vec{x}), \\ F(n', \vec{x}) &= H(F(n, \vec{x}), n, \vec{x}) \quad (n \in \omega). \end{aligned}$$

In particular, with no parameters, from any a and $H(s, n)$, we can define a function $\overline{f} : \omega \to \mathcal{V}$ such that

$$\overline{f}(0) = a, \quad \overline{f}(n') = H(F(n), n).$$

Proof. Set

$$\begin{aligned} P(n, \vec{x}, f) \iff n \in \omega \ \&\ &\text{Function}(f) \\ &\&\ \text{Domain}(f) = n' \ \&\ f(0) = G(\vec{x}) \\ \&\ (\forall m \in \text{Domain}(f))&[m' \in \text{Domain}(f) \Longrightarrow f(m') = H(f(m), m, \vec{x})]. \end{aligned}$$

Immediately from the definition

$$P(0, \vec{x}, f) \iff f = \{\langle 0, G(\vec{x}) \rangle\}, \quad P(n', \vec{x}, f) \Longrightarrow P(n, \vec{x}, f \setminus \{\langle n, f(n) \rangle\}),$$

and using these we can show easily by induction that

$$(\forall n \in \omega)(\exists! f) P(n, \vec{x}, f).$$

The required operation is

$$F(n, \vec{x}) = w \iff (\exists f)[P(n', \vec{x}, f) \ \&\ f(n) = w].$$

For the second claim, we apply the first with no parameters $\vec{x}$ to get $F(n)$ such that

$$F(0) = a, \quad F(n') = H(F(n), n),$$

and then appeal to the Replacement Axiom to set

$$\overline{f} = \{\langle n, F(n) \rangle : n \in \omega\}. \qquad \dashv$$

Corollary 7C.7. *Every set x is a member of some transitive set.*

Proof. By Theorem 7C.6, for each x there is a function $\text{TC}_x : \omega \to \mathcal{V}$ satisfying the equations

$$\text{TC}_x(0) = \{x\}, \quad \text{TC}_x(n') = \bigcup \text{TC}_x(n).$$

Let $y = \bigcup \text{TC}_x[\omega]$. Clearly $x \in y$ and y is transitive—because if $t \in u \in y$, then there is some n such that $t \in u \in \text{TC}_x(n)$ and so $t \in \text{TC}_x(n') \subseteq y$. $\dashv$

The *transitive closure of* x is the $\subseteq$-least transitive set which contains x as a member,

$$(172)\quad \mathrm{TC}(x) = \bigcup \mathrm{TC}_x[\omega] = \bigcup_{n\in\omega} \mathrm{TC}_x(n) = \bigcap\{z : \mathrm{Transitive}(z)\ \&\ x \in z\}.$$

It is easy to check that if x is transitive, then $\mathrm{TC}(x) = x \cup \{x\}$, cf. Problem x7.8.

Note. Sometimes the transitive closure of x is defined as the least transitive set which contains x as a subset,

$$(173)\quad \mathrm{TC}'(x) = \bigcap\{y \in \mathrm{TC}(x) : \mathrm{Transitive}(y)\ \&\ x \subseteq y\}.$$

Normally, $\mathrm{TC}'(x) = \mathrm{TC}(x) \setminus \{x\}$, but it could be that $\mathrm{TC}'(x) = \mathrm{TC}(x)$ if $x \in x$—which is not ruled out without assuming the Foundation Axiom!

We collect in one definition some basic and familiar conditions on sets whose definition refers to ω and the transitive closure operation.

Definition 7C.8. (1) Two sets are *equinumerous* if their members can be put into a one-to-one correspondence, i.e.,

$$x =_c y \iff (\exists f)[f : x \rightarrowtail\!\!\!\!\twoheadrightarrow y];$$

x is *no larger than* y *in size* if x can be embedded in y,

$$x \leq_c y \iff (\exists f)[f : \rightarrowtail y];$$

and x is *smaller than* y *in size* if the converse does not hold,

$$x <_c y \iff x \leq_c y\ \&\ x \neq_c y.$$

(2) A set x is *finite* if $x =_c n$ for some $n \in \omega$; and it is *hereditarily finite* if $\mathrm{TC}(x)$ is finite.

(3) A set x is *countable* (or *denumerable*, or *enumerable*) if either it is finite or equinumerous with ω; and it is *hereditarily countable* if $\mathrm{TC}(x)$ is countable.

(4) A set x is *grounded* (wellfounded) if the restriction of $\in$ to $\mathrm{TC}(x)$ is a wellfounded relation, in symbols

$$x \text{ is grounded} \iff \mathrm{WF}(\{\langle s,t\rangle \in \mathrm{TC}(x) \times \mathrm{TC}(x) : s \in t\}).$$

Next we establish the basic properties of the class ON of ordinal numbers, which suggest that it is a (very long) *number system*, a proper-class-size extension of ω. As with the results about ω, the (similar) proofs about ON are simple, but they depend essentially on the somewhat perverse identification of $<_\xi$ on each $\xi \in \mathrm{ON}$ and $<_{\mathrm{ON}}$ on ON with $\in$,

$$x <_\xi y \iff x \in y, \quad \eta <_{\mathrm{ON}} \xi \iff \eta \in \xi.$$

Theorem 7C.9 (Basic properties of ON)**.** (1) ON *is a transitive class wellordered by* $\leq_{\mathrm{ON}}$*, i.e., for all* $\eta, \zeta, \xi \in \mathrm{ON}$,

$$\xi \in \mathrm{ON} \Longrightarrow \xi \subseteq \mathrm{ON},$$
$$\eta \leq_{\mathrm{ON}} \zeta \leq_{\mathrm{ON}} \xi \Longrightarrow \eta \leq_{\mathrm{ON}} \xi, \quad (\eta \leq_{\mathrm{ON}} \xi \ \&\ \xi \leq_{\mathrm{ON}} \eta) \Longrightarrow \eta = \xi,$$
$$\eta \leq_{\mathrm{ON}} \xi \vee \eta = \xi \vee \xi \leq_{\mathrm{ON}} \eta,$$

and every non-empty class $A \subseteq \mathrm{ON}$ *has an* $\leq_{\mathrm{ON}}$*-least member.*
In other words:

$$\eta \in \zeta \in \xi \Longrightarrow \eta \in \xi, \qquad \eta \in \xi \vee \eta = \xi \vee \xi \in \eta,$$
$$\exists \eta \in A \subseteq \mathrm{ON} \Longrightarrow (\exists \xi \in A)(\forall \eta \in \xi)[\eta \notin A].$$

(2) *For each* $\xi \in \mathrm{ON}$, $\xi' = \xi \cup \{\xi\}$ *is the successor of* ξ *in* $\leq_{\mathrm{ON}}$*, i.e.,*

$$\xi <_{\mathrm{ON}} \xi' \ \&\ (\forall \eta)[\xi <_{\mathrm{ON}} \eta \Longrightarrow \xi \leq_{\mathrm{ON}} \eta].$$

(3) *Every ordinal is grounded.*

(4) *For every* $x \subseteq \mathrm{ON}$,

$$\bigcup x = \sup\{\xi : \xi \in x\} = \text{the least ordinal } \eta \text{ such that } (\forall \xi \in x)[\xi \leq_{\mathrm{ON}} \eta].$$

(5) *For every ordinal* ξ*, exactly one of the following three conditions holds:*

(i) $\xi = 0$.
(ii) ξ *is a successor ordinal, i.e.,* $\xi = \eta' = \eta \cup \{\eta\}$ *for a unique* $\eta < \xi$.
(iii) ξ *is a limit ordinal, i.e.,* $(\forall \eta <_{\mathrm{ON}} \xi)[\eta' <_{\mathrm{ON}} \xi]$ *and* $\xi = \bigcup \xi$.

It follows, in particular, that ON *is a proper class.*

Proof. We first show three properties of ON and $\leq_{\mathrm{ON}}$ which together imply (1).

(a) ON *is transitive*, i.e., every member of an ordinal is an ordinal.

Suppose, towards a contradiction, that $\xi \in \mathrm{ON}$ but $\xi \not\subseteq \mathrm{ON}$. Since $\leq_\xi$ wellorders ξ, there is a $\leq_\xi$-least $x \in \xi$ which is not an ordinal. Since ξ is transitive, $x \subseteq \xi$, and x is also transitive, because

$$s \in t \in x \Longrightarrow s <_\xi t <_\xi x \Longrightarrow s <_\xi x \Longrightarrow s \in x.$$

Moreover, x is wellorderd by the relation $\leq_x$ because $\leq_x = \leq_\xi \cap (x \times x)$. It follows that $x \in \mathrm{ON}$, which is a contradiction.

(b) *The condition* $\leq_{\mathrm{ON}}$ *is wellfounded*, i.e., for all classes A,

$$\emptyset \neq A \subseteq \mathrm{ON} \Longrightarrow (\exists \xi \in A)(\forall \eta \in A)[\eta \not<_{\mathrm{ON}} \xi].$$

Supposed $\emptyset \neq A \subseteq \mathrm{ON}$ and choose some $\xi \in A$. If ξ is $\in$-minimal in A, there is nothing to prove. If not, then there is some $\eta \in (\xi \cap A)$ and ξ is wellordered by $\leq_\xi$, so there is an $\in$-least η in $\xi \cap A$. We claim that this η is $\in$-minimal in A; if not, then there is some $\zeta \in A$ such that $\zeta <_{\mathrm{ON}} \eta$, which means that $\zeta \in \eta$—but then $\zeta \in \xi$, since ξ is transitive, and this contradicts the choice of η.

(c) *For any two ordinals η, ξ,*

$$(*) \qquad \eta \in \xi \vee \eta = \xi \vee \xi \in \eta.$$

Assume not, and choose by (a) an $\in$-minimal ξ so that $(*)$ fails for some η, and then choose an $\in$-minimal η for which $(*)$ fails with this ξ. In particular, $\xi \neq \eta$.

If $x \in \eta$, then $\xi \in x \vee x = \xi \vee x \in \xi$ by the choice of η, and the first two of these alternatives are not possible, because they both imply $\xi \in \eta$ which implies $(*)$; it follows that $x \in \xi$, and since x was an arbitrary member of η, $\eta \subseteq \xi$.

If $x \in \xi$, then $\eta \in x \vee \eta = x \vee x \in \eta$ by the choice of ξ, and the first two of these alternatives are not possible because they both imply $\eta \in \xi$ which again implies $(*)$; it follows that $x \in \eta$, so that $\xi \subseteq \eta$—which together with together with the conclusion of the preceding paragraph gives $\xi = \eta$, and that contradicts our hypothesis.

Now (a), (b) and (c) complete the proof of (1) in the theorem.

(2) – (5) and the claim that ON is a proper class follow from (1) and simple or similar arguments and we leave them for problems. ⊣

We will not cover *ordinal arithmetic* in this class (except for a few problems), but it is convenient to introduce the notation

$$\xi + 1 = \xi' = \xi \cup \{\xi\}$$

which is part of the definition of *ordinal addition*. We will also use a limit notation for increasing sequences of ordinals,

$$\lim_{n\to\infty} \xi_n = \sup\{\xi_n : n \in \omega\} \qquad (\xi_0 < \xi_1 < \cdots).$$

Theorem 7C.10 (Wellfounded recursion)**.** *For each operation $G(f,t)$ and each wellfounded relation r, there is exactly one function $\overline{f} : \mathrm{Field}(r) \to \mathcal{V}$ such that*

$$(174) \qquad \overline{f}(t) = G(\overline{f} \restriction \{s : s <_r t\}, t) \qquad (t \in \mathrm{Field}(r)).$$

Moreover, if $G(f,t) = H(f,t,\vec{x})$ with a definable operation $H(f,t,\vec{x})$, then there is a definable operation $H^*(t,r,\vec{x})$ such that for every wellordering $\leq$, $\overline{f}(t) = H^*(t,\leq,\vec{x})$.

Proof. Define "f is a piece of the function we want" by

$$\begin{aligned} P(f) \iff & \mathrm{Function}(f) \;\&\; \mathrm{Domain}(f) \subseteq \mathrm{Field}(r) \\ & \& \; (\forall t \in \mathrm{Domain}(f))(\forall s \in \mathrm{Field}(r))[s <_r t \Longrightarrow s \in \mathrm{Domain}(f)] \\ & \qquad \& \; (\forall t \in \mathrm{Domain}(f))[f(t) = G(f \restriction \{s : s <_r t\}, t)]. \end{aligned}$$

Lemma. If $P(f), P(g)$ and $t \in \mathrm{Domain}(f) \cap \mathrm{Domain}(g)$, then $f(t) = g(t)$.

Proof. Suppose not, let f, g witness the failure of the Lemma, and let $t \in \text{Field}(r)$ be $\leq_r$-minimal such that $f(t) \neq g(t)$. We know that

$$\{s : s <_r t\} \subseteq \text{Domain}(f) \cap \text{Domain}(g) \;\&\; f \restriction \{s : s <_r t\} = g \restriction \{s : s <_r t\}$$

by the definition of the condition P and the choice of t, and so by the definition of P, again,

$$f(t) = G(f \restriction \{s : s <_r t\}, t) = G(g \restriction \{s : s <_r t\}, t) = g(t),$$

contradicting the choice of t. (Lemma) $\dashv$

Set now

$$y = \Big\{t \in \text{Field}(r) : (\exists f)[P(f) \;\&\; t \in \text{Domain}(f)]\Big\},$$
$$Q(t, w) \iff t \in y \;\&\; (\exists f)[P(f) \;\&\; f(t) = w].$$

The Lemma insures that

$$(\forall t \in y)(\exists! w) Q(t, w),$$

and so the Replacement Scheme guarantees a function $\overline{f}$ with $\text{Domain}(\overline{f}) = y$ such that

$$\overline{f}(t) = G(\overline{f} \restriction \{s : s <_r t\}, t) \quad (t \in y),$$

so to conclude the proof, we only need verify that $y = \text{Field}(r)$. Suppose this fails, choose an r-minimal $t \in \text{Field}(r) \setminus y$ and set

$$f^* = \overline{f} \cup \{\langle t, G(\overline{f}, t)\rangle\}.$$

This is a function and it is easy to verify (directly from the definition) that $P(f^*)$, so $f^* \subseteq \overline{f}$, contradicting the assumption. $\dashv$

The next three, basic theorems are among the numerous applications of wellfounded recursion. We verify first a simple lemma about wellorderings which deserves separate billing:

Lemma 7C.11. *Suppose* $\text{WO}(\leq)$ *and* $\pi : \text{Field}(\leq) \rightarrowtail \text{Field}(\leq)$ *is an injection which preserves the strict ordering, i.e.,*

$$x < y \Longrightarrow \pi(x) < \pi(y);$$

it follows that for every $x \in \text{Field}(\leq)$, $x \leq \pi(x)$.

Proof. Assume the opposite and let x be $\leq$-least in $\text{Field}(\leq)$ such that $\pi(x) < x$; by the hypothesis then, $\pi(\pi(x)) < \pi(x)$, which contradicts the choice of x. $\dashv$

In the next theorem we confuse—as is common—an ordinal ξ with the wellordering $\leq_\xi$ which is determined by ξ.

Theorem 7C.12. *Every wellordering $\leq$ is similar with exactly one ordinal*

(175) $$\mathrm{ot}(\leq) = \text{the unique } \xi \in \mathrm{ON} \text{ such that } \leq =_o \leq_\xi .$$

The ordinal $\mathrm{ot}(\leq)$ is the *order type* or *length* of $\leq$.

Proof. Let

$$G(f,t) = f[\{s \in \mathrm{Field}(\leq) : s < t\}] = \{f(s) : s < t\}$$

when $t \in \mathrm{Field}(\leq)$ & $\mathrm{Function}(f)$ & $\{s : s < t\} \subseteq \mathrm{Domain}(f)$, and set $G(f,t) = 0$ (or any other, irrelevant value) otherwise. By Theorem 7C.10, there exists a function $\pi : \mathrm{Field}(\leq) \to \mathcal{V}$ such that

(176) $$\pi(t) = \Big\{\pi(s) : s < t\Big\} = G(\pi \restriction \{s : s < t\}, t).$$

We verify that the image

$$\xi = \pi[\mathrm{Field}(\leq)]$$

is the required ordinal and π is the required similarity. This is trivial if $\mathrm{Field}(\leq) = \emptyset$, so we assume that we are dealing with a non-trivial wellordering.

For any $\emptyset \neq x \subseteq \mathrm{Field}(\leq)$, let

$$\min(x) = \text{the } \leq\text{-least } t \in x.$$

(1) ξ *is transitive.*

Because if $x \in \pi(t) \in \xi$, then $x \in \{\pi(t') : t' < t\}$, so $x = \pi(t')$ for some t' and $x \in \xi$.

(2) $\pi : \mathrm{Field}(\leq) \rightarrowtail\!\!\!\!\rightarrow \xi$ *is a bijection.*

It is a surjection by the definition, so assume that it is not injective, let

$$t = \min\{t' : \text{for some } s > t', \pi(t') = \pi(s)\},$$

and choose some s which witnesses the characteristic property of t, i.e.,

$$t < s \;\&\; \{\pi(t') : t' < t\} = \pi(t) = \pi(s) = \{\pi(s') : s' < s\}.$$

Since $t < s$, $\pi(t) \in \pi(s) = \pi(t)$ and so there is some $t' < t$ such that $\pi(t) = \pi(t')$, which contradicts the choice of t.

(3) $s < t \iff \pi(s) \in \pi(t)$.

Immediately from the definition, $s < t \Longrightarrow \pi(s) \in \{\pi(t') : t' < t\} = \pi(t)$. For the converse, assume that $\pi(s) \in \pi(t)$ but $s \not< t$ and consider the two possibilities.

(i) $s = t$, so that $\pi(s) = \pi(t)$ and $\pi(t) \in \pi(t) = \{\pi(t') : t' < t\}$; so $\pi(t) = \pi(t')$ for some $t' < t$ contradicting (2).

(ii) $t < s$, so that by the forward direction

$$\{\pi(t') : t' < t\} = \pi(t) \in \pi(s) \in \pi(t);$$

so $\pi(s) = \pi(t')$ for some $t' < t < s$, which also contradicts (2).

(2) and (3) together give us that

$$s \leq t \iff \pi(s) = \pi(t) \vee \pi(s) \in \pi(t) \iff \pi(s) \leq_\xi \pi(t),$$

and so $\pi : \text{Field}(\leq) \rightarrowtail\!\!\!\!\twoheadrightarrow \xi$ carries the wellordering $\leq$ to the relation $\leq_\xi$, which is then a wellordering. And since ξ is also transitive by (1), it is an ordinal and π is a similarity.

Finally, to prove that $\leq$ cannot be similar to two, distinct ordinals, assume the opposite, i.e.,

$$\leq_\xi =_o \leq =_o \leq_\eta \text{ for some } \xi < \eta.$$

It follows that $\xi =_o \eta$, and so we have a similarity $\pi : \eta \rightarrowtail\!\!\!\!\twoheadrightarrow \xi$ such that $\pi(\xi) <_\eta \xi$. But $\pi : \eta \rightarrowtail \eta$ is an injection which preserves the strict ordering, and so $\xi \leq_\eta \pi(\xi)$ by Lemma 7C.11, which is a contradiction. $\dashv$

Definition 7C.13. A *decoration* or *Mostowski surjection* of a relation r is any function $d : \text{Field}(r) \to \mathcal{V}$ such that

(177) $$d(u) = \{d(v) : \langle v, u\rangle \in r\} \qquad (u \in \text{Field}(r)).$$

A set x is *wellorderable* if it admits a wellordering,

(178) $$\text{WOable}(x) \iff (\exists r)[\text{WO}(r) \;\&\; x = \text{Field}(r)].$$

It is easy to check that the class WOable is closed under (binary) unions and cartesian products, cf. Problem x7.30.

Theorem 7C.14 (Mostowski Collapsing Lemma)**.** (1) *Every grounded relation r admits a unique decoration, d_r.*

(2) *A set x is grounded if and only if there exists a grounded relation r such that $x \in d_r[\text{Field}(r)]$. Moreover, is $\text{TC}(x)$ is wellorderable, then we can choose r so that $\text{Field}(r)$ is an ordinal.*

Proof. (1) is immediate by wellfounded recursion—in fact the required decoration which satisfies (177) is defined exactly like the similarity π in the proof of Theorem 7C.12, only we do not assume that r is a wellordering.

(2) Suppose x is grounded, let

$$r = \{\langle u, v\rangle \in \text{TC}(x) \times \text{TC}(x) : u \in v\},$$

and let $d_r : \text{TC}(x) \to \mathcal{V}$ be the unique decoration of r. Notice that d_r is the identity on its domain,

$$d_r(u) = u \quad (u \in \text{TC}(x));$$

because if u is an $\in$-minimal counterexample to this, then

$$\begin{aligned} d_r(u) &= \{d_r(v) : v \in \text{TC}(x) \;\&\; v \in u\} \\ &= \{v : v \in \text{TC}(x) \;\&\; v \in u\} = \{v : v \in u\} = u, \end{aligned}$$

by the choice of u and the fact that $\mathrm{TC}(x)$ is transitive, which insures that $u \subseteq \mathrm{TC}(x)$. In particular, $d_r(x) = x$, as required.

If $\mathrm{TC}(x)$ is wellorderable, then there is a bijection $\pi : \lambda \rightarrowtail\!\!\!\!\twoheadrightarrow \mathrm{TC}(x)$ of an ordinal λ with it, and we can use this bijection to carry r to λ,

$$r' = \{\langle \xi, \eta \rangle \in \lambda \times \lambda : \pi(\xi) \in \pi(\eta)\}.$$

Easily

$$d_{r'}(\xi) = d_r(\pi(\xi)),$$

directly from the definitions of these two decorations, and so if $\pi(\xi) = x$, then $d_{r'}(\xi) = d_r(x) = x$. ⊣

There is an immediate, "foundational" consequence of the Mostowski collapsing lemma: if we know all the sets of ordinals, then we know all grounded sets. The theorem also has important mathematical implications, especially in its "class form", cf. Problems x7.18*, x7.19*.

Finally, we extend to the class of ordinals the principles of *proof by induction* and *definition by recursion*:

Theorem 7C.15 (Ordinal induction). *If* $A \subseteq \mathrm{ON}$ *and*

$$(\forall \xi \in \mathrm{ON})\Big((\forall \eta \in \xi)(\eta \in A) \Longrightarrow \xi \in A\Big),$$

then $A = \mathrm{ON}$.

Proof. Assume the hypothesis on A and (toward a contradiction) that $\xi \notin A$ for some ξ. The hypothesis implies that $\eta \notin A$ for some $\eta \in \xi$; so let $\eta^* = \min\{\eta \in \xi : \eta \notin A\}$ and infer

$$(\forall \eta < \eta^*)(\eta \in A), \quad \eta^* \notin A$$

from the choice of η^*, which contradicts the hypothesis. ⊣

Theorem 7C.16 (Ordinal recursion). *For any operation* $G : \mathcal{V}^2 \to \mathcal{V}$, *there is an operation* $F : \mathrm{ON} \to \mathcal{V}$ *such that*

$$F(\xi) = G(F \upharpoonright \xi, \xi) \quad (\xi \in \mathrm{ON}). \tag{179}$$

More generally, for any operation $G : \mathcal{V}^{m+2} \to \mathcal{V}$ *there is an operation* $F : \mathcal{V}^{m+1} \to \mathcal{V}$ *such that*

$$F(\xi, \vec{x}) = G(\{F(\eta, \vec{x}) : \eta \in \xi\}, \xi, \vec{x}) \quad (\xi \in \mathrm{ON}).$$

Moreover, in both cases, if G *is definable, then so is* F.

Proof. For the first claim, we apply Theorem 7C.10 to obtain for each ξ a unique function $\overline{f}_\xi : \xi \to \mathcal{V}$ such that

$$\overline{f}_\xi(\eta) = G(\overline{f}_\xi \upharpoonright \eta, \eta) \quad (\xi \in \mathrm{ON})$$

and verify easily that these functions *cohere*, i.e.,

$$\eta < \zeta < \xi \Longrightarrow \overline{f}_\zeta(\eta) = \overline{f}_\xi(\eta).$$

We then set

$$F(\xi) = \overline{f}_{\xi+1}(\xi) \ (= \overline{f}_\zeta(\xi) \text{ (for any } \zeta > \xi).$$

The case with parameters is proved similarly, and the last claim follows from the uniformity of the argument. ⊣

Ordinal recursion is (perhaps) the most basic tool that we will use in this chapter. Many of its applications are theorems of ZF, because they require the Powerset Axiom, but it is worth including here a few, simple corollaries of it which can be established in ZF^-.

A partially ordering $\leq$ is *chain-complete* if every chain has a least upper bound in $\leq$. One needs the Powerset Axiom to construct interesting chain-complete posets, but the basic fact about them can be proved in ZF^-:

Proposition 7C.17 (The Fixed Point Theorem)**.** *If $\leq$ is a chain-complete partial ordering, $\pi : \mathrm{Field}(\leq) \to \mathrm{Field}(\leq)$ and for every $x \in \mathrm{Field}(\leq)$, $x \leq \pi(x)$, then $\pi(x^*) = x^*$ for some x^*.*

Proof. Notice first that every chain-complete poset has a least element,

$$\perp_\leq = \sup_\leq(\emptyset).$$

Assume, towards a contradiction that $x < \pi(x)$ for all $x \in \mathrm{Field}(\leq)$, and define $F : \mathrm{ON} \to \mathrm{Field}(\leq)$ by

$$F(\xi) = \begin{cases} \perp_\leq, & \text{if } \xi = 0,\\ \pi(F(\eta)), & \text{if } \xi = \eta + 1,\\ \sup_\leq(\{F(\eta) : \eta < \xi\}), & \text{otherwise.} \end{cases}$$

It is easy to check (by transfinite induction on ξ) that

$$\eta \leq \xi \Longrightarrow F(\eta) \leq F(\xi);$$

but then there must be some ξ such that

$$x = F(\xi) = F(\xi + 1) = \pi(x),$$

otherwise F injects the class of ordinals into the set $\mathrm{Field}(\leq)$, so that $\mathrm{ON} = F^{-1}(\mathrm{Field}(\leq))$ is a set. ⊣

Definition 7C.18. A class K of ordinals is *unbounded* if

$$(\forall \xi)(\exists \eta > \xi)[\eta \in K];$$

and K is *closed* if for every limit ordinal λ,

$$(\forall \eta < \lambda)(\exists \zeta)[\eta < \zeta < \lambda \,\&\, \zeta \in K] \Longrightarrow \lambda \in K,$$

i.e., if K is closed in the natural order topology on ON.

Proposition 7C.19. (1) *If K_1 and K_2 are closed, unbounded classes of ordinals, then $K_1 \cap K_2$ is also closed and unbounded.*

(2) *If $F : \mathrm{ON} \to \mathrm{ON}$ is a class operation on ordinals, then the class*

$$K^* = \{\xi : (\forall \eta < \xi)[F(\eta) < \xi]\}$$

is closed and unbounded.

Proof. (1) $K_1 \cap K_2$ is obviously closed. To see that it is unbounded, given ξ, define (by recursion on ω) $\xi_0, \xi_1, \xi_2, \dots$ so that

$$\begin{array}{ccc} \xi < \xi_0 & \text{and} & \xi_0 \in K_1, \\ \xi_0 < \xi_1 & \text{and} & \xi_1 \in K_2, \\ \xi_1 < \xi_2 & \text{and} & \xi_2 \in K_1, \\ & \text{etc.} & \end{array}$$

and check that $\xi^* = \lim_n \xi_n \in K_1 \cap K_2$ because both K_1, K_2 are closed.

(2) Again, K^* is obviously closed. Given ξ, define ξ_n the recursion on ω,

$$\xi_0 = \xi$$
$$\xi_{n+1} = \text{the least } \xi \text{ such that supremum}\{f(\eta) : \eta < \xi_n\} + 1 < \xi$$

where the supremum exists by replacement and verify that $\eta = \xi_0 < \xi_1 < \cdots$ and $\lim_{n\to\infty} \xi_n \in K^*$. ⊣

Next we collect the few, basic results about *equinumerocity* which can be proved in ZF^-.

Theorem 7C.20. (1) *For any sets x, y, z, $x =_c y \Longrightarrow x \leq_c y$ and*

$$x =_c x, \quad x =_c y \Longrightarrow y =_c x, \quad (x =_c y =_c z) \Longrightarrow x =_c z,$$
$$(x \leq_c y \leq_c z) \Longrightarrow x \leq_c z.$$

(2) (The Schröder-Bernstein Theorem). *For any two sets x, y,*

$$(x \leq_c y \ \&\ y \leq_c x) \Longrightarrow x =_c y.$$

(1) is trivial, but the Schröder-Bernstein Theorem is actually quite difficult, cf. Problem x7.29*.

Every wellorderable set is equinumerous with an ordinal number by the basic Theorem 7C.12, and so we can measure their size—and compare them—using ordinals.

Definition 7C.21 (von Neumann cardinals). Set

$$\begin{array}{rcl} |x| & = & \text{the least } \xi \in \mathrm{ON} \text{ such that } x =_c \xi \quad (\mathrm{WOable}(x)), \\ \mathrm{Card}(\kappa) & \Longleftrightarrow & (\exists x)[\mathrm{WOable}(x) \ \&\ \kappa = |x|] \\ & \Longleftrightarrow & (\forall \xi \in \kappa)[\xi <_c \kappa], \end{array}$$

and on the class Card define

$$\kappa + \lambda = |\kappa \uplus \lambda| \quad (\kappa, \lambda \in \text{Card}),$$
$$\kappa \cdot \lambda = |\kappa \times \lambda| \quad (\kappa, \lambda \in \text{Card}).$$

Set also

$$\sum_{\eta<\zeta} \kappa_\eta = \Big|\{\langle \eta, \xi \rangle : \xi \in \kappa_\eta\}\Big|,$$

where $\{\eta \mapsto \kappa_\eta\}_{\eta \in \zeta} : \zeta \to \text{Card}$ is any function from an ordinal ζ with cardinal values.

Theorem 7C.22. (1) *Each $n \in \omega$ and ω are cardinals.*

(2) $\kappa + 0 = \kappa;\ \kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu;\ \kappa + \lambda = \lambda + \kappa.$

(3) *The absorption law for addition:*

$$\omega \leq \max\{\kappa, \lambda\} \Longrightarrow \kappa + \lambda = \max\{\kappa, \lambda\}.$$

(4) $\kappa \cdot 0 = 0,\ \kappa \cdot 1 = \kappa;\ \kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu;\ \kappa \cdot \lambda = \lambda \cdot \kappa,\ \kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu.$

(5) *The absorption law for multiplication:*

$$\Big(\kappa, \lambda \neq 0 \ \&\ \omega \leq \max\{\kappa, \lambda\}\Big) \Longrightarrow \kappa \cdot \lambda = \max\{\kappa, \lambda\}.$$

(6) $\Big(|\zeta| \leq \kappa \ \&\ (\forall \eta \in \zeta)[\kappa_\eta \leq \kappa] \ \&\ \kappa \geq \omega\Big) \Longrightarrow \sum_{\eta<\zeta} \kappa_\eta \leq \kappa.$

We leave the proofs the problems; (1) – (4) are easy, if a bit fussy, and (6) follows immediately from (5), but the absorption law for multiplication is not trivial. Of course nothing in this theorem produces an infinite cardinal greater than ω—and we will show that, indeed, it is consistent with ZF^- that ω is the only infinite cardinal number.

7D. Set theory without AC or foundation, ZF

We now add the Powerset Axiom and start with two, basic results about cardinality which can be established without the Axiom of Choice.

Theorem 7D.1 (ZF, Cantor's Theorem)**.** *For every set x, $x <_c \mathcal{P}(x)$.*

Proof is left for Problem x7.38. ⊣

This gives an infinite sequence of ever increasing infinite size

$$\omega <_c \mathcal{P}(\omega) <_c \mathcal{P}(\mathcal{P}(\omega)) <_c \cdots,$$

perhaps Cantor's most important discovery. But we cannot prove in ZF that *every two sets are $\leq_c$-comparable* which, as we will see, is equivalent to the Axiom of Choice. The best we can do without **AC** in this direction is the following, simple but very useful fact:

Theorem 7D.2 (ZF, Hartogs' Theorem)**.** *For every set x, there is an ordinal ξ which cannot be injected into x,*

$$(\forall x)(\exists \xi \in \mathrm{ON})[\xi \not\leq_c x].$$

Proof. Assume towards a contradiction that every ordinal can be injected into x and set

$$y = \Big\{\mathrm{ot}(r) : r \subseteq x \times x \;\&\; \mathrm{WO}(r)\Big\}.$$

This is the image of a subset of $\mathcal{P}(x \times x)$ by a class operation, and so it is a set. The assumption on x implies that $y = \mathrm{ON}$, contradicting the fact that ON is not a set. ⊣

An immediate consequence of Hartogs' Theorem is that

$$(\forall \eta \in \mathrm{ON})(\exists \xi \in \mathrm{ON})[\eta <_c \xi]$$

and so we can define the *next cardinal operation*:

(180) $$\kappa^+ = \text{the least } \lambda \in \mathrm{Card} \text{ such that } \kappa < \lambda;$$

and we can iterate this operation:

Definition 7D.3 (ZF, the alephs)**.** We define for each ξ the *ξ'th infinite cardinal number* $\aleph_\xi$ by the ordinal recursion

$$\begin{aligned}\aleph_0 &= \omega,\\ \aleph_{\xi+1} &= \aleph_\xi^+\\ \aleph_\lambda &= \sup\{\aleph_\xi : \xi < \lambda\}, \text{ if } \lambda \text{ is a limit ordinal.}\end{aligned}$$

It is easy to check that every infinite cardinal κ is $\aleph_\xi$, for some ξ and that

$$\eta < \xi \Longrightarrow \aleph_\eta <_c \aleph_\xi,$$

cf. Problem x7.37.

We can iterate in the same way the powerset operation:

Definition 7D.4 (ZF, the cumulative hierarchy of grounded sets)**.** Define V_ξ for each $\xi \in \mathrm{ON}$ by the ordinal recursion

$$\begin{aligned}V_0 &= \emptyset\\ V_{\xi+1} &= \mathcal{P}(V_\xi),\\ V_\lambda &= \textstyle\bigcup_{\xi<\lambda} V_\xi, \text{ if } \lambda \text{ is a limit ordinal,}\end{aligned}$$

and set

$$\mathrm{rank}(x) = \text{the least } \xi \text{ such that } x \in V_{\xi+1} \quad (x \in \textstyle\bigcup_{\xi \in \mathrm{ON}} V_\xi).$$

Let also V be the class of all grounded sets,

$$V = \{x : \mathrm{WF}(\{\langle s, t\rangle \in \mathrm{TC}(x) \times \mathrm{TC}(x) : s \in t\})\}.$$

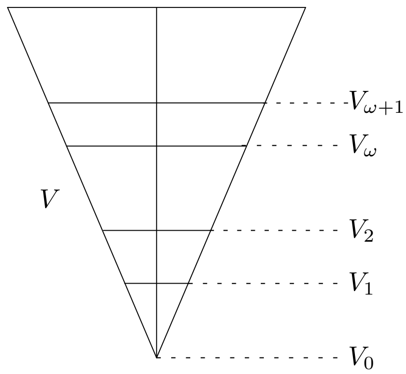


Figure 2

Theorem 7D.5 (ZF)**.** (1) *Each V_ξ is a transitive, grounded set,*

$$\eta \leq \xi \Longrightarrow V_\eta \subseteq V_\xi,$$

and $V = \bigcup_{\xi \in \mathrm{ON}} V_\xi$, i.e., every grounded set occurs in some V_ξ.

(2) *If $x \subseteq V$, then $x \in V$.*

(3) *The von Neumann universe V is a proper, transitive class.*

(4) *For each ordinal ξ, $\mathrm{rank}(\xi) = \xi$, so that, in particular, the operation $\xi \mapsto V_\xi$ is strictly increasing.*

Proof is left for the problems. ⊣

This hierarchy of partial universes gives a precise version of the intuitive construction for the universe of sets which we discussed in the introduction to this chapter, where *for stages we take the ordinals.* It suggests strongly that the Axiom of Foundation is true and, indeed, there is no competing intuitive idea of "what sets are" which justifies the axioms of ZF without also justifying foundation. We will not make it part of our "standard theory" yet, mostly because it is simply not needed for what we will do—and it is also not needed for developing classical mathematics in set theory.

Definition 7D.6 (Relativization)**.** For each definable class M and each $\mathbb{FOL}(\in)$-formula ϕ, we define recursively the *relativization* $(\phi)^M$ *of ϕ to M*:

$$(\mathbf{v}_i \in \mathbf{v}_j)^M :\equiv \mathbf{v}_i \in \mathbf{v}_j, (\mathbf{v}_i = \mathbf{v}_j)^M :\equiv \mathbf{v}_i = \mathbf{v}_j$$

$$(\neg\phi)^M :\equiv \neg\phi^M,\ (\phi \;\&\; \psi)^M :\equiv \phi^M \;\&\; \psi^M,$$

$$(\phi \vee \psi)^M :\equiv \phi^M \vee \psi^M,\ (\phi \rightarrow \psi)^M :\equiv \phi^M \rightarrow \psi^M,$$

$$(\exists \mathbf{v}_i \phi)^M :\equiv \exists \mathbf{v}_i(\mathbf{v}_i \in M \;\&\; \phi^M),\ (\forall \mathbf{v}_i \phi)^M :\equiv \forall \mathbf{v}_i(\mathbf{v}_i \in M \rightarrow \phi^M).$$

If $\phi(\mathbf{x}_1, \dots , \mathbf{x}_n)$ is a full extended formula, we also set

$$M \models \phi[x_1, \dots , x_n] :\equiv x_1, \dots , x_n \in M \;\&\; (\phi(x_1, \dots , x_n))^M.$$

This definition and the accompanying notational convention extend easily to classes definable with parameters (cf. Problem x7.52) and they allow us to interpret $\mathbb{FOL}(\in)$ in any "class structure" $(M, \in \restriction M)$. Notice that $M \models \phi[x_1, \dots , x_n]$ is a formula which expresses the truth of $\phi(\mathbf{x}_1, \dots , \mathbf{x}_n)$ when we interpret each variable $\mathbf{x}_i$ by x_i, assume that each $x_i \in M$ and restrict all the quantifiers in the formula to M; and that the relativization ϕ^M depends on the formula which defines the class M.

We will prove the next, basic result in a general context because it has many applications, but in a first reading one may as well take $C_\xi = V_\xi$.

Theorem 7D.7 (The Reflection Theorem)**.** *Let $\xi \mapsto C_\xi$ be an operation on ordinals to sets which is definable in $\mathbb{FOL}(\in)$ and satisfies the following two conditions:*

(i) $\zeta \leq \xi \Longrightarrow C_\zeta \subseteq C_\xi$.

(ii) *If λ is a limit ordinal, then $C_\lambda = \bigcup_{\xi<\lambda} C_\xi$.*

Let $C = \bigcup_\xi C_\xi$.

It follows that for any full extended formula $\varphi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ of $\mathbb{FOL}(\in)$, there is closed, unbounded class of ordinals K such that for $\xi \in K$ and $x_1, \dots, x_n \in C_\xi$,

$$C \models \varphi[x_1, \dots, x_n] \iff C_\xi \models \varphi[x_1, \dots, x_n].$$

In particular, if φ is any sentence of $\mathbb{FOL}(\in)$, then

$$C \models \varphi \Longrightarrow \text{for some } \xi,\ C_\xi \models \varphi.$$

Proof. We use induction on $\varphi(\mathbf{x}_1, \dots, \mathbf{x}_n)$, the result being trivial for prime formulas and following easily from the induction hypothesis for negations and conjunctions.

Suppose $(\exists \mathbf{y})\varphi(\mathbf{y}, \mathbf{x}_1, \dots, \mathbf{x}_n)$ is given and assume that K satisfies the result for $\varphi(\mathbf{y}, \mathbf{x}_1, \dots, \mathbf{x}_n)$. Let

$$G(x_1, \dots, x_n) = \begin{cases} \text{least } \xi \text{ such that } (\exists y \in C_\xi)[C \models \varphi[y, x_1, \dots, x_n]] \\ \quad \text{if one such } \xi \text{ exists,} \\ 0 \quad \text{otherwise} \end{cases}$$

and take

$$F(\xi) = \text{supremum}\{G(x_1, \dots, x_n) : x_1, \dots, x_n \in C_\xi\}$$

by replacement. By Proposition 7C.19, the class of ordinals

$$K \cap \{\xi : (\forall \eta < \xi)[F(\eta) < \xi]\} \cap \{\xi : \xi \text{ is limit}\}$$

is closed and unbounded and it is easy to verify that it satisfies the theorem for the formula $(\exists \mathbf{y})\varphi(\mathbf{y}, \mathbf{x}_1, \dots, \mathbf{x}_n)$. ⊣

Corollary 7D.8 (ZF). *$V \models \mathsf{ZF}_g$ and if* **AC** *holds, then $V \models \mathsf{ZFC}$.*

It follows that if ZF *is consistent, then it remains consistent when we add the Axiom of Foundation; and if* ZF + **AC** *is consistent, then so is* ZFC.

PROOF is left for Problem x7.53. ⊣

Gödel's Theorem 8C.9 in the next Chapter is a much stronger relative consistency result, and it is proved by appealing to Theorem 8A.7, which in its turn is a much stronger version of the first claim here. This theorem, however, was proved by von Neumann considerably before Gödel's work, and it was the first non-trivial relative consistency proof in set theory. It provided the general plan for Gödel's work.

Finally, we include in this section the basic list of equivalents of the Axiom of Choice which can be formulated and proved in ZF.

Theorem 7D.9 (ZF). *The following statements are equivalent:*

(1) *The Axiom of Choice,* **AC**.

(2) (The logical form of **AC**). *For every binary condition $R(u,v)$ and any two sets a, b,*

$$(\forall u \in a)(\exists v \in b)R(u,v) \Longrightarrow (\exists f : a \to b)(\forall u \in a)R(u, f(u)).$$

(3) *For every set x, there is a function $\varepsilon : \mathcal{P}(x) \setminus \{\emptyset\} \to x$ such that*

$$(\forall y \subseteq x)[y \neq \emptyset \Longrightarrow \varepsilon(y) \in y]. \tag{181}$$

We call any such ε a choice function for a.

(4) (Maximal Chain Principle). *In every very partial ordering $\leq$ there is a maximal chain.*

(5) (Zorn's Lemma). *If $\leq$ is a partial ordering on $x = \mathrm{Field}(\leq)$ in which every chain has an upper bound, then $\leq$ has a maximal element, some $a \in x$ such that $(\forall t \in x)(a \not< t)$.*

(6) (Cardinal Comparability Principle). *For any two sets $x, y,$, either $x \leq_c y$ or $y \leq_c x$.*

(7) (Zermelo's Wellordering Theorem). *Every set is equinumerous with an ordinal number.*

We have established all the ingredients needed for a simple round-robin proof $(1) \Longrightarrow (2) \Longrightarrow \cdots \Longrightarrow (7) \Longrightarrow (1)$, cf. Problem x7.41.

From the foundational point of view, the most interesting part of this theorem is the triple equivalence in ZF of the logical form of **AC** (2), which had been viewed as an obvious principle of logic, with the cardinal comparability principle (6), which looks like a technical result and with the wellordering principle (7), which had been considered false before Zermelo's proof—by many mathematicians, though not Cantor. From the point of view of its applications, all these "versions" of **AC** are useful in various parts of mathematics, but perhaps the most natural one is the existence of a choice functions (3): it makes it possible to say "choose a $y \in a$ such that ... " after showing that "there exists a $y \in a$ such that ... " in the course of a proof, with **AC** justifying in the end the validity of the argument.

7E. Cardinal arithmetic and ultraproducts, ZFC

We include in this Section a (very) few results about cardinal arithmetic and the ultraproduct construction, which need **AC**.

The most immediate effect of the Axiom of Choice is that it makes it possible to define *cardinal exponentiation*, which requires that the function space $(\lambda \to \kappa)$ is wellorderable,

$$\kappa^\lambda = |(\lambda \to \kappa)| \quad (\kappa, \lambda \in \text{Card}).$$

The definition gives (easily) "the laws of exponents":

Theorem 7E.1 (ZFC). (1) *For every* $\kappa \in \text{Card}$, $2^\kappa = |\mathcal{P}(\kappa)|$.

(2) *For all cardinal numbers* κ, λ, μ,

$$\kappa^0 = 1, \kappa^1 = \kappa, \ \kappa^n = \underbrace{\kappa \cdots \kappa}_{n \text{ times}} \ (n \in \omega)$$

$$(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu, \ \kappa^{(\lambda+\mu)} = \kappa^\lambda \cdot \kappa^\mu, \ \left(\kappa^\lambda\right)^\mu = \kappa^{\lambda \cdot \mu}.$$

(3) *For all cardinal numbers* κ, λ, μ,

$$\begin{aligned} &\kappa \le \mu \implies \kappa + \lambda \le \mu + \lambda, \ \kappa \cdot \lambda \le \mu \cdot \lambda, \\ &\lambda \le \mu \implies \kappa^\lambda \le \kappa^\mu \qquad (\kappa \neq 0), \\ &\kappa \le \lambda \implies \kappa^\mu \le \lambda^\mu. \end{aligned}$$

These are proved by constructing the required bijections and injections, without, in fact, using **AC**. For example, (1) and (2) follow from the following theorems of ZF:

$$\begin{aligned} \mathcal{P}(x) =_c (x \to \{0,1\}) \quad &(y \mapsto \chi_y : x \to \{0,1\}, \\ &(\chi_y = \text{ the characteristic function of } y \subseteq x), \end{aligned}$$

$$\begin{aligned} &(z \to (x \times y)) =_c (z \to x) \times (z \to y), \\ &((x \uplus y) \to z) =_c (x \to z) \times (y \to z), \\ &((x \times y) \to z) =_c (x \to (y \to z)). \end{aligned}$$

On the other hand, we must be careful with strict inequalities between infinite cardinal numbers because they are not always respected by the algebraic operations. For example,

$$\aleph_0 < \aleph_1 \text{ but } \aleph_0 + \aleph_1 = \aleph_1 + \aleph_1 \ (= \aleph_1).$$

A simple but basic consequence of **AC** to which we will appeal constantly (and silently) is

$$(\exists f)[f : a \twoheadrightarrow b] \Longrightarrow b \leq_c a, \tag{182}$$

which is proved by fixing a choice function $\varepsilon_a : \mathcal{P}(a) \setminus \{\emptyset\} \to a$ and defining the required injection $g : b \rightarrowtail a$ by

$$g(t) = \varepsilon_a(\{s \in a : f(s) = t\}).$$

It is known that (182) cannot be proved in ZF, but its exact axiomatic strength is not clear—for all I know, it may imply **AC**.

One of the basic problems in set theory—perhaps its most basic problem—is the size of the powerset $\mathcal{P}(\omega)$ or, equivalently, the size of *Baire space* or the real numbers, since we can show in ZF that

$$\mathcal{P}(\omega) =_c \mathcal{N} =_c \mathbb{R},$$

cf. Problems x7.33, x7.34. Cantor's famous *Continuum Hypothesis* expresses the natural conjecture about this, that there are no sets intermediate in size between ω and its powerset:

$$(\forall x \subseteq \mathcal{P}(\omega))[x \leq_c \omega \vee x =_c \mathcal{P}(\omega)]. \tag{\textbf{CH}}$$

The corresponding hypothesis for arbitrary sets is the *Generalized Continuum Hypothesis*,

$$(\forall y)(\forall x \subseteq \mathcal{P}(y))[x \leq_c y \vee x =_c \mathcal{P}(y)]. \tag{\textbf{GCH}}$$

The Continuum Hypothesis is intimately related to the Cardinal Comparability Principle, because it could fail for some $x \subset \mathcal{P}(\omega)$ such that $x <_c \mathcal{P}(\omega)$ simply because x is not $\leq_c$-comparable to ω—i.e., x is uncountable, smaller than $2^{\aleph_0}$, but has no infinite, countable subsets. In ZFC, these two hypotheses take the simple "cardinal arithmetic" forms

$$2^{\aleph_0} = \aleph_1, \quad 2^{\aleph_\xi} = \aleph_{\xi+1}.$$

This does not help determine their truth value.

Many of the consequences of the Axiom of Choice can be formulated as theorems of ZF about wellorderable sets. We state here a few, very basic facts whose proofs use **AC** in such a fundamental way (often within an argument by contradiction), that there is no useful way to view them as theorems of ZF.

An *indexed set* (or *family*) *of sets* is a function $a : I \to \mathcal{V}$. We often write $a_i = a(i)$ for these indexed sets, and we use them to define indexed unions and products,

$$\bigcup_{i\in I} a_i = \bigcup\{a_i : i \in I\},$$
$$\prod_{i\in I} a_i = \{f : I \to \bigcup_{i\in I} a_i : (\forall i \in I)[f(i) \in a_i]\}.$$

The infinite product comprises all choice functions which pick just one member from each a_i, and the equivalence

$$(\forall(i \mapsto a_i))[(\forall i \in I)[a_i \neq \emptyset] \iff \prod_{i\in I} a_i \neq \emptyset]. \tag{183}$$

is (easily) equivalent to **AC**, cf. Problem x7.44.

For indexed families of cardinal numbers, we also set

$$\sum_{i\in I} \kappa_i = |\{\langle i, t\rangle : i \in I \;\&\; t \in \kappa_i\}|,$$
$$\prod_{i\in I} \kappa_i = |\{f : I \to \bigcup_{i\in I} \kappa_i : (\forall i \in I)[f(i) \in \kappa_i]\}|,$$

so that $\prod_{\xi\in\lambda} \kappa = \kappa^\lambda$. (Use of the same notation for products and cardinal numbers of products is traditional and should not cause confusion.)

Theorem 7E.2 (ZFC, König's Theorem). *For any two families of sets $(i \mapsto a_i)$ and $(i \mapsto b_i)$ on the same index set $I \neq \emptyset$,*

$$\text{if } (\forall i \in I)[a_i <_c b_i], \text{then } \bigcup_{i\in I} a_i <_c \prod_{i\in I} b_i. \tag{184}$$

In particular, for families of cardinals, $(i \mapsto \kappa_i)$ and $(i \mapsto \lambda_i)$,

$$\text{if } (\forall i \in I)[\kappa_i <_c \lambda_i], \text{then } \sum_{i\in I} \kappa_i <_c \prod_{i\in I} \lambda_i. \tag{185}$$

Proof. The hypothesis and **AC** yield for each i an injection $\pi_i : a_i \rightarrowtail b_i$; and since π_i cannot be a surjection, there is also a function $c : I \to \bigcup_{i\in I} b_i$ such that for each i, $c(i) \in b_i \setminus \pi_i[a_i]$. For any $x \in \bigcup_{i\in I} a_i$, we set

$$f(x,i) = \begin{cases} \pi_i(x), & \text{if } x \in a_i, \\ c(i), & \text{if } x \notin a_i, \end{cases}$$
$$g(x) = (i \mapsto f(x,i)) \in \prod_{i\in I} b_i.$$

If $x \neq y$ and x, y belong to the same a_i for some i, then

$$g(x)(i) = \pi_i(x) \neq \pi_i(y) = g(y)(i),$$

because π_i is an injection, and hence $g(x) \neq g(y)$. If no a_i contains both x and y, suppose $x \in a_i$, $y \notin a_i$; it follows that $g(x)(i) = \pi_i(x) \in \pi_i[a_i]$ and $g(y)(i) = c(i) \in b_i \setminus \pi_i[a_i]$ so that again $g(x) \neq g(y)$. We conclude that the mapping $g : \bigcup_{i\in I} a_i \rightarrowtail \prod_{i\in I} b_i$ is an injection, and hence

$$\bigcup_{i\in I} a_i \leq_c \prod_{i\in I} b_i.$$

Suppose, towards a contradiction that there existed a bijection

$$h : \bigcup_{i\in I} a_i \rightarrowtail\!\!\!\!\!\twoheadrightarrow \prod_{i\in I} b_i,$$

so that these two sets are equinumerous. For every i, the function

$$h_i(x) =_{\mathrm{df}} h(x)(i) \quad (x \in a_i)$$

is (easily) a function of a_i into b_i and by the hypothesis it cannot be a surjection; hence by **AC** there exists a function ε which selects in each b_i some element not in its image, i.e.,

$$\varepsilon(i) \in b_i \setminus h_i[a_i], \quad (i \in I).$$

By its definition, $\varepsilon \in \prod_{i \in I} b_i$, so there must exist some $x \in A_j$, for some j, such that $h(x) = \varepsilon$; this yields

$$\varepsilon(j) = h(x)(j) = h_j(x) \in h_j[A_j],$$

contrary to the characteristic property of ε.

The cardinal version (185) follows by applying (184) to $a_i = \{i\} \times \kappa_i$ and $b_i = \lambda_i$. ⊣

Definition 7E.3 (Cofinality, regularity)**.** A limit ordinal ξ is *cofinal* with a limit ordinal $\zeta \le \xi$ if there exists a function $f : \zeta \to \xi$ which is unbounded, i.e., $\sup\{f(\eta) : \eta < \zeta\} = \xi$. (So each limit ξ is cofinal with itself.)

The *cofinality* of ξ is the least limit ordinal $\zeta \le \xi$ which is cofinal with ξ,

$$\mathrm{cf}(\xi) = \min\{\zeta \le \xi : (\exists f : \zeta \to \xi)[\sup\{f(\eta) \mid \eta < \zeta\} = \xi]\}.$$

A limit ordinal ξ is *regular* if $\mathrm{cf}(\xi) = \xi$, otherwise it is *singular*.

For example, ω is regular, since there is no limit ordinal less than it with which it could be cofinal, and $\aleph_\omega$ is singular, since (easily) $\mathrm{cf}(\aleph_\omega) = \omega$.

Proposition 7E.4. (1) *If ξ is cofinal with $\zeta \le \xi$ and ζ is cofinal with $\mu \le \zeta$, then ξ is cofinal with μ.*

(2) *For every limit ordinal ξ, $\mathrm{cf}(\xi)$ is a cardinal.*

(3) (ZF). *For every limit ordinal λ, $\mathrm{cf}(\aleph_\lambda) = \mathrm{cf}(\lambda)$.*

(4) *If $\lambda = \mathrm{cf}(\xi)$, then there is an injection $f : \lambda \rightarrowtail \xi$ which is cofinal and order preserving, i.e.,*

$$\eta_1 < \eta_2 < \lambda \Longrightarrow f(\eta_1) < f(\eta_2) < \xi, \qquad \sup\{f(\eta) : \eta < \lambda\} = \xi.$$

Proof is easy and left for Problem x7.46. ⊣

Theorem 7E.5 (ZFC)**.** *Every infinite, successor cardinal κ^+ is regular.*

Proof. Suppose towards a contradiction that some $f : \kappa \to \kappa^+$ is unbounded, so that

$$\kappa^+ = \sup\{f(\xi) : \xi < \kappa\}.$$

Now each $f(\xi) \le_c \kappa$, since κ^+ is an initial ordinal; so choose surjections

$$\pi_\xi : \kappa \twoheadrightarrow \max(1, f(\xi)) \quad \text{(just in case } f(\xi) = 0),$$

and define $\pi : \kappa \times \kappa \to \kappa^+$ by

$$\pi(\xi, \eta) = \pi_\xi(\eta).$$

The assumptions imply that π is a surjection, because if $\zeta \in \kappa^+$, then $\zeta \in f(\xi)$ for some $\xi \in \kappa$, and so $\zeta = \pi_\xi(\eta) = \pi(\xi, \eta)$ for some $\eta \in \kappa$; but this is a contradiction, because $|\kappa \times \kappa| = \kappa < \kappa^+$, and so there cannot be a surjection of $\kappa \times \kappa$ onto κ^+. $\dashv$

So $\aleph_0, \aleph_1, \dots \aleph_n, \dots$, are all regular, $\aleph_\omega$ is singular, $\aleph_{\omega+1}, \aleph_{\omega+2}, \dots$ are regular, etc.

Theorem 7E.6 (ZFC, König's inequality)**.** *For every infinite cardinal κ,*

$$\kappa < \kappa^{\mathrm{cf}(\kappa)}. \tag{186}$$

PROOF. Let $\lambda = \mathrm{cf}(\kappa) \leq \kappa$ and fix an unbounded function $f : \lambda \to \kappa$, so that

$$f(\xi) <_c \kappa \quad (\xi < \lambda)$$

since $f(\xi) \in \kappa$ and κ is a cardinal. By König's Theorem 7E.2,

$$\kappa = \bigcup\nolimits_{\xi\in\lambda} f(\xi) <_c \prod\nolimits_{\xi\in\lambda} \kappa = \kappa^\lambda, \qquad \dashv$$

König's inequality was the strongest, known result about cardinal exponentiation in ZFC until the 1970s, when Silver proved that that if the **GCH** holds up to $\kappa = \aleph_{\aleph_1}$, then it holds at κ,

$$(\forall \xi < \aleph_1)[2^{\aleph_\xi} = \aleph_{\xi+1}] \Longrightarrow 2^{\aleph_{\aleph_1}} = \aleph_{\aleph_1+1}.$$

In fact Silver proved much stronger results in ZFC and others, after him extended them substantially, but none of these results affects the Continuum Hypothesis; and it can not, because it was already known from the work of Paul Cohen in 1963 that for any $n \geq 1$, the statement $2^{\aleph_0} = \aleph_n$ is consistent with ZFC.

Definition 7E.7 (ZF, Inaccessible cardinals)**.** A limit cardinal κ is *weakly inaccessible* if it is regular and closed under the cardinal succession operation,

$$\lambda < \kappa \Longrightarrow \lambda^+ < \kappa; \tag{187}$$

it is (strongly) *inaccessible* if it is regular and closed under exponentiation,

$$\lambda < \kappa \Longrightarrow 2^\lambda < \kappa. \tag{188}$$

Notice that weakly inaccessible cardinals can be defined in ZF. We can also define strongly inaccessibles without **AC**, if we understand the definition to require that $\mathcal{P}(\lambda)$ is wellorderable for $\lambda < \kappa$, but nothing interesting about them can be proved without assuming **AC**. With **AC**, strongly inaccessible cardinals are weakly inaccessible, since

$$\lambda^+ \leq 2^\lambda.$$

We cannot prove in ZFC the existence of strongly inaccessible cardinals, cf. Problems x7.49*, x7.51*. In fact, ZFC does not prove the existence of weakly inaccessible cardinals either, as we will show in the next Chapter.

Finally, we include here the bare, minimum facts about ultrafilters and ultraproducts which have numerous applications in model theory.

Definition 7E.8. A (proper) *filter* on an infinite set I is a collection $F \subset \mathcal{P}(I)$ which satisfies the following conditions:

(1) If $X \in F$ and $X \subseteq Y$, then $Y \in F$.
(2) If $X_1, X_2 \in F$, then $X_1 \cap X_2 \in F$.
(3) F is neither empty nor the whole of $\mathcal{P}(I)$: i.e., $\emptyset \notin F$ and $I \in F$.

A filter on I is *maximal* or an *ultrafilter* if

$$X \in F \text{ or } X^c = (I \setminus X) \in F \qquad (X \subseteq I),$$

or F *decides* every $X \subseteq I$, as we will say.

For example, if $\emptyset \neq A \subseteq I$, then the set

$$F_A = \{X \subseteq I : A \subseteq X\}$$

of all supersets of A is a filter; and if $A = \{a\}$ is a singleton, then

$$F_{\{a\}} = U_a = \{X \subseteq I : a \in X\}$$

is an ultrafilter, the *principal ultrafilter* determined by a.

A more interesting example is the collection of *cofinite subsets* of I,

$$F_0(I) = \{X \subseteq I : X^c \text{ is finite}\}.$$

This is clearly not F_A for any $A \subseteq I$, and it is not an ultrafilter.

Intuitively, a filter F determines a notion of "largeness" for subsets of I, and its classical examples arise in this way: for example F might be the collection of sets of real numbers whose complement has (Lebesgue) measure 0 or whose complement is meager.

Theorem 7E.9 (ZFC). *Every filter F on an infinite set I can be extended to an ultrafilter $U \supseteq F$.*

Proof. Consider the set of all filters which extend F,

$$\mathcal{F} = \{F' \subset \mathcal{P}(I) : F \subseteq F' \ \&\ F' \text{ is a filter}\},$$

and view it as a poset $(\mathcal{F}, \subseteq)$. Every chain $\mathcal{C} \subset \mathcal{F}$ (easily) has an upper bound, namely its union $\bigcup \mathcal{C}$; and so by Zorn's Lemma, $\mathcal{F}$ has a maximal member U. It suffices to prove that U decides every $X \subseteq I$, so suppose that for some X_0

$$X_0 \notin U \text{ and } X_0^c \notin U.$$

Let $G = \{Y : (\exists X \in U)[Y \supseteq (X \cap X_0)]\}$. Clearly $U \subsetneq G$, since G contains $X_0 = I \cap X_0$, and G is trivially closed under supersets. It is also closed under intersections, since if for some $X_1, X_2 \in U$,

$$Y_1 \supseteq (X_1 \cap X_0),\ Y_2 \supseteq (X_2 \cap X_0),$$

then $Y_1 \cap Y_2 \supseteq (X_1 \cap X_2 \cap X_0)$, and $X_1 \cap X_2 \in U$. Since G cannot be a (proper) filter because U is maximal, it must be that $\emptyset \supseteq (X \cap X_0)$ for some $X \in U$; which implies that $X \subseteq X_0^c$, and so $X_0^c \in U$, contrary to our assumption. ⊣

The most interesting immediate corollary is the existence of non-principal ultrafilters on every infinite set I: because if $U \supset F_0(I)$ extends the filter of cofinite subsets of I, then U is not principal. As far as the strength of these claims goes, it is known that the existence of non-principal ultrafilters cannot be proved in ZF_g, but even the stronger claim in the theorem does not imply **AC**.

Suppose U is an ultrafilter on I and $\{A_i\}_{i\in I}$ is a family of sets indexed by I, and let

$$f \sim_U g \iff \{i \in I : f(i) = g(i)\} \in U \quad (f, g \in \textstyle\prod_{i\in I} A_i).$$

It is easy to check that $\sim_U$ is an equivalence relation on $\prod_{i\in I} A_i$. We let

$$\overline{f} = \{g \in \textstyle\prod_{i\in I} A_i : f \sim_U g\} \qquad (f \in \textstyle\prod_{i\in I} A_i)$$

be the equivalence class of f modulo $\sim_U$, so that

(189) $$\overline{f} = \overline{g} \iff \{i \in I : f(i) = g(i)\} \in I.$$

We will also let

(190) $$\overline{A} = \Big(\textstyle\prod_{i\in I} A_i\Big)/U = \{\overline{f} : f \in \textstyle\prod_{i\in I} A_i\}$$

for the corresponding set of equivalence classes. The notation is compact (and in particular does not show explicitly the dependence on U) but it is useful.

Definition 7E.10 (ZFC, ultraproducts)**.** Suppose $\{\mathbf{A}_i\}_{i\in I}$ a family of τ-structures indexed by an infinite set I and U is an ultrafilter on I. The *ultraproduct*

(191) $$\overline{\mathbf{A}} = \Big(\textstyle\prod_{i\in I} \mathbf{A}_i\Big)/U$$

of the family $\{\mathbf{A}_I\}_{i\in I}$ modulo U is the τ-structure defined as follows:

(1) The universe $\overline{A}$ is the set of equivalence classes as in (190).

(2) For each constant c in τ,

$$c^{\overline{\mathbf{A}}} = \overline{g},\ \text{where } g(i) = c^{\mathbf{A}_i}.$$

(3) For each relation symbol R in τ,

$$R^{\overline{\mathbf{A}}}(\overline{f}_1, \dots, \overline{f}_k) \iff \{i \in I : R^{\mathbf{A}_i}(f_1(i), \dots, f_k(i))\} \in I.$$

(4) For each function symbol f in τ,

$$f^{\overline{\mathbf{A}}}(\overline{f}_1, \dots, \overline{f}_k) = \overline{g} \text{ where } g(i) = f^{\mathbf{A}_i}(f_1(i), \dots, f_k(i)).$$

If $\mathbf{A}_i = \mathbf{A}$ for all $i \in I$, then $\overline{\mathbf{A}} = \Big(\prod_{i \in I} \mathbf{A}\Big)/I$ is the *ultrapower* of $\mathbf{A}$ module U.

To make sense of the last two clauses in this definition we need to check that if $f_1 \sim_U f_1', \dots f_k \sim_U f_k'$, then

$$\{i \in I : R^{\mathbf{A}_i}(f_1(i), \dots, f_k(i)) \iff R^{\mathbf{A}_i}(f_1'(i), \dots, f_k'(i))\} \in U,$$
$$\{i \in I : f^{\mathbf{A}_i}(f_1(i), \dots, f_k(i)) = f^{\mathbf{A}_i}(f_1'(i), \dots, f_k'(i))\} \in U.$$

These are true because the claimed equivalence and identity hold on

$$X = \bigcap\nolimits_{j=1,\dots,k} \{i \in I : f_j(\vec{x}) = f_j'(\vec{x})\}$$

and $X \in U$ by the hypothesis.

Theorem 7E.11 (ZFC, Łós' Theorem). *Let $\{\mathbf{A}_i\}_{i \in I}$ be family of τ-structures indexed by an infinite set I and let $\overline{\mathbf{A}}$ be their ultraproduct modulo a ultrafilter U as in* (191)*. Then for each full extended formula $\phi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ and all $\overline{f}_1, \dots, \overline{f}_n \in \overline{A}$,*

(192) $$\overline{\mathbf{A}} \models \phi[\overline{f}_1, \dots, \overline{f}_n] \iff \{i \in I : \mathbf{A}_i \models \phi[f_1(i), \dots, f_n(i)]\} \in I.$$

In particular, for every sentence θ,

$$\overline{\mathbf{A}} \models \theta \iff \{i \in I : \mathbf{A}_i \models \theta\} \in I.$$

PROOF. We first check by induction that for each term $t(\mathbf{x}_1, \dots, \mathbf{x}_n)$,

$$t^{\overline{\mathbf{A}}}[\overline{f}_1, \dots, \overline{f}_n] = \overline{g} \text{ where } g(i) = t^{\mathbf{A}_i}[f_i(i), \dots, f_n(i)],$$

and then we check (192) by another, simple induction on ϕ. The only case where some thought is required is when

$$\phi(\vec{\mathbf{x}}) \equiv (\exists \mathbf{y})\psi(\vec{\mathbf{x}}, \mathbf{y}),$$

and this is where **AC** comes in. We leave the detail for Problem x7.56. ⊣

We have put in the problems a few additional facts about ultrapowers, including a classical, purely semantic proof of the Compactness Theorem for arbitrary signatures. But it should be emphasized that the subject is large—especially rich in its applications to non-standard models—and we will not cover it here.

7F. Problems for Chapter 7

For each vocabulary τ, let

$$\tau' = \tau \cup \{\mathsf{P}_i^n : n, i \in \mathbb{N}\}$$

be the expansion of τ by infinitely many n-ary relation symbols

$$\mathsf{P}_0^n, \mathsf{P}_1^n, \mathsf{P}_1^n, \ldots$$

for each n and no new function symbols or constants. A τ-*axiom scheme* is any τ'-sentence θ; and a τ-*instance* of θ is the τ-sentence constructed by associating with each P_i^n which occurs in θ a full, extended τ-formula $\phi_i^n(v_1, \ldots, v_n)$ and replacing each prime formula $\mathsf{P}_i^n(t_1, \ldots, t_n)$ in θ with the τ-formula $\phi_i^n(t_1, \ldots, t_n)$, where the substitution $\{v_1 :\equiv t_1, \ldots, v_n :\equiv t_n\}$ is assumed free.

For example, the sentence

$$\theta \equiv (\forall x)(\exists w)(\forall u)[u \in w \leftrightarrow [u \in x \;\&\; P(u)]]$$

is an $\in$-scheme, and the instances of it are all $\in$-sentences of the form

$$\theta\{P(v) :\equiv \phi(v)\} \equiv (\forall x)(\exists w)(\forall u)[u \in w \leftrightarrow [u \in x \;\&\; \phi(u)]],$$

where $\phi(u)$ is an arbitrary, full extended $\in$-formula.

A τ-theory T is *axiomatized by schemes* if its axioms (i.e., the members of T) comprise a set of τ-sentences and all τ-instances of a set of axiom schemes.

Problem x7.1. Prove that Peano arithmetic PA and ZF^- are axiomatized by schemes.

Problem x7.2* (Eliminability of descriptions, 7B.1)**.** Fix a signature τ, and suppose $\phi(\vec{v}, w) \equiv \phi(v_1, \ldots, v_n, w)$ is a full extended τ-formula and F is an n-ary function symbol not in τ.

(1) With each full, extended (τ, F)-formula $\theta'(\vec{u})$ we can associate a full, extended τ-formula $\theta(\vec{u})$ such that

$$(\forall \vec{v})(\exists! w)\phi(\vec{v}, w) \;\&\; (\forall \vec{v})\phi(\vec{v}, F(\vec{v})) \vdash \theta'(\vec{u}) \leftrightarrow \theta(\vec{u}).$$

(2) Suppose T is a τ-theory axiomatized by schemes such that

$$T \vdash (\forall \vec{v})(\exists! w)\phi(\vec{v}, w),$$

and let T' be the (τ, F)-theory whose axioms are those of T, the sentence $(\forall \vec{v})\phi(\vec{v}, F(\vec{v}))$, and all instances with (τ, F) formulas of the axiom schemes of T. Then T' is a conservative extension of T, i.e., for all τ-sentences θ,

$$T' \vdash \theta \iff T \vdash \theta.$$

Problem x7.3. Prove that a set x is definable if and only if its singleton $\{x\}$ is a definable class.

Problem x7.4 (Lemma 7C.1)**.** Prove that if $H, G_1, \dots, G_m$ are definable class operations, then their (generalized) composition

$$F(\vec{x}) = H(G_1(\vec{x}), \dots, G_m(\vec{x}))$$

is also definable.

Problem x7.5. Prove that for every set x,

$$\text{Russel}(x) = \{t \in x : t \notin t\} \notin x.$$

Infer that the class $\mathcal{V}$ of all sets is not a set.

Problem x7.6. Determine which of the claims in Theorem 7C.2 is a formal *theorem scheme* (rather than a theorem) of ZF^- and write out these schemes.

Problem x7.7. Prove that if every member of x is transitive, then $\bigcup x$ is transitive.

Problem x7.8. Prove that if x is transitive, then $\mathrm{TC}(x) = x \cup \{x\}$.

Problem x7.9. Prove that the restriction $S = \{\langle n, n' \rangle : n \in \omega\}$ of the operation $x' = x \cup \{x\}$ to ω is a bijection of ω with $\omega \setminus \{0\}$. (This and the Induction Principle 7C.3 together comprise the *Peano axioms* for the structure $(\omega, 0, S)$.)

Problem x7.10* (Zermelo's Axiom of Infinity)**.** Prove that

$$(\mathsf{Z}\text{-infty}) \qquad (\exists z)[\emptyset \in z) \ \&\ (\forall t \in z)[\{t\} \in z]].$$

Outline a proof of the Axiom of Infinity in

$$\mathsf{ZF} - \text{Infinity} + (\mathsf{Z}\text{-infty}).$$

Problem x7.11. Prove that the following are equivalent for every x:

(1) x is finite, i.e., $x =_c n$ for some $n \in \omega$.
(2) There is exactly one $n \in \omega$ such that $x =_c n$.
(3) $x <_c \omega$.

Problem x7.12. Prove that a set x is countable exactly when $x \leq_c \omega$.

Problem x7.13. Prove that for each relation r, if $r' = <_r$, then $<_{r'} = <_r$.

Problem x7.14 ((2) and (3) of Theorem 7C.9)**.** Prove that for each ordinal ξ, $\xi' = \xi \cup \{\xi\}$ is the successor of ξ in $\leq_{\mathrm{ON}}$, i.e.,

$$\xi <_{\mathrm{ON}} \xi' \ \&\ (\forall \eta)[\xi <_{\mathrm{ON}} \eta \Longrightarrow \xi \leq_{\mathrm{ON}} \eta].$$

Infer that every ordinal is a grounded set.

Problem x7.15 ((4) of Theorem 7C.9)**.** Prove that for every $x \subseteq \mathrm{ON}$,

$$\bigcup x = \sup\{\xi : \xi \in x\} = \text{the least ordinal } \eta \text{ such that } (\forall \xi \in x)[\xi \leq_{\mathrm{ON}} \eta].$$

Problem x7.16. Prove that a set $x \subseteq \mathrm{ON}$ of ordinals is an ordinal if and only if x is transitive.

Problem x7.17 ((5) of Theorem 7C.9)**.** Prove that every ordinal number is (uniquely) 0, a successor or a limit, and also that ON is a proper class.

Problem x7.18* (Mostowski collapsing for classes)**.** Suppose $E(u,v)$ is a binary condition such that:

(1) For each v, $\{u : E(u,v)\}$ is a set.
(2) $(\forall x \neq \emptyset)(\exists t \in x)(\forall u \in x)\neg E(u,t)$, i.e., $E(x,y)$ is (strict and) grounded.

Prove that there is exactly one operation $D : \mathrm{Field}(E) \to \mathcal{V}$ such that

$$D(v) = \{D(u) : E(u,v)\} \qquad (v \in \mathrm{Field}(E)). \tag{193}$$

Verify that the hypotheses of the problem are satisfied if the Axiom of Foundation holds and for some class M,

$$E_M(u,v) \iff u, v \in M \ \&\ u \in v.$$

The operation D is the *decoration* or *Mostowski surjection* of the condition $E(u,v)$.

Problem x7.19*. Suppose $E(u,v)$ satisfies (1) and (2) of Problem x7.18* and it is also *extensional*, i.e.,

$$(\forall t)[E(t,u) \leftrightarrow E(t,v)] \to u = v \qquad (u, v \in \mathrm{Field}(E)). \tag{194}$$

Let $D : \mathrm{Field}(E) \to \mathcal{V}$ be the Mostowski surjection of $E(u,v)$.

Prove that the image $\overline{\mathrm{Field}(E)} = \{D(v) : v \in \mathrm{Field}(E)\}$ is a transitive, grounded class and D is an injection which carries E to the membership relation, i.e., for $u, v \in \mathrm{Field}(E)$,

$$u = v \iff D(u) = D(v), \quad D(u) \in D(v) \iff E(u,v). \tag{195}$$

Problem x7.20 (Ordinal addition)**.** Define a binary operation $\alpha + \beta$ on ordinals such that

$$\begin{aligned} \alpha + 0 &= \alpha, \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1, \\ \alpha + \lambda &= \sup\{\alpha + \beta : \beta \in \lambda\} \quad (\lambda \text{ limit}). \end{aligned}$$

Show that $\alpha + \beta = \mathrm{ot}(\leq_{\alpha \uplus \beta})$ where $\leq_{\alpha\uplus\beta}$ is the wellordering defined by adding $\leq_\beta$ at the end of $\leq_\alpha$:

$$\mathrm{Field}(\leq_{\alpha\uplus\beta}) = \alpha \uplus \beta,$$
$$\langle i, \xi \rangle <_{\alpha\uplus\beta} \langle j, \eta \rangle \iff i < j \vee [i = j \ \&\ [\xi \in \eta] \qquad (i = 0, 1).$$

Problem x7.21 (Ordinal addition inequalities)**.** Show that for all ordinals $\alpha, \beta, \gamma, \delta$:

$$
\begin{gathered}
0+\alpha=\alpha, \text{ and } n \in \omega \leq \alpha \Longrightarrow n+\alpha=\alpha, \\
0<\beta \Longrightarrow \alpha<\alpha+\beta, \\
\alpha \leq \beta \,\&\, \gamma \leq \delta \Longrightarrow \alpha+\gamma \leq \beta+\delta, \\
\alpha \leq \beta \,\&\, \gamma<\delta \Longrightarrow \alpha+\gamma<\beta+\delta .
\end{gathered}
$$

Show also that, in general,

$$
\alpha<\beta \text{ does not imply } \alpha+\gamma<\beta+\gamma .
$$

Problem x7.22. Give examples of strictly increasing sequences of ordinals such that

$$
\begin{aligned}
\lim_n(\alpha_n+\beta) &\neq \lim_n \alpha_n+\beta, \\
\lim_n(\alpha_n+\beta_n) &\neq \lim_n \alpha_n+\lim_n \beta_n .
\end{aligned}
$$

Problem x7.23 (Ordinal multiplication)**.** Define a binary operation $\alpha \cdot \beta$ on ordinals such that

$$
\begin{aligned}
\alpha \cdot 0 &= 0, \\
\alpha \cdot(\beta+1) &= (\alpha \cdot \beta)+\alpha, \\
\alpha \cdot \lambda &= \sup \{\alpha \cdot \beta: \beta \in \lambda\} \quad (\lambda \text{ limit}).
\end{aligned}
$$

Show that $\alpha \cdot \beta=\operatorname{ot}(\leq_{\alpha \times \beta})$ where $\leq_{\alpha \times \beta}$ is the inverse lexicographic wellordering on $\alpha \times \beta$,

$$
\begin{gathered}
\operatorname{Field}(\leq_{\alpha \times \beta})=\alpha \times \beta, \\
\langle\xi_1, \eta_1\rangle<_{\alpha, \beta}\langle\xi_2, \eta_2\rangle \iff \eta_1 \in \eta_2 \vee[\eta_1=\eta_2 \,\&\, \xi_1 \in \xi_2],
\end{gathered}
$$

so that $\alpha \cdot \beta$ is the rank of the wellordering constructed by laying out β copies of α one after the other. Verify that

$$
\begin{aligned}
\alpha \cdot(\beta \cdot \gamma) &= (\alpha \cdot \beta) \cdot \gamma, \\
\alpha \cdot(\beta+\gamma) &= \alpha \cdot \beta+\alpha \cdot \gamma .
\end{aligned}
$$

Problem x7.24. Show that $2 \cdot \omega=\omega$ while $\omega<\omega \cdot 2$, so that ordinal multiplication is not in general commutative. Show also that for all $\alpha \geq \omega$,

$$
\begin{aligned}
&(\alpha+1) \cdot n=\alpha \cdot n+1 \quad (1<n<\omega), \\
&(\alpha+1) \cdot \omega=\alpha \cdot \omega,
\end{aligned}
$$

and infer that in general

$$
(\alpha+\beta) \cdot \gamma \neq \alpha \cdot \gamma+\beta \cdot \gamma .
$$

Problem x7.25 (Cancellation laws)**.** For all ordinals α, β, γ,

$$\begin{aligned} \alpha + \beta < \alpha + \gamma &\Longrightarrow \beta < \gamma, \\ \alpha + \beta = \alpha + \gamma &\Longrightarrow \beta = \gamma, \\ \alpha \cdot \beta < \alpha \cdot \gamma &\Longrightarrow \beta < \gamma, \\ 0 < \alpha \;\&\; \alpha \cdot \beta = \alpha \cdot \gamma &\Longrightarrow \beta = \gamma. \end{aligned}$$

Show also that, in general,

$$0 < \alpha \;\&\; \beta \cdot \alpha = \gamma \cdot \alpha \text{ does not imply } \beta = \gamma.$$

A *rank function* for a relation r is any

$$f : \mathrm{Field}(r) \to \mathrm{ON} \text{ such that } x <_r y \Longrightarrow f(\xi) \in f(y).$$

A rank function is *tight* if its image $f[\mathrm{Field}(r)]$ is an ordinal.

Problem x7.26. Prove that a relation r is wellfounded if and only if it admits a rank function. Show also that a wellfounded relation admits a unique tight rank function.

Problem x7.27. Prove that a set x is grounded if and only if every $y \in x$ is grounded.

Problem x7.28. Prove that the Axiom of Foundation holds if and only if every set is grounded.

Problem x7.29* ((2) of Theorem 7C.20)**.** Prove that for any two sets x, y,

$$(x \leq_c y \;\&\; y \leq_c x) \Longrightarrow x =_c y.$$

Problem x7.30. Prove that if x and y are wellorderable, then so are $x \cup y$ and $x \times y$.

Problem x7.31. Prove (1) – (4) of Theorem 7C.22.

Problem x7.32*. Prove the absorption law for cardinal multiplication, (5) of Theorem 7C.22.

Problem x7.33 (ZF)**.** Prove that $\mathcal{P}(\omega) =_c \mathcal{N}$, where $\mathcal{N} = (\omega \to \omega)$ is *Baire space*, the set of all functions on the natural numbers.

Problem x7.34 (ZF)**.** In one of the standard *arithmetizations of analysis*, the real numbers are identified with the set of *Dedekind cuts* of rationals,

$$\begin{aligned} \mathbb{R} = \{x \subseteq \mathbb{Q} : \emptyset \neq x \neq \mathbb{Q} \\ \& (\forall u \in x)(\forall v \in \mathbb{Q})[v < u \Longrightarrow v \in x] \;\&\; (\forall u \in x)(\exists v \in x)[u < v]. \end{aligned}$$

Outline a proof of $\mathbb{R} =_c \mathcal{P}(\omega)$ based on this definition of $\mathbb{R}$. (You will need to define $\mathbb{Q}$ in some natural way and check that $\mathbb{Q} =_c \omega$.)

Problem x7.35 (ZF)**.** Prove that for every set x, there is an ordinal ξ onto which x cannot be surjected,

$$(\forall x)(\exists \xi \in \mathrm{ON})(\forall f : x \to \xi)[f[x] \subsetneq \xi].$$

Problem x7.36 (ZF)**.** Prove that the class Card of cardinal numbers is proper, closed and unbounded.

Problem x7.37 (ZF)**.** Prove that for all ordinals η, ξ,

$$\eta < \xi \Longrightarrow \aleph_\eta < \aleph_\xi.$$

Problem x7.38 (ZF, Cantor's Theorem 7D.1)**.** Prove that for every set x, $x <_c \mathcal{P}(x)$.

Problem x7.39 (ZF)**.** Prove that a set x is grounded if and only if $\mathcal{P}(x)$ is grounded.

Problem x7.40 (ZF)**.** Prove Theorem 7D.5, the basic properties of the cumulative hierarchy of sets.

Problem x7.41 (ZF)**.** Prove the equivalence of the basic, elementary expressions of the Axiom of Choice, Theorem 7D.9.

Problem x7.42* (ZF)**.** Prove that if the powerset of every wellorderable set is wellorderable, then every grounded set is wellorderable.

Problem x7.43 (ZF)**.** Prove that $V \models$ ZF + Foundation, specifying whether this is a theorem or a theorem scheme. Infer that ZF cannot prove the existence of an *illfounded* (not grounded) set.

Problem x7.44 (ZF)**.** Prove that the equivalence

$$(\forall (i \mapsto a_i))[(\forall i \in I)[a_i \neq \emptyset] \iff \prod_{i \in I} a_i \neq \emptyset]$$

is equivalent to **AC**.

Problem x7.45 (ZFC)**.** Prove the cardinal equations and inequalities in Theorem 7E.1, and determine the values of λ, μ for which the implication

$$\lambda \leq \mu \Longrightarrow 0^\lambda \leq 0^\mu \qquad (\kappa \neq 0)$$

fails.

Problem x7.46. Prove Theorem 7E.4.

Problem x7.47. Write out the theorem scheme which is expressed by the Reflection Theorem 7D.7.

Problem x7.48***.** Prove that ZF, ZF_g and ZFC are not finitely axiomatizable (unless, of course, they are inconsistent). (Recall that by Definition 4A.6, a τ-theory T is finitely axiomatizable if there is a finite set T of τ-sentences which has the same theorems as T.)

Problem x7.49* (ZFC)**.** Prove that if κ is a strongly inaccessible cardinal, then $V_\kappa \models \mathsf{ZFC}$, specifying whether this is a theorem or a theorem scheme. Infer that

$$\mathsf{ZFC} \not\vdash (\exists\kappa)[\kappa \text{ is strongly inaccessible}].$$

Problem x7.50 (ZFC)**.** Prove that if there exists a strongly inaccessible cardinal, then there exists a countable, transitive set M such that

$$M \models \mathsf{ZFC}.$$

Problem x7.51* (ZFC)**.** True or false: *if* $V_\kappa \models \mathsf{ZFC}$*, then* κ *is strongly inaccessible.* You must prove your answer.

Problem x7.52. Give a correct version of the construction $\phi \mapsto (\phi)^M$ in Definition 7D.6 when M is a class defined by a formula with parameters.

Problem x7.53 (ZF)**.** Prove Theorem 7D.8.

Problem x7.54 (ZFC)**.** What is $\left(\prod_{i\in I} \mathbf{A}_i\right)/U$ is U is a principal ultrafilter on I?

Problem x7.55 (ZFC)**.** Let $\overline{\mathbf{A}} = \left(\prod_{i\in I} \mathbf{A}\right)/U$ be the ultrapower of a structure $\mathbf{A}$ modulo an ultrafilter U. Prove that there exists an elementary embedding $\pi : \mathbf{A} \rightarrowtail \overline{\mathbf{A}}$, and that π is an isomorphism if and only if U is principal. (Elementary embeddings are defined in Definition 2A.1.)

Problem x7.56 (ZFC)**.** Finish the argument in the proof of Łós's Theorem 7E.11.

Problem x7.57. Let I be an infinite set and F_0 a set of non-empty subsets of I which has the (weak) *finite intersection property*, i.e.,

$$X_1, X_2 \in F_0 \Longrightarrow (\exists X \in F_0)[X_1 \cap X_2 \supseteq X].$$

Prove that the set

$$F = \{Z \subseteq I : (\exists X \in F_0)[Z \supseteq X]\}$$

is a filter which extends F_0.

Problem x7.58. Give a proof of the Compactness Theorem 1J.1 for languages of arbitrary cardinality following the hint below.

Compactness Theorem (ZFC). *For any signature* τ*, if* T *is a* τ*-theory and every finite subset of* T *has a model, then* T *has a model.*

HINT: Let I be the set of all finite conjunctions $\phi_1 \mathbin{\&} \cdots \mathbin{\&} \phi_n$ of sentences in T, and choose (by the hypothesis) for each $\phi \in I$ a τ-structure $\mathbf{A}_\phi$ such that $\mathbf{A}_\phi \models \phi$. Let

$$X_\phi = \{\psi \in I : \mathbf{A}_\phi \models \psi\}, \quad F_0 = \{X_\phi : \phi \in I\}.$$

Check that each $X_\phi \neq \emptyset$ and that $X_\phi \cap X_\psi \supseteq X_{\phi \,\&\, \psi}$, so that F_0 has the weak intersection property and can be extended to a filter F by Problem x7.57 and then to an ultrafilter U on I by Theorem 7E.9. Now apply Łós's Theorem.

CHAPTER 8

THE CONSTRUCTIBLE UNIVERSE

Our main aim in this Chapter is to define Gödel's class L of constructible sets and to prove (in ZF) that it satisfies all the axioms of ZFC, as well as the Generalized Continuum Hypothesis. One of many corollaries will be the consistency of $\mathsf{ZFC} + \mathbf{GCH}$ relative to ZF.

Convention: *Unless otherwise specified* (as in Chapter 7), *all results in this Chapter are proved from the axioms of* ZF_g^-, i.e., ZF^- + Foundation.

This, means, in effect, that we are working in von Neumann's universe V of grounded sets but do not appeal to the powerset axiom—except as specified.

In fact, most of the arguments we will give do not depend on the axiom of foundation, and in a few cases, where it is important, we will point this out. It simplifies the picture, however, to include it in the background theory.

8A. Preliminaries and the basic definition

Our main aim in this section is to define L and show (in ZF_g) that is it is a model of ZF_g. The method is robust and can be extended to define many interesting "inner models" of set theory.

We have often made the argument that all classical mathematics can be "developed" in set theory. This is certainly true of mathematical logic, as we covered the subject in the first five chapter of these lecture notes, and perhaps more naturally than it is true of (say) analysis or probability, since the basic notions of logic are inherently set theoretical.

To be just a bit more specific:

- We fix once and for all a specific sequence $\mathbf{v} : \omega \to V$ whose values $\mathbf{v}_0, \mathbf{v}_1, \dots$, are the *variables*, (perhaps setting $\mathbf{v}_i = 2i \in \omega$).
- We fix once and for all specific sets for the logical symbols $\neg$, $\&$, $\dots \exists, \forall$, the parentheses and the comma (perhaps $\neg = 1, \& = 3, \dots$).

- A vocabulary (or signature) is any finite tuple

$$\tau = \langle \text{Const}, \text{Rel}, \text{Funct}, \text{arity} \rangle,$$

  such that the sets Const, Rel, Funct are pairwise disjoint (and do not contain any variables, logical or punctuation symbols as we chose those), and arity : Const $\cup$ Rel $\cup$ Funct $\to \omega$.

The syntactic objects of $\mathbb{FOL}(\tau)$ (terms, formulas, etc.) are now finite sequences from these basic sets and their formal definitions in $\mathbb{FOL}(\in)$ are obtained by formalizing their customary definitions. Structures of a specific signature τ are tuples of the form

$$\mathbf{A} = \langle A, \{c^{\mathbf{A}}\}_{c \in \text{Const}}, \{R^{\mathbf{A}}\}_{R \in \text{Rel}}, \{f^{\mathbf{A}}\}_{f \in \text{Funct}} \rangle$$

which satisfy the obvious conditions, and the definitions of all the other semantic notions (homomorphisms, satisfaction, etc.) are also assumed to have been formalized in $\mathbb{FOL}(\in)$. Especially interesting is the *structure of arithmetic*

$$\mathbf{N} = \langle \omega, 0, S, +, \cdot \rangle \tag{196}$$

which is definable in ZF^-, since ω is definable and addition and subtraction on ω can be defined by recursion, Theorem 7C.6. We will often use without explicit mention the fact that arithmetical relations on ω are definable in $\mathbb{FOL}(\in)$.

We do not need to get into the details of these formalizations of the basic notions of logic or the proofs in axiomatic set theory of the results in Chapters 1 – 5 any more than we need to do this in topology or probability theory. Except for one thing: for some of the metamathematical results with which we are concerned, it is sometimes very important to note that some theorems can be proved in a relatively weak set theory—ZF^- or ZF_g (without **AC**) for example—and so we will need to notice this. *As a general rule, most every result in Chapters 1 – 5 can be formalized and proved in* ZF^-, without using the Powerset, Foundation or Choice axioms. (The most notable exception is the Downward Skolem-Löwenheim Theorem 2B.1 which depends on **AC**.)

When we use variables m, n, k in the next theorem, it is understood that the conditions in question do not hold and the operations in question are set $= \emptyset$, unless $m, n, k \in \omega$. We continue with the numbering in Theorem 7C.2.

Theorem 8A.1. *The following conditions and operations on sets are definable:*

#37. $\text{Formula}(m, n) \iff m$ is the code of a (full extended) formula $\varphi(\mathbf{v}_0, \ldots, \mathbf{v}_{n-1})$ of the language $\mathbb{FOL}(\in)$

#38. $\mathrm{Sat}(m,n,x,A,e) \iff \mathrm{Formula}(m,n)$
$\& \, x : n \to A \,\&\, e \subseteq A \times A$
$\& \, \big[$ if $\varphi(\mathbf{v}_0, \dots, \mathbf{v}_{n-1})$ is the formula with code m, then $(A,e) \models \varphi\big[x(0), \dots, x(n-1)\big]\big]$

#39. $\mathbf{Def}_1(m,n,x,A,e) = \big\{ s \in A : \mathrm{Sat}(m, n+1, x \cup \{\langle n, s\rangle\}, A, e)\big\}$

#40. $\mathbf{Def}(A) = \big\{ \mathbf{Def}_1(m,n,x,A,\{\langle u,v\rangle : u \in v \,\&\, u \in A \,\&\, v \in A\}) : m \in \omega \,\&\, n \in \omega \,\&\, x : n \to A \big\}$

Proof. #37 is immediate since $\mathrm{Formula}(m,n)$ is recursive.

#39 and #40 will follow immediately once we prove #38, that the satisfaction condition is definable.

To prove #38, let

$$F_1(m,n,x,A,e) = \begin{cases} 1 & \text{if } m \text{ is the code of some full extended formula} \\ & \varphi(\mathbf{v}_0, \dots, \mathbf{v}_{n-1}) \text{ and } x : n \to A \text{ and } e \subseteq A \times A \\ & \text{and } (A,e) \models \varphi\big[x(0), \dots, x(n-1)\big], \\ 0 & \text{otherwise} \end{cases}$$

and put

$$F(m,A,e) = \{\langle i,n,x,F_1(i,n,x,A,e)\rangle : n \in \omega \,\&\, i < m \in \omega \,\&\, x : n \to A \,\&\, e \subseteq A \times A\};$$

it is enough to show that F is definable in $\mathbb{FOL}(\in)$, since

$$\mathrm{Sat}(m,n,x,A,e) \iff \langle m,n,x,1\rangle \in F(m+1,A,e).$$

To define F by recursion, applying Theorem 7C.6, we need definable operations G_1, G_2 such that

$$F(0,A,e) = G_1(A,e),$$
$$F(m+1,A,e) = G_2\big(F(m,A,e),m,A,e\big).$$

The first of these is trivial, since $F(0,A,e) = \emptyset$. On the other hand,

$$F(m+1,A,e) = F(m,A,e) \cup G_3(m,A,e)$$

where $G_3(m,A,e) = \emptyset$, unless m is the code of some full extended formula $\varphi(\mathbf{v}_0, \dots, \mathbf{v}_{n-1})$; and if m is the code of some such formula, then we can easily compute $G_3(m,A,e)$ from $F(m,A,e)$ because of the inductive nature of the definition of satisfaction—and the fact that formulas are assigned bigger codes than their proper subformulas. We will skip the details. ⊣

In (mathematical) English:

$x \in \mathbf{Def}(A) \iff x \subseteq A$ and there is a full extrended formula $\varphi(\mathbf{v}_0, \dots, \mathbf{v}_{n-1}, \mathbf{v}_n)$ in the language $\mathbb{FOL}(\in)$ and members $x_0, \dots, x_{n-1}$ of A, such that for all $s \in A$, $s \in x \iff (A, \in) \models \varphi[x_0, \dots, x_{n-1}, s]$.

Definition 8A.2 (ZF^-)**.** We now define the constructible hierarchy by the ordinal recursion

$$\begin{aligned} L_0 &= \emptyset, \\ L_{\xi+1} &= \mathbf{Def}(L_\xi), \\ L_\lambda &= \bigcup_{\xi<\lambda} L_\xi, \text{ if } \lambda \text{ is a limit ordinal} \end{aligned}$$

and we set $L = \bigcup_\xi L_\xi$. This is Gödel's class of *constructible sets*.

More generally, for any set A, put

$$\begin{aligned} L_0(A) &= \mathrm{TC}(A), \\ L_{\xi+1}(A) &= \mathbf{Def}\big(L_\xi(A)\big), \\ L_\lambda(A) &= \bigcup_{\xi<\lambda} L_\xi(A), \text{ if } \lambda \text{ is a limit ordinal,} \end{aligned}$$

and set $L(A) = \bigcup_\xi L_\xi(A)$. This is the class of sets *constructible from A*.

Theorem 8A.3 (ZF^-)**.** (i) *The operation $\xi \mapsto L_\xi$ is definable and L is a definable class.*

(ii) $\eta \leq \xi \Longrightarrow L_\eta \subseteq L_\xi$.

(iii) *Each L_ξ is a transitive, grounded set, L is a transitive class and $L \subseteq V$.*

Similarly,

(ia) *The operation $(\xi, A) \mapsto L_\xi(A)$ is definable, and if A is a definable set, then $L(A)$ is a definable class.*

(iia) $\eta \leq \xi \Longrightarrow L_\eta(A) \subseteq L_\xi(A)$.

(iiia) *Each $L_\xi(A)$ is a transitive set and $L(A)$ is a transitive class. If, in addition, A is grounded, then every $L_\xi(A)$ is grounded and $L(A) \subseteq V$.*

Proof. (i) follows immediately from Theorem 7C.16.

To prove (ii) and (iii) we show simultaneously by ordinal induction that for each ξ,

$$L_\xi \text{ is transitive, grounded and } \eta < \xi \Longrightarrow L_\eta \subseteq L_\xi.$$

This is trivial for $\xi = 0$ or limit ordinals ξ.

If $\xi = \zeta + 1$, suppose first that $\eta = \zeta$ and $x \in L_\zeta$. The induction hypothesis gives us that $x \subseteq L_\zeta$; and since x is clearly definable in L_ζ by the formula $\mathbf{v}_i \in x$ (with the parameter x), we have $x \in L_{\zeta+1}$. So $L_\zeta \subseteq L_{\zeta+1}$, and the transitivity of $L_{\zeta+1}$ follows immediately. If $\eta < \zeta$, then the induction hypothesis gives again $x \in L_\zeta$, and so $x \in L_{\zeta+1}$ by what we have just proved.

Now L is easily transitive as the union of transitive sets and (ia)–(iiia) are proved similarly. ⊣

To prove that L satisfies ZF^-_g, we need to look a little more carefully at its definition.

Definition 8A.4 (Σ_0 formulas)**.** Let Σ_0 be the smallest collection of formulas in the language $\mathbb{FOL}(\in)$ which contains all prime formulas

$$\mathbf{v}_i \in \mathbf{v}_j, \quad \mathbf{v}_i = \mathbf{v}_j$$

and is closed under the propositional operations and the bounded quantifiers, so that if φ and ψ are in Σ_0, then so are the formulas

$$\neg(\varphi),\ (\varphi)\,\&\,(\psi),\ (\varphi)\vee(\psi),\ (\varphi)\rightarrow(\psi),\ (\exists \mathbf{v}_i \in \mathbf{v}_j)\phi,\ (\forall \mathbf{v}_i \in \mathbf{v}_j)\phi.$$

Proposition 8A.5. *Prove that the conditions #1, #2, #8, #9, #14, #17 and #18 or 7C.2 are definable by Σ_0 formulas.*

One of the simplifying consequences of the Axiom of Foundation is that the class of ordinals becomes definable by a Σ_0 formula:

(197) $\xi \in \mathrm{ON}$

$$\iff (\forall x \in \xi)(\forall x \in y)[x \in \xi]\ \&\ (\forall x, y \in \xi)[x \in y \vee x = y \vee y \in x].$$

This is very useful, because of the following, simple but very basic fact about Σ_0:

Lemma 8A.6. *Let M be a transitive class.*

(i) *If $\varphi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ is a full extended Σ_0 formula and $x_1, \dots, x_n \in M$, then*

$$V \models \varphi[x_1, \dots, x_n] \iff M \models \varphi[x_1, \dots, x_n].$$

(ii) *M satisfies the Axioms of Extensionality and Foundation.*

(iii) *If M is closed under pairing and union, then it satisfies the Pairing and Unionset axioms.*

(iv) *If some infinite ordinal $\lambda \in M$, then M satisfies the Axiom of Infinity.*

Proof. (i) Reverting to the notation of Theorem 1C.9 which is more appropriate here, we need to verify that if φ is any formula in Σ_0 and π : Variables $\to M$ is any assignment into M, then

$$V, \pi \models \varphi \iff M, \pi \models \varphi.$$

This is immediate for prime formulas, e.g.,

$$\begin{aligned} V, \pi \models \mathbf{v}_i \in \mathbf{v}_j &\iff \pi(\mathbf{v}_i) \in \pi(\mathbf{v}_j) \\ &\iff M, \pi \models \mathbf{v}_i \in \mathbf{v}_j \end{aligned}$$

(because π takes values in M) and if the required equivalence holds for φ and ψ, it obviously holds for $\neg(\varphi)$ and for $(\varphi)\,\&\,(\psi)$. By induction on the length of formulas then, in one of the non-trivial cases,

$$\begin{aligned} V,\pi \models (\exists \mathbf{v}_i)[\mathbf{v}_i \in \mathbf{v}_j \,\&\, \varphi] &\iff \text{for some } z \in \pi(\mathbf{v}_j),\, V,\pi\{\mathbf{v}_i := z\} \models \varphi \\ &\iff \text{for some } z \in \pi(\mathbf{v}_j),\, M,\pi\{\mathbf{v}_i := z\} \models \varphi \\ &\iff M,\pi \models (\exists \mathbf{v}_i)[\mathbf{v}_i \in \mathbf{v}_j \,\&\, \varphi], \end{aligned}$$

where we have used the transitivity of M and (again) the fact that π takes values in M in the main, middle equivalence.

(ii) Both of these axioms are expressed in $\mathbb{FOL}(\in)$ by formulas of the form $(\forall \mathbf{x}_1)\cdots(\forall \mathbf{x}_n)\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ where $\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ is in Σ_0 and

$$\text{for all } x_1,\ldots,x_n \in M, V \models \phi[x_1,\ldots,x_n];$$

this implies with (i) that $M \models (\forall \mathbf{x}_1)\cdots(\forall \mathbf{x}_n)\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n)$.

(iii) Again, it is easy to find a formula $\varphi(\mathbf{x},\mathbf{y},\mathbf{z})$ in Σ_0 such that for x, y,

$$z = \{x, y\} \iff V \models \varphi[x, y, z].$$

To show that M satisfies the Pairing Axiom then, we must verify that for each $x \in M$, $y \in M$, there is some $z \in M$ such that $M \models \varphi[x, y, z]$; of course, we take $z = \{x, y\}$ and we use (i).

The argument for the Unionset Axiom is similar.

(v) If $\lambda \in M$ and λ is infinite, then either $\omega = \lambda$ or $\omega \in \lambda$ and in either case, by the transitivity of M, $\omega \in M$. Checking the definition of ω in Theorem 7C.2, we can construct a Σ_0 formula $\varphi(\mathbf{x})$ such that

$$x = \omega \iff V \models \varphi[x];$$

in part $\varphi(\mathbf{x})$ asserts that $\mathbf{x}$ is the z required to exist by the Axiom of Infinity. Clearly $V \models \varphi[\omega]$ and then by (i), $M \models \varphi[\omega]$ so that M satisfies the Axiom of Infinity. ⊣

The lemma implies immediately that L satisfies all the axioms of ZF_g except perhaps for the Power and Replacement Axioms. The key to deriving these for L is the Reflection Theorem 7D.7, but it is worth putting down a general result.

It is convenient to call a class M *grounded* if every set in it is grounded, i.e., if $M \subseteq V$ (cf. Problem x8.5). All classes are grounded in ZF_g^-, but it is instructive make an exception to the general convention of this Chapter and show the next theorem with the minimum hypotheses.

Theorem 8A.7 (ZF^-). *Let $\xi \mapsto C_\xi$ be an operation on ordinals to sets which satisfies the following four conditions, where $C = \bigcup_{\xi \in \mathrm{ON}} C_\xi$.*

(i) *Each C_ξ is a grounded, transitive set.*

(ii) $\zeta \le \xi \Longrightarrow C_\zeta \subseteq C_\xi$.

(iii) *If λ is a limit ordinal, then* $C_\lambda = \bigcup_{\xi<\lambda} C_\xi$.

(iv) *For each* ξ, $\mathbf{Def}(C_\xi) \subseteq C$, *i.e., for each* ξ, *if* $x \subseteq C_\xi$ *is elementary in the structure*

$$\mathbf{C}_\xi = (C_\xi, \in \restriction C_\xi, \{s : s \in C_\xi\}),$$

then there is some ζ *such that* $x \in C_\zeta$.

It follows that C *is a transitive subclass of* V*, it contains all the ordinals and* $C \models \mathsf{ZF}_g^-$*; and if, in addition, we assume the Powerset Axiom, then* $C \models \mathsf{ZF}_g$.

In particular, $L \subseteq V$*, it is a transitive model of* ZF_g^- *which contains all the ordinals, and if we assume the Powerset Axiom, then* $L \models \mathsf{ZF}_g$.

Similarly for $L(A)$*, if* A *is grounded.*

Proof. To begin with, we know from Lemma 8A.6 that C satisfies extensionality, pairing and unionset, since condition (iv) in the hypothesis implies easily that C is closed under pairing and union and these parts of Lemma 8A.6 where proved without the axiom of foundation. Also, $C_\xi \subseteq V$ by ordinal induction, and so $C \subseteq V$—and then it satisfies the Axiom of Foundation because V does.

We argue that C must contain all ordinals: if not, let λ be the least ordinal not in C and choose ξ large enough so that $\lambda \subseteq C_\xi$. Since V satisfies the Axiom of Foundation, for $x \in V$,

$$\text{Ordinal}(x) \iff V \models \phi_{\text{ON}}[x]$$

where

$$\phi_{\text{ON}}(\mathbf{x}) \equiv (\forall u \in \mathbf{x})(\forall v \in u)[v \in \mathbf{x}] \ \&\ (\forall u, v \in \mathbf{x})[u \in v \vee u = v \vee v \in u]$$

is a Σ_0-formula, as in (197). Since no ordinal $\geq \lambda$ can be in C_ξ (by transitivity), we have

$$\{x \in C_\xi : \mathbf{C}_\xi \models \varphi_{\text{ON}}[x]\} = \lambda;$$

hence by condition (iv), $\lambda \in C$, which is a contradiction.

It follows in particular that $\omega \in C$, so that C also satisfies the Axiom of Infinity by 8A.6.

Verification of the Powerset Axiom (ZF). It is enough to show that for each $x \in C$, there is some $z \in C$ such that z has as members precisely all the members of C which are subsets of x—from this we can infer that C satisfies the Powerset Axiom as above. Let

$$\text{rank}_C(u) = \begin{cases} \text{least } \eta \text{ such that } u \in C_\eta, & \text{if } u \in C,\\ 0 & \text{otherwise,}\end{cases}$$

and set

$$\lambda = \bigcup \text{rank}_C[\mathcal{P}(x)]$$

so that if $u \in C$ and $u \subseteq x$, then $u \in C_\lambda$. Thus

$$z = \{u \in C_\lambda : u \subseteq x\}$$

has as members precisely the subsets of x which are in C and since z is clearly definable in $\mathbf{C}_\lambda$, it is a member of C by (iv).

Verification of the Axiom Scheme of Replacement. Suppose $x \in C$ and $F : C \to C$ is an operation which is definable (with parameters) on C, i.e., for some formula $\psi(\mathbf{v}_1, \dots, \mathbf{v}_n, \mathbf{s}, \mathbf{t})$ and fixed $y_1, \dots, y_n \in C$,

$$F(s) = t \iff C \models \psi[y_1, \dots, y_n, s, t] \qquad (s, t \in C);$$

as above, it is enough to show that the image

$$F[x] = \{F(s) : s \in x\}$$

is also a member of C.

Using the Reflection Theorem 7D.7, choose λ so that $x, y_1, \dots, y_n \in C_\lambda$ and for $s, t \in C_\lambda$,

$$C \models \psi[y_1, \dots, y_n, s, t] \iff C_\lambda \models \psi[y_1, \dots, y_n, s, t],$$

make sure as in the argument above that $F[x] \subseteq C_\lambda$, and set

$$\psi^*(\mathbf{y}_1, \dots, \mathbf{y}_n, \mathbf{x}, \mathbf{t}) \equiv (\exists \mathbf{s} \in \mathbf{x})\psi(\mathbf{y}_1, \dots, \mathbf{y}_n, \mathbf{x}, \mathbf{t}).$$

Clearly

$$F[x] = \{t \in C_\lambda : \mathbf{C}_\lambda \models \psi^*[y_1, \dots, y_n, \mathbf{s}, t]\},$$

and hence $F[x]$ is elementary in $\mathbf{C}_\lambda$ and must be in C by (iv).

This concludes the proof of the main part of the theorem and the fact that L and $L(A)$ satisfy the hypotheses follows easily from their definitions. $\dashv$

The recursive definition of the constructible hierarchy $\{L_\xi : \xi \in \mathrm{ON}\}$ makes it possible to define explicitly a wellordering of L. We prove this in some detail, as it is the key to our showing in the next section that the Axiom of Choice holds in L.

Theorem 8A.8 (The wellordering of L)**.** *There is a definable binary condition $x \leq_L y$ which wellorders L, and in such a way that*

$$x \leq_L y \,\&\, y \in L_\xi \Longrightarrow x \in L_\xi.$$

Proof. The idea is to define by ordinal recursion an operation

$$F : \mathrm{ON} \to V$$

so that for each ξ, $F(\xi) = \ \leq_\xi$ is a wellordering of L_ξ, i.e., $\leq_\xi \subseteq L_\xi \times L_\xi$ and $\leq_\xi$ wellorders L_ξ.

We will build up F step-by-step.

Step 1. There is a definable operation $F_1 : \omega \times V \times V \to V$ such that if w wellorders A, then $F_1(n, w, A)$ wellorders the set $(n \to A)$ of n-term sequences from A.

Proof. Order the n-tuples from A lexicographically, using w.

Step 2. There is a definable operation $F_2 : V^2 \to V$ such that if w wellorders A, then $F_2(w, A)$ wellorders $A^* = \bigcup_{n\in\omega}(n \to A)$.

Proof. For x, x' in A^*, put

$$\begin{aligned}\langle x, x'\rangle \in F(w, A) \iff\ & \text{Domain}(x) < \text{Domain}(x')\\ & \vee(\exists n)[\text{Domain}(x) = \text{Domain}(x') = n\\ & \qquad \& \,\langle x, x'\rangle \in F_1(n, w, A)].\end{aligned}$$

Step 3. There is a definable operation $F_3 : V^2 \to V$ such that if w wellorders A, then $F_3(w, A)$ wellorders $\mathbf{Def}(A)$.

Proof. Using the operation $\mathbf{Def}_1$ of Theorem 8A.1, put

$$G_1(m, n, x, A) = \mathbf{Def}_1(m, n, A, \{\langle u, v\rangle : u \in A \,\&\, v \in A \,\&\, u \in v\})$$

and for $y \in \mathbf{Def}(A)$ define successively:

$$\begin{aligned}G_2(y, w, A) &= \text{least } m \text{ such that } (\exists n)(\exists x : n \to A)[y = G_1(m, n, x, A)],\\ G_3(y, w, A) &= \text{least } n \text{ such that } (\exists x : n \to A)[y = G_1\big(G_2(y, w, A), n, x, A\big)],\\ G_4(y, w, A) &= \text{least } x \text{ in the ordering } F_2(w, A) \text{ such that}\\ &\qquad y = G_1\big(G_2(y, w, A), G_3(y, w, A), x, A\big).\end{aligned}$$

Now each $y \in \mathbf{Def}(A)$ is completely determined by the triple

$$\big(G_2(y, w, A), G_3(y, w, A), G_4(y, w, A)\big)$$

and we can order these triples lexicographically, using the wellordering $F_2(w, A)$ in the last component.

Step 4. There is a definable operation $F : \mathrm{ON} \to V$ such that for each ξ, $F(\xi)$ is a wellordering of L_ξ.

We define $F(\xi)$ by ordinal recursion, taking cases on whether ξ is 0, a successor or limit.

Two of the cases are trivial: we set $F(0) = \emptyset$ and $F(\xi+1) = F_3\big(F(\xi), L_\xi\big)$.

If λ is limit, define first $G : L \to \mathrm{ON}$ by

$$G(x) = \text{least } \xi \text{ such that } x \in L_\xi$$

and put

$$\begin{aligned}F(\lambda) = \big\{\langle x, y\rangle \in\ & L_\lambda \times L_\lambda : G(x) < G(y)\\ & \vee\big[G(x) = G(y) \,\&\, \langle x, y\rangle \in F\big(G(x)\big)\big]\big\}.\end{aligned}$$

The theorem follows from this by setting again

$$x \leq_L y \iff G(x) < G(y) \vee \big[G(x) = G(y) \,\&\, \langle x, y\rangle \in F\big(G(x)\big)\big]. \qquad \dashv$$

8B. Absoluteness

At first blush, it seems like Theorem 8A.8 proves that L satisfies **AC**: we defined a condition $x \leq_L y$ on the constructible sets and we showed that it wellorders L, from which it follows that

$$\text{(198)} \quad \text{“if every set is in } L\text{, then } \{(x,y) : x \leq_L y\} \text{ wellorders the universe of all sets”.}$$

This is a very strong, "global" and definable form of the Axiom of Choice for L, and we proved it in ZF_g^- (in fact in ZF^-)—but it does not quite mean the same thing as "$L \models \mathbf{AC}$"!

To see the subtle difference in meaning between the two claims in quotes, let us express (198) in the language $\mathbb{FOL}(\in)$. Choose first a formula $\varphi_L(\mathbf{x}, \boldsymbol{\xi})$ of $\mathbb{FOL}(\in)$ by 8A.3 so that

$$\text{(199)} \qquad x \in L_\xi \iff V \models \varphi_L[x, \xi]$$

and let

$$\text{(200)} \qquad V = L :\equiv (\forall \mathbf{x})(\exists \boldsymbol{\xi})\varphi_L(\mathbf{x}, \boldsymbol{\xi}).$$

The formal sentence "$V = L$" expresses in $\mathbb{FOL}(\in)$ the proposition that *every (grounded) set is constructible.* Choose then another formula $\psi_L(\mathbf{x}, \mathbf{y})$ of $\mathbb{FOL}(\in)$ by 8A.8 such that

$$x \leq_L y \iff V \models \psi_L[x, y]$$

and set

$$\psi^* \iff \text{“}\{(\mathbf{x}, \mathbf{y}) : \psi_L(\mathbf{x}, \mathbf{y})\} \text{ is a wellordering of the universe”},$$

where it is easy to turn the symbolized English in quotes into a formal sentence of $\mathbb{FOL}(\in)$. Now (198) is expressed by the formal sentence of $\mathbb{FOL}(\in)$

$$(V = L) \rightarrow \psi^*,$$

and what we would like to prove is that

$$\text{(201)} \qquad L \models \psi^*.$$

It is important here that Theorem 8A.8 was proved in ZF without appealing to **AC**. Since L is a model of ZF_g by 8A.7, it must also satisfy all the consequences of ZF_g and certainly

$$\text{(202)} \qquad L \models (V = L) \rightarrow \psi^*.$$

Now the hitch is that in order to infer (201) from (202), we must prove

$$\text{(203)} \qquad L \models V = L \qquad \text{(Caution! Not proved yet).}$$

This is what we are tempted to take as "obvious" in a sloppy reading of (198). But is (203) obvious?

By the definition of satisfaction and the construction of the sentence $V = L$ above, (203) is equivalent to

(204) for each $x \in L$, there exists $\xi \in L$ such that $L \models \varphi_L[x, \xi]$,

while what we know is

(205) for each $x \in L$, there exists $\xi \in L$ such that $V \models \varphi_L[x, \xi]$.

Thus, to complete the proof of (203) and verify that L satisfies the Axiom of Choice, we must prove that we can choose the formula $\varphi_L(\mathbf{x}, \boldsymbol{\xi})$ so that in addition to (199), it also satisfies

(206) $$V \models \varphi_L[x, \xi] \iff L \models \varphi_L[x, \xi],$$

when $x \in L$. In other words, we must show that *the basic condition of constructibility can be defined in* $\mathbb{FOL}(\in)$ *so that the model* L *recognizes that each of its members is constructible.*

The theory of *absoluteness* (for grounded classes) which we will develop to do this is the key to many other results, including the fact that $V = L$ implies the Generalized Continuum Hypothesis. We will study here the basic facts about absoluteness and then we will derive the consequences about L in the next section.

Definition 8B.1 (Absoluteness)**.** Let R be an n-ary condition on V, let $\phi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ be a full extended $\mathbb{FOL}(\in)$-formula, and let $\mathcal{D}$ be a collection of transitive subclasses of V. We say that $\phi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ *defines* R *absolutely for* $M \in \mathcal{D}$ if

$$R(x_1, \dots, x_n) \iff M \models \varphi[x_1, \dots, x_n] \quad (M \in \mathcal{D}, x_1, \dots, x_n \in M).$$

A condition R is *absolute for* $\mathcal{D}$ if it is defined by some formula absolutely for $M \in \mathcal{D}$. It is also common to call *absolute for* $\mathcal{D}$ the relevant formula $\varphi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ of $\mathbb{FOL}(\in)$ which defines a condition absolutely for $\mathcal{D}$.

Notice that if $\varphi(\mathbf{x}_1, \dots, \mathbf{x}_n)$ defines R absolutely for $\mathcal{D}$, then in particular, for M, N in $\mathcal{D}$, if $M \subseteq N$ and $x_1, \dots, x_n \in M$, then

$$M \models \varphi[x_1, \dots, x_n] \iff N \models \varphi[x_1, \dots, x_n].$$

In all the cases we will consider, the universe V of grounded sets will be in $\mathcal{D}$; then for each M in $\mathcal{D}$ and $x_1, \dots, x_n \in M$, we have

$$\begin{aligned} R(x_1, \dots, x_n) &\iff V \models \varphi[x_1, \dots, x_n] \\ &\iff M \models \varphi[x_1, \dots, x_n]. \end{aligned}$$

We express this by saying that R *is absolute for* M.

Following the same idea, an operation $F : C_1 \times \cdots \times C_n \to V$ (where $C_1, \dots, C_n$ are given classes) is *definable absolutely for* $\mathcal{D}$ or just *absolute for* $\mathcal{D}$, if three things hold.

(1) The classes $C_1, C_2, \ldots, C_n$ are absolute for $\mathcal{D}$—i.e., each membership condition $x \in C_i$ is absolute for $\mathcal{D}$.

(2) If $M \in \mathcal{D}$ and $x_1 \in C_1 \cap M, \ldots, x_n \in C_n \cap M$, then

$$F(x_1, \ldots, x_n) \in M.$$

(3) There is a formula $\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y})$ of $\mathbb{FOL}(\in)$ such that for each $M \in \mathcal{D}$ and $x_1 \in C_1 \cap M, \ldots, x_n \in C_n \cap M$,

$$F(x_1, \ldots, x_n) = y \iff M \models \varphi[x_1, \ldots, x_n, y].$$

A set c is *absolute for* $\mathcal{D}$ if for each $M \in \mathcal{D}$, $c \in M$ and the condition

$$R_c(x) \iff x = c$$

is absolute for $\mathcal{D}$.

We now come to the central metamathematical concept of T-absoluteness, where T is any *set theory*, e.g., ZF^-, ZF^-_g, ZF, ZFC, etc. We simplify the discussion a bit by collectively calling *notions* the relations and operations on V as well as the members of V (following Gödel).

Definition 8B.2 (T-absoluteness)**.** Let T be a set of $\mathbb{FOL}(\in)$-sentences—a *set theory.*

A *standard model* of T is any transitive, grounded class M (perhaps a set) such that $M \models T$; if in addition M contains all the ordinals, then M is an *inner model* of T. (By Theorem 8A.7, *L and each $L(A)$ are inner models of ZF^-_g*, and in ZF we proved that they are both inner models of ZF_g.)

A notion N is *T-absolute* if there exists a finite set $T^0 \subseteq T$ of axioms of T such that N is absolute for the collection $\mathcal{D}^0$ of standard models of T^0,

$$M \in \mathcal{D}^0 \iff M \text{ is transitive and } M \models T^0.$$

Notice that *if N is T-absolute and $T \subseteq T'$, then N is T'-absolute.* We are especially interested in ZF^-_g-absolute notions, which are then T-absolute for every axiomatic set theory stronger than ZF^-_g. Intuitively, a notion N is T-absolute if there is a formula of $\mathbb{FOL}(\in)$ which defines N in all standard models of some sufficiently large, finite part of T.

We will need to know that a good many notions are ZF^-_g-absolute, including all those defined in Theorems 7C.2 and 8A.1, and we start with the closure properties of the collection of T-absolute notions.

All but the last two parts of the next theorem have nothing to do with any particular set-theoretic principles—they are simple facts of logic.

Theorem 8B.3. *Let T be any set theory such that $V \models T$.*

(i) *The collection of T-absolute conditions contains $\in$ and $=$ and is closed under the propositional operations $\neg$, $\&$, $\vee$, $\Longrightarrow$, $\iff$.*

(ii) *The collection of T-absolute operations is closed under addition and permutation of variables and under composition; each n-ary projection operation*

$$F(x_1, \ldots, x_n) = x_i$$

is T-absolute.

(iii) *An object $c \in V$ is T-absolute if and only if each n-ary constant operation*

$$F(x_1, \ldots, x_n) = c$$

is T-absolute.

(iv) *If $R \subseteq V^m$ and $F_1 : C_1 \times \cdots \times C_n \to V, \ldots, F_m : C_1 \times \cdots \times C_n \to V$ are all T-absolute and*

$$P(x_1, \ldots, x_n) \iff x_1 \in C_1 \,\&\, \cdots \,\&\, x_n \in C_n \\ \& \, R\big(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)\big),$$

then P is also T-absolute.

(v) *If $R \subseteq V^{n+1}$ is T-absolute and*

$$P(x_1, \ldots, x_n, z) \iff (\exists y \in z) R(x_1, \ldots, x_n, y),$$
$$Q(x_1, \ldots, x_n, z) \iff (\forall y \in z) R(x_1, \ldots, x_n, y),$$

then P and Q are also T-absolute.

(vi) *Suppose $P \subseteq V^{n+1}$ and $Q \subseteq V^{n+1}$ are both T-absolute, and there exists a finite $T^0 \subseteq T$ such that for each standard M, if $M \models T^0$ and $x_1, \ldots, x_n \in M$, then*

$$(\exists y \in M) P(x_1, \ldots, x_n, y) \iff (\forall y \in M) Q(x_1, \ldots, x_n, y);$$

then the condition $R \subseteq V^n$ defined by

$$R(x_1, \ldots, x_n) \iff (\exists y) P(x_1, \ldots, x_n, y)$$

is T-absolute.

(vii) *Suppose $T \supseteq \mathsf{ZF}^-_g$. If $G : V^{n+1} \to V$ is T-absolute, then so is the operation $F : V^{n+1} \to V$ defined by*

$$F(x_1, \ldots, x_n, w) = \{G(x_1, \ldots, x_n, t) : t \in w\}.$$

Similarly with parameters, if $G : V^{n+m} \to V$ is T-absolute, so is

$$F(x_1, \ldots, x_n, w_1, \ldots, w_m) \\ = \{G(x_1, \ldots, x_n, t_1, \ldots, t_m) : t_1 \in w_1 \,\&\, \cdots \,\&\, t_n \in w_n\}.$$

(viii) *If $T \supseteq \mathsf{ZF}^-_g$ and $R \subseteq V^{n+1}$ is T-absolute, then so is the operation*

$$F(x_1, \ldots, x_n, w) = \{t \in w : R(x_1, \ldots, x_n, t)\} \quad (x_1, \ldots, x_n, w \in V).$$

Proof. Parts (i) – (iv) are very easy, using the basic properties of the language $\mathbb{FOL}(\in)$.

For example if

$$R(x_1,\dots,x_n) \iff P(x_1,\dots,x_n)\,\&\,Q(x_1,\dots,x_n)$$

with P and Q given T-absolute conditions, choose finite $T^0 \subseteq \mathbf{ZF}$, $T^1 \subseteq T$ and formulas $\varphi(\mathbf{x}_1,\dots,\mathbf{x}_n)$, $\psi(\mathbf{x}_1,\dots,\mathbf{x}_n)$ of $\mathbb{FOL}(\in)$ such that

$$P(x_1,\dots,x_n) \iff M \models \varphi[x_1,\dots,x_n] \quad (M \models T^0,\ x_1,\dots,x_n \in M)$$

and for $M \models T^1$, $x_1,\dots,x_n \in M$,

$$Q(x_1,\dots,x_n) \iff M \models \psi[x_1,\dots,x_n].$$

It is clear that if $M \models T^0 \cup T^1$ and $x_1,\dots,x_n \in M$, then

$$R(x_1,\dots,x_n) \iff M \models \varphi[x_1,\dots,x_n]\,\&\,\psi[x_1,\dots,x_n],$$

so the formula $\varphi(\mathbf{x}_1,\dots,\mathbf{x}_n)\,\&\,\psi(\mathbf{x}_1,\dots,\mathbf{x}_n)$ defines R absolutely on all standard models of $T^0 \cup T^1$.

Suppose again that

$$F(x) = G\big(H_1(x), H_2(x)\big)$$

where G, H_1, H_2 are T-absolute and we have chosen one binary and two unary operations to simplify notation. Choose finite subsets T^G, T^1, T^2 of T and formulas $\psi(\mathbf{u},\mathbf{v},\mathbf{z})$, $\varphi_1(\mathbf{x},\mathbf{u})$, $\varphi_2(\mathbf{x},\mathbf{v})$ of $\mathbb{FOL}(\in)$ such that for $M \models T^G$ and $u,v,z \in M$ we have $G(u,v) \in M$ and

$$G(u,v) = z \iff M \models \psi[u,v,z]$$

and similarly with H_1, T^1 and $\varphi_1(\mathbf{x},\mathbf{u})$, H_2, T^2 and $\varphi_2(\mathbf{x},\mathbf{v})$. (It is easy to arrange that the free variables in these formulas are as indicated.) Now it is clear that if

$$M \models T^G \cup T^1 \cup T^2,$$

then

$$x \in M \Longrightarrow F(x) \in M$$

and for $x, z \in M$,

$$F(x) = z \iff M \models \chi[x,z]$$

where

$$\chi(\mathbf{x},\mathbf{z}) \iff (\exists\mathbf{u})(\exists\mathbf{v})[\varphi_1(\mathbf{x},\mathbf{u})\,\&\,\varphi_2(\mathbf{x},\mathbf{v})\,\&\,\psi(\mathbf{u},\mathbf{v},\mathbf{z})].$$

Proof of (iv) is very similar to this.

(v) The argument is very similar to the proof of (i) in Lemma 8A.6 and we will omit it—the transitivity of M is essential here.

(vi) Choose a formula $\varphi(\mathbf{x}_1,\dots,\mathbf{x}_n,\mathbf{y})$ and a finite $T^P \subseteq T$ such that for all standard $M \models T^P$ and $x_1,\dots,x_n \in M$,

$$P(x_1,\dots,x_n,y) \iff M \models \varphi[x_1,\dots,x_n,y]$$

and take

$$\chi(\mathbf{x}_1,\ldots,\mathbf{x}_n) \iff (\exists\mathbf{y})\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{y}).$$

If $M \models T^P \cup T^0$ and $x_1,\ldots,x_n \in M$, then

$$\begin{aligned}
R(x_1,\ldots,x_n) &\Longrightarrow (\exists y)P(x_1,\ldots,x_n,y) \\
&\Longrightarrow (\forall y)Q(x_1,\ldots,x_n,y) && \text{(since } V \models T^0\text{)} \\
&\Longrightarrow (\forall y\in M)Q(x_1,\ldots,x_n,y) && \text{(obviously)} \\
&\Longrightarrow (\exists y\in M)P(x_1,\ldots,x_n,y) && \text{(since } M \models T^0\text{)} \\
&\Longrightarrow \text{for some } y\in M,\ M \models \varphi[x_1,\ldots,x_n,y] && \text{(since } M \models T^P\text{)} \\
&\Longrightarrow M \models (\exists\mathbf{y})\varphi[x_1,\ldots,x_n,\mathbf{y}];
\end{aligned}$$

Conversely,

$$\begin{aligned}
M \models (\exists\mathbf{y})\varphi[x_1,\ldots,x_n,\mathbf{y}] &\Longrightarrow (\exists y\in M)P(x_1,\ldots,x_n,y) \\
&\Longrightarrow (\exists y)P(x_1,\ldots,x_n,y) \\
&\Longrightarrow R(x_1,\ldots,x_n),
\end{aligned}$$

so $\chi(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ defines R on all models of $T^P \cup T^0$ and hence R is T-absolute.

(vii) Suppose that if $M \models T^0$, then

$$x_1,\ldots,x_n,t \in M \Longrightarrow G(x_1,\ldots,x_n,t) \in M$$

and

$$G(x_1,\ldots,x_n,t) = s \iff M \models \varphi[x_1,\ldots,x_n,t,s].$$

Let ψ be the instance of the Replacement Axiom Scheme which concerns $\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{t},\mathbf{s})$,

$$\begin{aligned}
\psi \iff (\forall\mathbf{x}_1)\cdots(\forall\mathbf{x}_n)(\forall\mathbf{w})\big\{&(\forall\mathbf{t})(\exists!\mathbf{s})\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{t},\mathbf{s}) \\
&\to (\exists\mathbf{z})(\forall\mathbf{s})\big[\mathbf{s}\in\mathbf{z} \leftrightarrow (\exists\mathbf{t})[\mathbf{t}\in\mathbf{w}\,\&\,\varphi(\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{t},\mathbf{s})]\big]\big\}
\end{aligned}$$

and take

$$T^1 = T^0 \cup \{\psi\}.$$

If $M \models T^1$ and $x_1,\ldots,x_n,w \in M$, this means easily that there is some $z \in M$ so that for all $a \in M$,

$$\begin{aligned}
s \in z &\iff \text{for some } t\in w,\ M \models \varphi[x_1,\ldots,x_n,t,s] \\
&\iff (\exists t\in w)[G(x_1,\ldots,x_n,t) = s].
\end{aligned}$$

Since $M \models T^0$ and hence M is closed under G, this implies that in fact

$$\begin{aligned}
z &= \{G(x_1,\ldots,x_n,t) : t\in w\} \\
&= F(x_1,\ldots,x_n,w),
\end{aligned}$$

hence M is closed under F. Moreover, taking

$$\chi(\mathbf{x}_1,\dots,\mathbf{x}_n,\mathbf{w},\mathbf{z}) \iff (\forall \mathbf{s})\big[\mathbf{s}\in\mathbf{z} \leftrightarrow (\exists \mathbf{t})[\mathbf{t}\in\mathbf{w} \,\&\, \varphi(\mathbf{x}_1,\dots,\mathbf{x}_n,\mathbf{t},\mathbf{s})]\big],$$

is is clear that

$$F(x_1,\dots,x_n,w)=z \iff M\models \chi[x_1,\dots,x_n,w,z],$$

so F is T absolute.

The argument with $m>1$ is similar.

(viii) Let

$$G(x_1,\dots,x_n,w,t)=\begin{cases} t & \text{if } R(x_1,\dots,x_n,t),\\ w & \text{if } \neg R(x_1,\dots,x_n,t).\end{cases}$$

This is T-absolute by (ii) and then by the hypothesis that $T\supseteq \mathsf{ZF}^-_g$, and (vii) (and (ii) again), the operation

$$F(x_1,\dots,x_n,w)=\{G(x_1,\dots,x_n,w,t) : t\in w\}\cap w$$

is also T-absolute. Clearly

$$\begin{aligned} s\in F(x_1,\dots,x_n,w) \iff\ & s\in w \,\&\, R(x_1,\dots,x_n,s)\\ & \vee [s=w \,\&\, w\in w \,\&\, (\exists t)\neg R(x_1,\dots,x_n,t)]; \end{aligned}$$

and since $w\in V$ so $w\notin w$,

$$s\in F(x_1,\dots,x_n,w) \iff s\in w \,\&\, R(x_1,\dots,x_n,s)$$

as required. ⊣

Corollary 8B.4. *The notions #1 – #21 of Theorem 7C.2 are all* ZF^-_g*-absolute.*

Proof is routine using the theorem and we will skip it. ⊣

Before proceeding to show the ZF^-_g-absoluteness of several other notions, it will be instructive to notice that *many natural and useful notions are not even* ZFC*-absolute*, cf. Problem x8.2*. Roughly speaking, no notion related to *cardinality* is ZFC-absolute.

The next result is fundamental.

Theorem 8B.5 (Mostowski's Theorem)**.** *The condition*

$$\mathrm{WF}(r) \iff r \text{ is a wellfounded relation}$$

is ZF^-_g*-absolute.*

Proof. Put

$$P(r,x) \iff \text{Relation}(r)\ \&\ [x=\emptyset \vee (\exists t\in x)(\forall s\in x)\langle s,t\rangle \notin r].$$

Clearly P is ZF_g^--absolute and

$$\text{WF}(r) \iff (\forall x)P(r,x).$$

Similarly, let

$$\begin{aligned} Q(r,f) &\iff \text{Relation}(r)\,\&\,[f \text{ is a rank function for } r]\\ &\iff \text{Relation}(r)\ \&\ f:\text{Field}(r)\to \text{ON}\\ &\qquad \&\ (\forall x,y\in\text{Field}(r))[x<_r y \Longrightarrow f(x)\in f(y)]. \end{aligned}$$

Again Q is ZF_g^--absolute (using the fact that ON is definable by a Σ_0 formula) and

$$\text{WF}(r) \iff (\exists f)Q(r,f).$$

Hence

$$(*)\qquad (\forall r)\Big[(\forall x)P(x,r) \iff (\exists f)Q(r,f)\Big].$$

This equivalence is Problem x7.26, and it can be proved in ZF_g^-.

Let θ be the formal sentence which expresses $(*)$, so that $\mathsf{ZF}_g^-\vdash\theta$. Let $T^*\subseteq\mathsf{ZF}_g^-$ be the finite set of ZF_g^- axioms used in the proof of θ, so that θ is true in all models of T^*, including all the standard models. Let T^0, T^1 be finite subsets of ZF_g^- such that P and Q are absolute for standard models of T^0 and T^1 respectively. It follows that if M is a standard model of $T^0\cup T^1\cup T^*$, then for $r\in M$

$$(**)\qquad (\forall x\in M)P(x,r) \iff (\exists f\in M)Q(r,f).$$

Now part (vi) of 8B.3 implies that WF(r) is ZF_g^--absolute. ⊣

Mostowski's proof is simple but typically metamathematical and generally causes uneasiness to people who encounter it for the first time. The subtle part of it is that *we do not need to identify the specific instances of replacement needed to prove θ*—we only need to notice that there are only finitely many of them, and then put them in T^*. In this instance, we could probably pinpoint these instances, but that would be the wrong way to go about understanding the proof: because this sort of argument is used repeatedly, in ever more complex situations where chasing the specific instances of replacement used would be practically impossible. The argument rests on the fact that *proofs are finite*, so that for any formal τ-theory T and any τ-sentence ϕ,

$$T\vdash\phi \Longrightarrow (\exists \text{ finite } T_0\subseteq T)[T_0\vdash\phi].$$

The same kind of metamathematical argument is needed in the proof of the next result.

Theorem 8B.6 (Absoluteness of ordinal recursion)**.** *Suppose the operation $G : V^{n+1} \to V$ is ZF^-_g-absolute, and let*

$$F : \mathrm{ON} \times V^n \to V$$

be the unique operation satisfying

$$F(\xi, x_1, \dots, x_n) = G\big(\{\langle \eta, F(\eta, x_1, \dots, x_n)\rangle : \eta < \xi\}, x_1, \dots, x_n\big);$$

then F is also ZF^-_g-absolute.

Proof. Assume G is absolute for all standard models of $T^0 \subseteq \mathsf{ZF}^-_g$. Go back to the proof of Theorem 7C.16 to recall that F is defined by an expression of the form

$$F(\xi, x_1, \dots, x_n) = w \iff (\exists h)\{P(\xi, x_1, \dots, x_n, h) \,\&\, \mathrm{Function}(h) \\ \&\, \xi \in \mathrm{Domain}(h) \,\&\, h(\xi) = w\},$$

where P is easily absolute for all models of T^0. Moreover, we can prove

$$(\forall \xi, x_1, \dots, x_n)(\exists h) P(\xi, x_1, \dots, x_n, h)$$

using only finitely many additional instances of the Axiom Scheme of Replacement, say those in $T^1 \subseteq \mathsf{ZF}^-_g$. Thus for every standard model M of $T^0 \cup T^1$ and $\xi, x_1, \dots, x_n$ in M we have $(\exists h \in M) P(\xi, x_1, \dots, x_n, h)$, which implies immediately that M is closed under F.

We can also prove easily in ZF^-_g (using only some finite $T^2 \subseteq \mathsf{ZF}^-_g$) that

$$(\forall \xi, x_1, \dots, x_n, w)\big\{(\exists h)[P(\xi, x_1, \dots, x_n, h) \,\&\, \mathrm{Function}(h) \\ \&\, \xi \in \mathrm{Domain}(h) \,\&\, h(\xi) = w] \iff (\forall h)\big[[P(\xi, x_1, \dots, x_n, h) \\ \&\, \mathrm{Function}(h) \,\&\, \xi \in \mathrm{Domain}(h)] \Longrightarrow h(\xi = w\big]\big\};$$

thus by part (vi) of 8B.3, the condition

$$R(\xi, x_1, \dots, x_n, w) \iff F(\xi, x_1, \dots, x_n) = w$$

is ZF^-_g-absolute and so F is ZF^-_g-absolute. ⊣

A special case of definition by recursion on ON is simple recursion on ω.

Corollary 8B.7. *Suppose $F(k, x_1, \dots, x_n)$ satisfies the recursion*

$$F(0, x_1, \dots, x_n) = G(x_1, \dots, x_n) \\ F(k+1, x_1, \dots, x_n) = G\big(F(k, x_1, \dots, x_n), k, x_1, \dots, x_n\big)$$

where G_1 and G_2 are ZF^-_g-absolute. Then F is also ZF^-_g-absolute.

PROOF. Define

$$G(f,k,x_1,\dots,x_n) = \begin{cases} G_1(x_1,\dots,x_n) & \text{if } m=0,\\ G_2\big(f(k-1,x_1,\dots,x_n),k-1,x_1,\dots,x_n\big) & \\ & \text{if } k\in\omega,\ k\neq 0,\\ 0 & \text{otherwise}\end{cases}$$

and verify easily that G is ZF^-_g-absolute and F is definable from G as in the theorem. ⊣

Corollary 8B.8. *All the conditions and operations #1 – #40 in Theorems 7C.2 and 8A.1 are* ZF^-_g*-absolute.*

PROOF. Go back and reread the proofs of these theorems keeping in mind the results of this section. ⊣

8C. The basic facts about L

Let us start by collecting in one theorem the basic absoluteness facts about the constructible hierarchy that follow from the results of the preceding section.

Theorem 8C.1. (i) *The operation $\xi \mapsto L_\xi$ and the binary condition $x \in L_\xi$ are both* ZF^-_g*-absolute.*

(ii) *There is a canonical wellordering of L, $x \le_L y$ which is* ZF^-_g*-absolute and such that*

$$y \in L_\xi \,\&\, x \le_L y \Longrightarrow x \in L_\xi.$$

(iii) *The operation $(\xi, A) \mapsto L_\xi(A)$ and the ternary condition $x \in L_\xi(A)$ are both* ZF^-_g*-absolute.*

(iv) *The conditions $x \in L$ and $x \in L(A)$ are both absolute for inner models of some finite subset $T^0 \subseteq \mathsf{ZF}^-_g$.*

PROOF. (i) and (ii) follow immediately from the definitions, 8B.8, 8B.6 and of course, the basic closure properties of ZF^-_g-absoluteness listed in 8B.3. Part (ii) also follows easily by examining the proof of 8A.8.

To prove (iv), let $\varphi_L(\mathbf{x}, \boldsymbol{\xi})$ be a formula of $\mathbb{FOL}(\in)$ by (i) such that for some finite $T^0 \subseteq \mathsf{ZF}^-_g$ and any standard M

(207) $$x \in L_\xi \iff M \models \varphi_L[x,\xi] \quad (M \text{ standard}, M \models T^0),$$

and set $\psi_L(\mathbf{x}) :\equiv (\exists \boldsymbol{\xi})\varphi_L(\mathbf{x}, \boldsymbol{\xi})$. If M is an inner model of T^0 so that $M \models T^0$ and M contains all the ordinals, then for $x \in M$,

$$\begin{aligned} x \in L &\iff \text{for some } \xi,\ x \in L_\xi \\ &\iff \text{for some } \xi \in M,\ M \models \varphi_L[x,\xi] \\ &\iff M \models \psi_L[x]. \end{aligned}$$

The argument for $x \in L(A)$ is similar. ⊣

We are now in a position to prove (203), that L "believes" that every set is constructible.

Fix once and for all a formula $\varphi_L(\mathbf{x}, \boldsymbol{\xi})$ and a finite $T^0 \subset \mathsf{ZF}_g^-$ so that (207) holds and let "$V = L$" abbreviate the formal sentence of $\mathbb{FOL}(\in)$ which says that every set is constructible using this formula,

$$V = L :\equiv (\forall \mathbf{x})(\exists \boldsymbol{\xi})\varphi_L(\mathbf{x}, \boldsymbol{\xi}). \tag{208}$$

We also construct a similar formula $V = L(\mathbf{a})$ with a free variable $\mathbf{a}$ which says that "every set is constructible from $\mathbf{a}$".

Theorem 8C.2. (i) *$L \models V = L$.*

(ii) *For each grounded set A, $L(A), \mathbf{a} := A \models V = L(\mathbf{a})$.*

Proof. Compute:

$$\begin{aligned} L \models V = L &\iff L \models (\forall \mathbf{x})(\exists \boldsymbol{\xi})\varphi_L(\mathbf{x}, \boldsymbol{\xi}) \\ &\iff \text{for each } x \in L, \text{ there exists } \xi \in L,\ L \models \varphi_L(x, \xi) \\ &\iff \text{for each } x \in L, \text{ there exists } \xi \in L,\ x \in L_\xi, \end{aligned}$$

and the last assertion is true by the definition of L and the fact that it contains all the ordinals. ⊣

This is a very basic result about L. One of its applications is that it allows us to prove theorems about L without constant appeal to metamathematical results and methods: we simply assume $V = L$ in addition to the axioms of ZF_g^- and any consequence of these assumptions must hold in L.

We also put down for the record the result about the Axiom of Choice in L which we discussed in the beginning of Section 8B.

Theorem 8C.3. *There is a formula $\psi_L(\mathbf{x}, \mathbf{y})$ of $\mathbb{FOL}(\in)$ such that*

$$L \models \text{"}\{(x, y) : \psi_L(x, y)\} \text{ is a wellordering of } V\text{"}.$$

*In particular, $L \models$ **AC**.*

Proof. If ψ^* is the formal sentence of $\mathbb{FOL}(\in)$ expressing the symbolized English in quotes, then by 8A.8 and the fact that $L \models \mathsf{ZF}_g^-$,

$$L \models V = L \rightarrow \psi^*$$

while by 8C.2 we have $L \models V = L$. ⊣

For the Generalized Continuum Hypothesis we need another basic fact about L which is also proved by absoluteness arguments. Its proof requires two general facts, not particularly related to L, which could have been included in Chapter 7.

The first of these is the natural generalization of Theorem 2B.1 to uncountable structures.

Lemma 8C.4 (The Downward Skolem-Löwenheim Theorem)**.** *If the universe B of a structure $\mathbf{B}$ of countable signature τ is wellorderable and $X \subseteq B$, then there exists an elementary substructure $\mathbf{A} \preceq \mathbf{B}$ such that $X \subseteq A$ and $|A| = \max(\aleph_0, |X|)$.*

Proof. The assumption that B is wellorderable is needed to avoid appealing to the Axiom of Choice in the proof of Lemma 2B.5. Except for that, the required argument is a very minor modification of the proof of Theorem 2B.1. We enter it here in full, to avoid the need for extensive page-flipping.

Given $\mathbf{B}$ and $X \subseteq B$, fix some $y_0 \in B$, let

$$Y = X \cup \{y_0\} \cup \{c^{\mathbf{B}} \mid c \text{ a constant symbol}\},$$

so that Y is not empty (even if $X = \emptyset$ and there are no constants). Let $\mathcal{S}_\phi$ be a finite Skolem set for each formula ϕ, by Lemma 2B.5, and set

$$\mathcal{F} = \{f^{\mathbf{B}} \mid f \text{ is a function symbol in } \tau\} \cup \bigcup\nolimits_\phi \mathcal{S}_\phi.$$

The set $\mathcal{F}$ of Skolem functions is countable, since there are countably many formulas. We define the sequence $n \mapsto A_n$ by the recursion

$$A_0 = Y, \quad A_{n+1} = A_n \cup \bigcup \{f(y_1, \dots, y_k) : f \in \mathcal{F}, y_1, \dots, y_k \in A_n\}$$

and set $A = \bigcup_{n\in\omega} A_n$. This is the universe of some substructure $\mathbf{A} \subseteq \mathbf{B}$ by Lemma 2B.2. Moreover, for each ϕ, A is closed under a Skolem set for ϕ, and so (34) holds, which means that $\mathbf{A} \preceq \mathbf{B}$. Finally, to show that $|A| \le \max(\aleph_0, |X|)$, we check by induction on n that

$$|A_n| \le \max(\aleph_0, |X|) = \kappa, \tag{209}$$

which in the end gives $|A| \le \aleph_0 \cdot \kappa = \kappa$. The inequality (209) is trivial at the base,

$$|A_0| = |Y| \le |X| + 1 + \aleph_0 = \kappa,$$

and also in the inductive step: if k_f is the arity of each $f \in \mathcal{F}$, then

$$|A_{n+1}| \le |A_n| + |\bigcup\nolimits_{f\in\mathcal{F}} f[A_n^{k_f}]| \le \kappa + \sum\nolimits_{f\in\mathcal{F}} \kappa^{k_f} \le \kappa + \aleph_0 \cdot \kappa = \kappa. \qquad \dashv$$

The second lemma we need is a version of the *Mostowski collapsing* construction, which we have covered in three, different forms in Theorem 7C.14 and Problems x7.18*, x7.19*.

Lemma 8C.5 (Mostowski Isomorphism Theorem)**.** *Suppose M is a (grounded) set which* (as a structure with $\in$) *satisfies the Axiom of Extensionality, i.e.,*

$$u = v \iff (\forall t \in M)[t \in u \iff t \in v] \qquad (u, v \in M).$$

Let $d_M : M \to d_M[M]$ *be the Mostowski surjection of* $\in\restriction M$*, so that*

$$d_M(u) = \{d_M(v) : v \in M \cap u\} \qquad (u \in M). \tag{210}$$

Then $\overline{M} = d_M[M]$ *is a transitive set,* $d_M : M \rightarrowtail\!\!\!\!\twoheadrightarrow \overline{M}$ *is an* $\in$*-isomorphism of* $(M, \in)$ *with* $(\overline{M}, \in)$*, and if* $y \subseteq M$ *is transitive, then* $d_M(t) = t$ *for every* $t \in y$*.*

Proof. The unique function $d_M : M \to V$ satisfying (210) is defined by wellfounded recursion, and its image is a transitive set, directly from (210): because if $s \in d_M(u)$ for some $u \in M$, then

$$s = d_M(v) = \{d_M(t) : t \in M \cap v\}$$

for some $v \in M \cap u$ and so $s \subseteq d_M[M]$.

To prove that d_M is an injection, assume not and let u be an $\in$-minimal counterexample, so that for some $v \in M$, $v \neq u$,

$$d_M(u) = \{d_M(s) : s \in M \cap u\} = \{d_M(t) : t \in M \cap v\} = d_M(v).$$

It follows that if $s \in M \cap u$, then $d_M(s) = d_M(t)$ for some $t \in M \cap v$, so that by the choice of u, $s = t \in M \cap v$. Similarly, if $t \in M \cap v$, then $t \in M \cap u$. So $M \cap u = M \cap v$, and since M satisfies extensionality, $u = v$, which contradicts our assumption.

Finally, if d_M is not the identity on some transitive $y \subseteq M$, choose an $\in$-minimal $t \in y$ such that $d_M(t) \neq t$ and compute:

$$\begin{aligned} d_M(t) &= \{d_M(s) : s \in t\} && \text{(because } t \subseteq y \subseteq M) \\ &= \{s : s \in t\} && \text{(by the choice of } t) \\ &= t && \text{(because } t \subseteq y \subseteq M), \end{aligned}$$

which again contradicts our assumption. ⊣

In the context of the metamathematics of set theory (especially the study of L and other inner models), "the Mostowski Collapsing Lemma" most likely refers to this theorem. We used a different (standard but less common) name for it here, to avoid confusion. In any case, these two results (and Problems x7.18*, x7.19*) have different applications, but they are proved by the same method and they are all significant.

Theorem 8C.6 (The Condensation Lemma)**.** *There is a finite set of sentences* $T^0 \subset \mathsf{ZF}^-_g$ *such that with*

$$T^L = T^0 \cup \{V = L\}$$

the following hold.

(i) $L \models T^L$.

(ii) *If* A *is a transitive set and* $A \models T^L$*, then* $A = L_\lambda$ *for some limit ordinal* λ*.*

(iii) *For every infinite ordinal ξ and every set $x \in L$ such that $x \subseteq L_\xi$, there is some ordinal λ such that*

$$\xi \leq \lambda < \xi^+, \quad L_\lambda \models T^L, \text{ and } x \in L_\lambda.$$

Proof. Choose T^0 so that the operations $\xi \mapsto \xi + 1$, $\xi \mapsto L_\xi$, are absolute for the standard models of T^0 and the condition $x \in L_\xi$ is defined on all standard models of T^0 by the specific formula $\varphi_L(\mathbf{x}, \boldsymbol{\xi})$ which we used to construct the sentence $V = L$.

Clearly $L \models T^L$.

If A is a transitive set and $A \models T^L$, let

$$\lambda = \text{least ordinal not in } A$$

and notice that λ is a limit ordinal, since A is closed under the successor operation. Now

$$\xi < \lambda \Longrightarrow L_\xi \in A,$$

by the absoluteness of $\xi \mapsto L_\xi$, so

$$L_\lambda = \bigcup_{\xi<\lambda} L_\xi \subseteq A.$$

On the other hand, $A \models V = L$, so that

$$\text{for each } x \in A, \text{ there exists } \xi \in A,\ A \models \varphi_L[x, \xi]$$

i.e., (by the absoluteness of $\varphi_L(x, \xi)$), $A \subseteq L_\lambda$.

To prove (iii) suppose $x \subseteq L_\xi$ and $x \in L_\zeta$—where ζ may be a much larger ordinal than ξ. Using the Reflection Theorem 7D.7 on the hierarchy $\{L_\eta : \eta \in \mathrm{ON}\}$ and the fact that $L \models T^L$, choose $\mu > \max(\zeta, \xi)$ such that $L_\mu \models T^L$. Now $x \in L_\mu$ and $L_\mu \models T^L$.

By the Downward Skolem-Löwenheim Theorem 8C.4 applied to the (well-orderable) structure $(L_\mu, \in)$, we can find an elementary substructure

$$(M, \in) \preceq (L_\mu, \in)$$

such that $L_\xi \subseteq M$, $x \in M$ and $|M| = |L_\xi| = |\xi|$ by x8.6. Since $(M, \in)$ is elementarily equivalent with $(L_\mu, \in)$, it satisfies in particular the Extensionality Axiom, so by the Mostowski Isomorphism Theorem 8C.5, there is a transitive set $\overline{M}$ and an $\in$-isomorphism

$$d : M \rightarrowtail\!\!\!\!\rightarrow \overline{M}.$$

Moreover, since the transitive set $y = L_\xi \cup \{x\} \subseteq M$, d is the identity on y and hence $x = d(x) \in \overline{M}$. Now $(L_\mu, \in) \models T^L$ and therefore the elementarily equivalent structure $(M, \in) \models T^L$, so that the isomorphic structure $(\overline{M}, \in) \models T^L$; by (ii) then,

$$\overline{M} = L_\lambda$$

for some λ and of course, $\lambda < \xi^+$, since $|\overline{M}| = |\xi|$. $\dashv$

From this key theorem we get immediately the Generalized Continuum Hypothesis for L.

Corollary 8C.7 (ZF). *If $V = L$, then for each cardinal λ, $2^\lambda = \lambda^+$.*

Proof. By the theorem, if $V = L$, then $\mathcal{P}(\lambda) \subseteq L_{\lambda^+}$, and hence

$$|\mathcal{P}(\lambda)| \leq |L_{\lambda^+}| = \lambda^+. \qquad \dashv$$

We should point out that the models $L(A)$ need not satisfy either the Axiom of Choice or the Continuum Hypothesis. For example, if in V truly $2^{\aleph_0} > \aleph_1$, then there is some surjection

$$\pi : \mathcal{N} \twoheadrightarrow \aleph_2$$

and obviously

$$L\big(\{\langle \alpha, \pi(\alpha)\rangle : \alpha \in \mathcal{N}\}\big) \models 2^{\aleph_0} \geq \aleph_2.$$

As another application of the basic Theorem 8C.1, we obtain intrinsic characterizations of the models L, $L(A)$.

Theorem 8C.8. *L is the smallest inner model of ZF_g^- and for each (grounded) set A, $L(A)$ is the smallest inner model of ZF_g^- which contains A.*

Proof. Suppose M is an inner model of ZF_g^- and $A_0 \in M$. Since the operation

$$(\xi, A) \mapsto L_\xi(A)$$

is ZF_g^--absolute, M is closed under this operation; since $A_0 \in M$ and every ordinal $\xi \in M$, we have $(\forall \xi)[L_\xi(A_0) \in M]$ so that $L(A_0) \subseteq M$. $\dashv$

We also put down for the record the relative consistency consequences of of the theory of constructible sets:

Theorem 8C.9. *If ZF is consistent, then so is the theory $\mathsf{ZF}_g + V = L$, and a fortiori the weaker theories ZFC, $\mathsf{ZFC} + \mathbf{GCH}$.*

Proof. It is useful here to revert to the relativization notation of Definition 7D.6. The key observation is that for any $\mathbb{FOL}(\in)$ formula ϕ,

$$\text{if } \mathsf{ZF}_g + V = L \vdash \phi, \text{ then } \mathsf{ZF} \vdash (\phi)^L. \tag{211}$$

This is because $\mathsf{ZF} \vdash (\psi)^L$ for every axiom ψ of ZF_g by Theorem 8A.7; $\mathsf{ZF} \vdash (V = L)^L$ by Theorem 8C.2; and, pretty trivially,

$$\text{if } \psi_1, \dots, \psi_n \vdash \psi, \text{ then } (\psi_1)^M, \dots, (\psi_n)^M \vdash (\psi)^M,$$

for any definable class M, not just L. If $\mathsf{ZF} + V = L$ were inconsistent, then $\mathsf{ZF} + V = L \vdash \chi \ \& \ \neg\chi$ for some χ for some χ, and then $\mathsf{ZF} \vdash (\chi)^L \ \& \ \neg(\chi)^L$, so that ZF would also be inconsistent. $\dashv$

This is an example of a *finitistic relative consistency proof*: it can be formalized in a (very small) fragment of Peano arithmetic, but, more than that, it is generally recognized as a valid, constructive, combinatorial argument which assumes nothing about infinite objects beyond the usual properties of finite strings of symbols.

8D. $\Diamond$

Our (very limited) aim in this section is to introduce a basic principle of infinite combinatorics and prove that it holds in L. It was first formulated by Jensen to prove that L satisfies several propositions which are independent of ZFC, but we will not go into this here beyond a brief comment at the end: our main interest in $\Diamond$ is that its proof in L illustrates in a novel way many of the methods we have developed.

A *guessing sequence* (for ω_1) is any ω_1-sequence of functions on countable ordinals

$$s = \{s_\xi\}_{\xi \in \omega_1} \quad (s_\xi : \xi \to \xi). \tag{212}$$

Definition 8D.1. $\Diamond$: *There exists a guessing sequence $s = \{s_\xi\}_{\xi \in \omega_1}$ such that for every $f : \omega_1 \to \omega_1$, there is at least one $\xi > 0$ such that $f \restriction \xi = s_\xi$.*

The *diamond principle* seems weak, but the next Proposition shows that it has considerable strength. For the proof, we will need to appeal to some simple properties of *pairing functions* on ordinals which we will leave for Problem x8.12.

Proposition 8D.2 (ZFC). *If $\Diamond$ holds, then there is a guessing sequence $\{t_\xi\}_{\xi \in \omega_1}$ which guesses correctly $\aleph_1$-many restrictions of every $f : \omega_1 \to \omega_1$, i.e.,*

$$|\{\xi : f \restriction \xi = t_\xi\}| = \aleph_1 \quad (f : \omega_1 \to \omega_1).$$

Proof. Let $\{s_\xi\}_{\xi \in \omega_1}$ be a guessing sequence guaranteed by $\Diamond$, suppose $f : \omega_1 \to \omega_1$ is given, fix $\zeta < \omega_1$, and set

$$h_\zeta(\eta) = \langle f(\eta), \zeta \rangle \text{ so that } f(\eta) = (h_\zeta(\eta))_0.$$

Let $\xi(\zeta) > 0$ be such that

$$h_\zeta \restriction \xi(\zeta) = s_{\xi(\zeta)}.$$

This means that for every $\eta < \xi(\zeta)$, $f(\eta) = (s_{\xi(\zeta)})_0$; and it implies immediately that the sequence

$$t_\xi(\eta) = (s_\xi(\eta))_0 \le s_\xi(\eta) < \xi \quad (\xi < \omega_1, \eta < \xi)$$

guesses $f \restriction \xi(\zeta)$ correctly for every ζ. Moreover, these ordinals are all distinct, since

$$(s_{\xi(\zeta)}(0))_1 = \zeta,$$

so that we cannot have $\xi(\zeta_1) = \xi(\zeta_2) > 0$ when $\zeta_1 \neq \zeta_2$. ⊣

It is important in this proof, of course, to notice that the new guessing sequence $\{t_\xi\}_{\xi \in \omega_1}$ is defined directly from the one guaranteed by $\Diamond$, without reference to any specific f or ordinal ζ.

Corollary 8D.3 (ZFC). $\Diamond \Longrightarrow$ **CH**.

Proof. Fix a guessing sequence $\{t_\xi\}_{\xi \in \omega_1}$ which guesses correctly $\aleph_1$-many restrictions of every $f : \omega_1 \to \omega_1$, and for each $f : \omega \to \omega$ apply its characteristic property to the extension $\tilde{f} : \omega_1 \to \omega$ of f which is set $= 0$ for $\xi \geq \omega$. Let $\xi(f)$ be the least infinite ordinal such that $\tilde{f} \restriction \xi(f) = t_{\xi(f)}$; now $\xi(f)$ determines f uniquely, so that the map $f \mapsto \xi(f)$ is an injection of $(\omega \to \omega)$ into ω_1 and establishes the Continuum Hypothesis. ⊣

Theorem 8D.4 (ZFC). *If $V = L$, then $\Diamond$.*

Proof. We assume $V = L$ and define s_ξ by recursion on $\xi < \omega_1$, starting with (the irrelevant) $s_0 = \emptyset$. For $\xi > 0$, let

(213) $s_\xi =$ the $\leq_L$-least function $h : \xi \to \xi$ such that
for every $\zeta < \xi, \zeta \neq 0$, $h \restriction \zeta \neq s_\zeta$,

with the understanding that if no h with the required property exists, then s_ξ is the constant 0 on ξ. Recall that by our general convention about "indexed sequences",

$$\{s_\xi\}_{\xi \in \omega_1} = s : \omega_1 \to (\omega_1 \to \omega_1),$$

i.e., s is a function, and $s_\xi = s(\xi)$ for every $\xi \in \omega_1$.

To prove that for every $f : \omega_1 \to \omega_1$, this sequence s guesses correctly $f \restriction \xi$ for at least one $\xi > 0$, assume that it does not, and let

(214) $f =$ the $\leq_L$-least function $h : \omega_1 \to \omega_1$ such that
for every $\zeta < \omega_1, \zeta > 0$, $h \restriction \zeta \neq s_\zeta$.

Notice that by the Condensation Lemma, $s, f \in L_{\omega_2}$, cf. Problem x8.11.

A set $a \in L_{\omega_2}$ is definable (in L_{ω_2}) if there is a formula $\phi(\mathbf{x})$ such that

$$L_{\omega_2} \models (\exists! \mathbf{x})\phi(\mathbf{x}) \text{ and } L_{\omega_2} \models \phi[a].$$

We let

$$M = \{a \in L_{\omega_2} : a \text{ is definable in } L_{\omega_2}\}.$$

Lemma 1. $M \prec L_{\omega_2} \models \mathsf{ZF}^-_g$ *and* $\omega, \omega_1, s, f \in M$.

Proof. By Problem x8.10, $L_{\omega_2} \models \mathsf{ZF}^-_g$, and so all ZF^-_g-absolute notions are absolute for L_{ω_2}. In particular, the usual definitions of ω, ω_1 define these sets in L_{ω_2} and the formula which defines the canonical wellordering $\leq_L$ is also absolute for L_{ω_2}, and so we can interpret the definitions of s and f in L_{ω_2}; which means that $s, f \in M$.

To prove that $M \prec L_{\omega_2}$ by the basic test for elementary substructures Lemma 2B.3, it is enough to check that for every full extended formula $\phi(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y})$ and all $\vec{x} = x_1, \dots, x_n \in M$,

$$\text{if there exists some } y \in L_{\omega_2} \text{ such that } L_{\omega_2} \models \phi[\vec{x}, y],$$
$$\text{then there exists some } z \in M \text{ such that } L_{\omega_2} \models \phi[\vec{x}, z].$$

This is immediate setting

$$z = \text{the } \leq_L\text{-least } y \in L_{\omega_2} \text{ such that } L_{\omega_2} \models \phi[\vec{x}, y]. \quad \dashv \text{ (Lemma 1)}$$

Let $d : M \rightarrowtail\!\!\!\!\rightarrow L_\lambda$ be the Mostowski isomorphism for M, so $\lambda < \omega_1$ and

$$d : M \rightarrowtail\!\!\!\!\rightarrow L_\lambda \models \mathsf{ZF}^-_g,\ (\forall y)[\mathrm{TC}(y) \subset M \Longrightarrow d(y) = y].$$

Lemma 2. If $F : L^n \to L$ is a ZF^-_g-absolute operation, then

$$x_1, \dots, x_n \in M$$
$$\Longrightarrow F(x_1, \dots, x_n) \in M \ \&\ d(F(x_1, \dots, x_n)) = F(d(x_1), \dots, d(x_n)).$$

Proof. Suppose $\phi(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y})$ defines F on every transitive model of ZF^-_g. In particular, $L_{\omega_2} \models (\forall \vec{\mathbf{x}})(\exists! \mathbf{y})\phi(\vec{\mathbf{x}}, \mathbf{y})$, and so $M \models (\forall \vec{\mathbf{x}})(\exists! \mathbf{y})\phi(\vec{\mathbf{x}}, \mathbf{y})$ which means that M is closed under F. Moreover, for $x_1, \dots, x_n, y \in M$,

$$M \models \phi[x_1, \dots, x_n, y] \iff L_\lambda \models \phi[d(x_1), \dots, d(x_n), d(y)]$$
$$\iff F(d(x_1), \dots, d(x_n)) = d(y),$$

the last because $L_\lambda \models \mathsf{ZF}^-_g$ and so $\phi(\vec{\mathbf{x}}, \mathbf{y})$ also defines F on it. $\dashv$ (Lemma 2)

Lemma 2 implies in particular that if $g \in M$, then $\mathrm{Domain}(g) \in M$ and for every $a \in \mathrm{Domain}(g) \cap M$,

$$d(g(a)) \in M \text{ and } d(g(a)) = d(g)(d(a)), \tag{215}$$

simply because the operations

$$g \mapsto \mathrm{Domain}(g), \quad (g, a) \mapsto g(a)$$

are ZF^-_g-absolute. In particular, if $\xi < \omega_1$, then

$$\xi \in M \Longrightarrow f(\xi), s_\xi \in M, \text{ and } [\eta, \xi \in M \ \&\ \eta < \xi] \Longrightarrow s_\xi(\eta) \in M.$$

Lemma 3. If ξ is countable and $\xi \in M$, then $d(\xi) = \xi$.

PROOF. We can prove in ZF^-_g that *every countable ordinal* ξ *is the image of some* $g : \omega \twoheadrightarrow \xi$, and so if ξ is definable in L_{ω_2}, then so is

$$g = \text{the } \leq_L\text{-least } g : \omega \twoheadrightarrow \xi.$$

It follows that every $\eta < \xi$ is $g(n)$ for some $n \in \omega$ and hence definable in L_{ω_2}; and then $\xi + 1 = \mathrm{TC}(\xi) \subset M$, and so the Mostowski isomorphism d is the identity on $\xi + 1$ and gives $d(\xi) = \xi$. ⊣ (Lemma 3)

Lemma 4. If $\mu = d(\omega_1)$, *then* $d(f) = f \restriction \mu$ *and for* $\xi < \mu$, $d(s_\xi) = s_\xi$.

PROOF. The key observation is that

$$\xi < \mu \iff [\xi \in M \ \& \ \xi < \omega_1].$$

This is because using Lemma 3,

$$\xi \in M \ \& \ \xi < \omega_1 \Longrightarrow \xi = d(\xi) \ \& \ d(\xi) < d(\omega_1) = \mu,$$

and on the other hand,

$$\begin{aligned} \xi < \mu &\Longrightarrow (\exists \eta)[\eta \in M \ \& \ \eta < \omega_1 \ \& \ \xi = d(\eta)] \\ &\Longrightarrow (\exists \eta)[\eta \in M \ \& \ \eta < \omega_1 \ \& \ \xi = \eta] \Longrightarrow \xi \in M \ \& \ \xi < \omega_1. \end{aligned}$$

In particular, $\xi < \mu \Longrightarrow d(\xi) = \xi$, and since $f \in M$ and $f(\xi) < \omega_1$, by (215),

$$\xi < \mu \Longrightarrow f(\xi) = d(f(\xi)) = d(f)(d(\xi)) = d(f)(\xi),$$

i.e., $d(f) = f \restriction \mu$. Similarly,

$$\eta < \xi < \mu \Longrightarrow s_\xi(\eta) = d(s_\xi(\eta)) = d(s_\xi)(\eta),$$

and so for $\xi < \mu$, $d(s_\xi) = s_\xi$. ⊣ (Lemma 4)

We now consider the definition (213) of s_μ: it is the unique $g : \mu \to \mu$ which satisfies the condition

$$\phi[g, \mu] \equiv g \text{ is the } \leq_L\text{-least } h : \mu \to \mu \text{ such that} \\ \text{for every } \zeta < \mu, \zeta > 0, h \restriction \mu \neq s_\zeta.$$

Since the formula $\phi(\mathbf{x}, \mathbf{y})$ is ZF^-_g-absolute and $s_\mu \in L_{\omega_2}$, this implies that

$$s_\mu \text{ is the unique } g \text{ such that } L_{\omega_2} \models \phi[g, \mu].$$

By the definition (214) of f and the same reasoning,

$$f \text{ is the unique } h \text{ such that } L_{\omega_2} \models \phi[h, \aleph_1];$$

and so $M \models \phi[f, \aleph_1]$, hence $L_\lambda \models \phi[d(f), \mu]$. We now appeal again to the fact that $\phi(\mathbf{x}, \mathbf{y})$ is ZF^-_g-absolute: since $L_\lambda \models \mathsf{ZF}^-_g$, $N \models \phi[d(f), \mu]$ for every transitive $N \models \mathsf{ZF}^-_g$ which contains $d(f)$ and μ, and in particular,

$$L_{\omega_2} \models \phi[d(f), \mu].$$

So $s_\mu = d(f)$ and $d(f) = f \restriction \mu$ by Lemma 4, which contradicts the choice of f. ⊣

How large can we make the set of correct guesses

$$\{\xi > 0 : f \upharpoonright \xi = t_\xi\}$$

for every $f : \omega_1 \to \omega_1$ by choosing cleverly the guessing sequence $\{t_\xi\}_{\xi\in\omega_1}$? We cannot (rather trivially) insure that this set is always a closed unbounded subset of ω_1, cf. Problem x8.13, but we can insure the next, best possible result.

A set $C \subseteq \omega_1$ is *stationary* if it intersects every closed, unbounded subset of ω_1.

Theorem 8D.5 (ZFC). *If $\Diamond$ holds, then there is a guessing sequence $\{t_\xi\}_{\xi\in\omega_1}$ such that for every $f : \omega_1 \to \omega_1$ the set $\{\xi > 0 : f \upharpoonright \xi = t_\xi\}$ is stationary.*

Proof is left for Problem x8.15*. $\dashv$

This is about the strongest version of $\Diamond$ which is close to the formulation we chose as "primary", but there are many other equivalent propositions, each with its own uses and applications.

The Suslin Hypothesis. The order $(\mathbb{R}, \leq)$ on the real numbers can be characterized up to similarity by the following two properties which do not refer to the field structure of $\mathbb{R}$:

(1) $(X, \leq)$ is a linear ordering with no least or greatest element; it is *dense in itself*, i.e., $a < b \Longrightarrow (\exists x)[a < x < b]$; and it is *order complete*, i.e., every set $X \subseteq (a, b)$ contained in an open interval has a least upper bound and a greatest lower bound.

(2) $(X, \leq)$ is *separable*, i.e., there is a countable set $\mathbb{Q} \subset X$ which intersects every open interval (a, b).

Suslin's question was whether (2) can be replaced by the weaker

(2′) There is no uncountable set of disjoint open intervals in X.

Call $(X, \leq)$ a *Suslin line* if it satisfies (1) and (2′) but not (2).

Suslin Hypothesis. There is no Suslin line.

The Suslin Hypothesis is neither provable nor disprovable in ZFC. Both of these results were established by forcing techniques soon after Cohen's introduction of the method in 1963, and they were among the most important early results in forcing—especially the consistency of Suslin's Hypothesis. Soon afterwards Jensen proved that *there is a Suslin line in L*. His proof is combinatorial complex (and uses the intermediate notion of a *Suslin tree*) but the main tool for it was the proof of $\Diamond$ in L. It is fair to say that Jensen's theorem was the first, substantial result which started the modern development of *combinatorial set theory*, in and outside L.

8E. L and Σ^1_2

We finish this Chapter with some basic results of Shoenfield which relate the constructible universe to the analytical hierarchy developed in Sections 5H and 5I. We will assume for simplicity ZFC as the underlying theory, although most of what we will prove can be established without the full versions of either the powerset axiom or the axiom of choice.

Theorem 8E.1. (i) *The set $\mathcal{N} \cap L$ of constructible members of Baire space is Σ^1_2.*

(ii) *The restriction of $\le_L$ to $\mathcal{N}$ is a Σ^1_2-good wellordering of $\mathcal{N} \cap L$; i.e., it is a Σ^1_2 relation on $\mathcal{N}$, and if $P \subseteq \omega^n \times \mathcal{N}^\nu$ is in Σ^1_2, then so are the relations*

$$Q(\alpha, \vec{x}, \vec{\beta}) \iff \alpha \in L \;\&\; (\exists \beta \le_L \alpha) P(\beta, \vec{x}, \vec{\beta}),$$
$$R(\alpha, \vec{x}, \vec{\beta}) \iff \alpha \in L \,\&\, (\forall \beta \le_L \alpha) P(\beta, \vec{x}, \vec{\beta}).$$

(iii) *If $\mathcal{N} \subseteq L$, then $\mathcal{N}$ admits a Σ^1_2-good wellordering of rank $\aleph_1$.*

Proof. (i) is an easy consequence of (ii), but it is instructive to show (i) first.

First of all, we claim that if T^L is the finite set of sentences in the Condensation Lemma 8C.6, then

(216) $\alpha \in L \iff$ there exists a countable, transitive set A such that $(A, \in) \models T^L$ and $\alpha \in A$.

The implication ($\Longleftarrow$) in (216) is immediate, because by Theorem 8C.6, if $(A, \in) \models T^L$, then $A = L_\lambda$ for some ordinal λ. For the other direction, notice that (as a set of pairs of natural numbers), each α is a subset of L_ω so by (iii) of 8C.6

$$\alpha \in L \iff \text{for some countable } \lambda,\ \alpha \in L_\lambda \text{ and } L_\lambda \models T^L.$$

The key idea of the proof is that the structures of the form $(A, \in)$ with countable transitive A can be characterized *up to isomorphism* by the version for sets of the Mostowski Collapsing Lemma in Problem x7.18*. In fact, if (M, E) is any structure with countable M and $E \subseteq M \times M$, then by x7.18*, immediately

$$(M, E) \text{ is isomorphic with some } (A, \in) \text{ where } A \text{ is countable, transitive}$$
$$\iff E \text{ is wellfounded and } (M, E) \models \text{“axiom of extensionality”};$$

thus

(217) $\alpha \in L \iff$ there exists a countable, wellfounded structure (M, E) such that $(M, E) \models$ "axiom of extensionality", $(M, E) \models T^L$ and $\alpha \in \overline{M} =$ the unique transitive set such that (M, E) is isomorphic with $(\overline{M}, \in)$.

To see how to express the last condition in a model-theoretic way, recall that the condition "$\alpha \in \mathcal{N}$" is ZF^-_g-absolute and choose some $\varphi_0(\boldsymbol{\alpha})$ such that for all transitive models M of some finite $T_0 \subseteq \mathsf{ZF}^-_g$,

$$\alpha \in \mathcal{N} \iff M \models \varphi_0[\alpha].$$

Next define for each integer n a formula $\psi_n(\mathbf{x})$ which asserts that $\mathbf{x} = n$, by the recursion

$$\psi_0(\mathbf{x}) \iff \mathbf{x} = 0,$$
$$\psi_{n+1}(\mathbf{x}) \iff (\exists \mathbf{y})[\psi_n(\mathbf{y}) \,\&\, \mathbf{x} = \mathbf{y} \cup \{\mathbf{y}\}]$$

and for each n, m, let

$$\psi_{n,m}(\boldsymbol{\alpha}) :\equiv (\exists \mathbf{x})(\exists \mathbf{y})[\psi_n(\mathbf{x}) \,\&\, \psi_m(\mathbf{y}) \,\&\, \boldsymbol{\langle} \mathbf{x}, \mathbf{y} \boldsymbol{\rangle} \in \boldsymbol{\alpha}].$$

It follows that

(218) $\alpha \in L \iff$ there exists a countable, wellfounded structure (M, E) such that $(M, E) \models$ "axiom of extensionality", $(M, E) \models T^L$ and for some $a \in M$, $(M, E) \models \varphi_0[a]$ and for all n, m, $\alpha(n) = m \iff (M, E) \models \psi_{n,m}[a]$.

Let

$$f(m, n) = \text{the code of the formula } \psi_{m,n}(\boldsymbol{\alpha}),$$

so that f is obviously a recursive function. Let also k_0 be the code of the conjunction of the sentences in T^L and the Axiom of Extensionality and let k_1 be the code of the formula $\varphi_0(\boldsymbol{\alpha})$ which defines $\alpha \in \mathcal{N}$; we are assuming that both in $\psi_{m,n}(\boldsymbol{\alpha})$ and in $\varphi_0(\boldsymbol{\alpha})$, the free variable $\boldsymbol{\alpha}$ is actually the first variable $\mathbf{v}_0$. It is now clear that with $u = \langle 2 \rangle$ the code of the vocabulary for structures with just one binary relation,

$$\begin{aligned}
\alpha \in L \iff (\exists \beta)\Big\{&\mathrm{Sat}(u, \beta, k_0, 1) \\
&\& \{(t, s) : (\beta)_0(t) = (\beta)_0(s) = 1 \,\&\, (\beta)_1(\langle t, s \rangle) = 1\} \\
&\qquad \text{is wellfounded} \\
&\& (\exists a)\Big[\mathrm{Sat}(u, \beta, k_1, \langle a \rangle) \\
&\qquad \& (\forall n)(\forall m)\big[\alpha(n) = m \iff \mathrm{Sat}\big(u, \beta, f(n, m), \langle \alpha \rangle\big)\big]\Big]\Big\}
\end{aligned}$$

which implies directly that $L \cap \mathcal{N}$ is Σ^1_2, using the fact that wellfoundedness is Π^1_1.

To prove (ii), let $\psi_L(\mathbf{v}_0, \mathbf{v}_1)$ be a formula which defines the canonical wellordering of L absolutely on all transitive models of some finite $T^L_1 \subseteq \mathsf{ZF}^-_g$ (by (ii) of 8C.1) and let $S^L \subseteq \mathsf{ZF}^-_g$ be finite and large enough to include T^L_1, T^L, the Axiom of Extensionality and the set T_0 of part (i), chosen so that $\varphi_0(\boldsymbol{\alpha})$ defines $\boldsymbol{\alpha} \in \mathcal{N}$ on all transitive models of T_0. Using the key fact

$$\alpha \in L_\xi \,\&\, \beta \leq_L \alpha \Longrightarrow \alpha \in L_\xi$$

and Mostowski collapsing as above, we can verify directly that for $\alpha \in L$ and arbitrary $P \subseteq \mathcal{N} \times \mathcal{Z}$ (with $\mathcal{Z} = \omega^n \times \mathcal{N}^\nu$),

$$\begin{aligned}
&(\forall \beta \leq_L \alpha) P(\beta, z)\\
&\quad\Longleftrightarrow \text{ there exists a countable, wellfounded structure}\\
&\qquad\quad (M, E) \models S^L \text{ and some } a \in M \text{ such that } (M, E) \models \varphi_0[a]\\
&\qquad\quad \text{and } (\forall n)(\forall m)[\alpha(n) = m \iff (M, E) \models \psi_{n,m}[a]]\\
&\qquad\quad \text{and } (\forall b)\big\{(M, E) \models \varphi_0[b] \,\&\, \psi_L(b, a) \Longrightarrow\\
&\qquad\qquad\quad (\exists \beta)\big[(\forall n)(\forall m)[\beta(n) = m\\
&\qquad\qquad\qquad\qquad \iff (M, E) \models \psi_{n,m}[b]] \,\&\, P(\beta, z)\big]\big\}.
\end{aligned}$$

If P is Σ^1_2, then it is easy to see that this whole expression on the right leads to a Σ^1_2 condition by coding the structures (M, E) by irrationals as above—the key being that the universal quantifier $\forall \beta$ has been turned to the number quantifier $\forall b$. ⊣

We put down the argument for (i) in considerable detail, because it illustrates a very useful technique for making analytical computations of conditions defined by set-theoretic constructions. For the next result we will do the opposite, i.e., we will give a set-theoretic construction for Σ^1_2 subsets of $\omega^n \times \mathcal{N}^\nu$ which will establish that (as conditions) they are absolute for L.

We show first a basic result, which has many applications beyond our immediate concern:

Theorem 8E.2 (Shoenfield's Lemma). *If $A \subseteq \mathcal{N}$ is Σ^1_2, then there exists a ZF^-_g-absolute operation*

$$\xi \mapsto T^\xi$$

which assigns to each ordinal $\xi \geq \omega$ a tree T^ξ on $\omega \times \xi$ such that the following holds, when λ is any uncountable ordinal:

$$\begin{aligned}
\alpha \in A &\iff (\exists \xi \geq \omega)[T^\xi(a) \text{ is not wellfounded}]\\
&\iff (\exists \xi \geq \omega)[\xi < \omega_1 \,\&\, T^\xi(\alpha) \text{ is not wellfounded}]\\
&\iff T^\lambda(\alpha) \text{ is not wellfounded.}
\end{aligned}$$

PROOF. Choose a recursive, monotone R so that

$$\alpha \in A \iff (\exists\beta)(\forall\gamma)(\exists t)R\big(\overline{\alpha}(t), \overline{\beta}(t), \overline{\gamma}(t)\big),$$

and for all $\overline{\alpha}(n), \overline{\beta}(n), \overline{\gamma}(n)$,

$$\Big(\neg R(\overline{\alpha}(t), \overline{\beta}(t), \overline{\gamma}(t)) \ \&\ s < t\Big) \Longrightarrow \neg R(\overline{\alpha}(s), \overline{\beta}(s), \overline{\gamma}(s)).$$

It follows that for each α, β, the set of sequences

$$S^{\alpha,\beta} = \big\{(c_0, \dots, c_{s-1}) : (\forall t < s)\neg R\big(\overline{\alpha}(t), \overline{\beta}(t), \langle c_0, \dots, c_{t-1}\rangle\big)\big\}$$

is a tree and easily

$$\begin{aligned}(1)\quad \alpha \in A &\iff (\exists\beta)\{S^{\alpha,\beta} \text{ is wellfounded}\}\\ &\iff (\exists\beta)(\exists f : S^{\alpha,\beta} \to \omega_1)\{\text{if } (c_0, \dots, c_{s-1}) \in S^{\alpha,\beta} \text{ and } t < s,\\ &\qquad\qquad \text{then } f(c_0, \dots, c_{t-1}) > f(c_0, \dots, c_{s-1})\}.\end{aligned}$$

In the computation below we will represent $S^{\alpha,\beta}$ by the set of codes in ω $\langle c_0, \dots, c_{s-1}\rangle$ of sequences $(c_0, \dots, c_{s-1}) \in S^{\alpha,\beta}$.

For each $\xi \geq \omega$, define first a tree S^ξ on $\omega \times \omega \times \xi$ as follows:

$$\begin{aligned}&\big((a_0, b_0, \xi_0), \dots, (a_{n-1}, b_{n-1}, \xi_{n-1})\big) \in S^\xi \iff \xi_0, \dots, \xi_{n-1} < \xi\\ &\& \ (\forall c_0, \dots, c_t, s < t)\Big[\neg R(\langle a_0, \dots, a_{t-1}\rangle, \langle b_0, \dots, b_{t-1}\rangle, \langle c_0, \dots, c_{t-1}\rangle)\Big]\\ &\qquad\qquad \Longrightarrow \xi_{\langle c_0, \dots, c_{s-1}\rangle} > \xi_{\langle c_0, \dots, c_{t-1}\rangle}.\end{aligned}$$

Notice that the operation

$$\xi \mapsto S^\xi$$

is clearly ZF^-_g-absolute and

$$\xi \leq \eta \Longrightarrow S^\xi \subseteq S^\eta.$$

Now set for any ξ, α,

$$S^\xi(\alpha) = \Big\{\big((b_0, \xi_0), \dots, (b_{n-1}, \xi_{n-1})\big) : \Big(\big(\alpha(0), b_0, \xi_0\big), \dots, \big(\alpha(n-1), b_{n-1}, \xi_{n-1}\big)\Big) \in S^\xi\Big\}.$$

This is a tree on $\omega \times \xi$, the *tree of all attempts to prove that for some β, $S^{\alpha,\beta}$ is wellfounded with rank $\leq \xi$*: any infinite branch in $S^\xi(\alpha)$ provides a β and a rank function $f : S^{\alpha,\beta} \to \xi$. More precisely, we have the following two, simple facts:

$$(2)\qquad \alpha \in A \Longrightarrow (\exists\xi \in \omega_1)[S^\xi(\alpha) \text{ is not wellfoounded}],$$

$$(3)\qquad S^\xi(\alpha) \text{ is not wellfounded} \Longrightarrow \alpha \in A \quad (\xi \text{ infinite}).$$

To prove (2) choose $\beta = (b_0, b_1, \dots)$ such that $S^{\alpha,\beta}$ is wellfounded, choose $f : S^{\alpha,\beta} \to \omega_1$ as in (1), set $\xi_i = f(c_0, \dots, c_{s-1})$ if $i = \langle c_0, \dots, c_{s-1}\rangle$ for some $c_0, \ldots, c_{s-1}$ and $\xi_i = 0$ otherwise. To prove (3), choose an infinite branch $(b_0, \xi_0), (b_1, \xi_1), \ldots$ in $S^\xi(\alpha)$, take $\beta = (b_0, b_1, \ldots)$ and define $f : S^{\alpha,\beta} \to \xi$ by

$$f(c_0, \ldots, c_{s-1}) = \xi_i \iff i = \langle c_0, \ldots, c_{s-1} \rangle$$

so that it satisfies the defining condition in (1).

Now (2) and (3) imply directly the assertions in the theorem taking $T^\xi = S^\xi$, except that S^ξ is a tree on $\omega \times (\omega \times \xi)$ rather than a tree on $\omega \times \xi$. To complete the proof, put

$$\begin{aligned} T^\xi = {} & \text{all initial segments of sequences of the form} \\ & \big((a_0, b_0), (a_1, \xi_0), (a_2, b_1), (a_3, \xi_1), \ldots, (a_{2n}, b_n), (a_{2n+1}, \xi_n)\big) \\ & \text{such that} \\ & \big((a_0, b_0, \xi_0), (a_1, b_1, \xi_1), \ldots, (a_n, b_n, \xi_n)\big) \in S^\xi \end{aligned}$$

so that T^ξ is a tree on $\omega \times \xi$ (because $\omega \subseteq \xi$) and easily, for any α,

$$T^\xi(\alpha) \text{ is not wellfounded} \iff S^\xi(\alpha) \text{ is not wellfounded.} \qquad \dashv$$

Theorem 8E.3 (Shoenfield's Theorem (I))**.** *Each Σ^1_2 set $A \subseteq \mathcal{N}$ is absolute as a condition for all standard models M of some finite $T_* \subseteq \mathsf{ZF}^-_g$ such that $\omega_1 \subseteq M$.*

In particular, every Σ^1_2 subset $A \subseteq \omega^n$ is constructible.

Proof. Suppose $A \subseteq \mathcal{N}$ is Σ^1_2 and by Shoenfield's Lemma, let $\varphi(\boldsymbol{\xi}, \mathbf{T})$ be a formula of $\mathbb{FOL}(\in)$ such that for all standard models M of some finite $T_1 \subseteq \mathsf{ZF}^-_g$,

$$\begin{aligned} \xi \in M &\Longrightarrow T^\xi \in M, \\ T = T^\xi &\iff M \models \varphi[\xi, T]. \end{aligned}$$

Notice also that the operation

$$(\alpha, T) \mapsto T(\alpha)$$

is easily ZF^-_g-absolute, so choose $\psi(\boldsymbol{\alpha}, \mathbf{S}, \mathbf{T})$ so that for all standard models M of some finite $T_2 \subseteq \mathsf{ZF}^-_g$,

$$\begin{aligned} \alpha, T \in M &\Longrightarrow T(\alpha) \in M, \\ S = T(\alpha) &\iff M \models \psi[\alpha, S, T]. \end{aligned}$$

Finally use Mostowski's Theorem 8B.5 to construct a formula $\chi(\mathbf{S})$ of $\mathbb{FOL}(\in)$ such that for all standard models M of some finite $T_3 \subseteq \mathsf{ZF}^-_g$ and $S \in M$,

$$S \text{ is wellfounded} \iff M \models \chi[S].$$

Now if M is any standard model of

$$T_* = T_1 \cup T_2 \cup T_3$$

such that $\omega_1 \subseteq M$, then by the lemma, for $\alpha \in M$

$$\begin{aligned}
\alpha \in A &\iff \text{there exists some } \xi \in M \text{ such that } T^\xi(\alpha) \text{ is not wellfounded}\\
&\iff \text{there exists some } \xi \in M \text{ such that}\\
&\qquad M \models (\exists \mathbf{S})(\exists \mathbf{T})[\varphi(\xi, \mathbf{T}) \,\&\, \psi(\alpha, \mathbf{S}, \mathbf{T}) \,\&\, \neg\chi(\mathbf{S})]\\
&\iff M \models (\exists \boldsymbol{\xi})(\exists \mathbf{S})(\exists \mathbf{T})[\varphi(\boldsymbol{\xi}, \mathbf{T}) \,\&\, \psi(\alpha, \mathbf{S}, \mathbf{T}) \,\&\, \neg\chi(\mathbf{S})].
\end{aligned}$$

To prove the second assertion, take $A \subseteq \omega$ for simplicity of notation, suppose

$$n \in A \iff P(n)$$

where P is Σ^1_2, and let $\psi(\mathbf{n})$ define P absolutely as in the first part, so that in particular

$$P(n) \iff L \models \psi[n].$$

The sentence

$$(\exists \mathbf{x})\big[\mathbf{x} \subseteq \omega \,\&\, (\forall \mathbf{n})[\mathbf{n} \in \mathbf{x} \iff \psi(\mathbf{n})]\big]$$

is a theorem of ZF^-_g and hence it holds in L. This implies that there is some $x \in L$ such that $x \subseteq \omega$ and for all n,

$$\begin{aligned}
n \in x &\iff L \models \psi[n]\\
&\iff P(n)\\
&\iff n \in A;
\end{aligned}$$

thus $x = A$ and $A \in L$. ⊣

To appreciate the significance of Shoenfield's Theorem, recall from the exercises of **??** that a formula $\theta(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m)$ of the language of second order arithmetic A^2 is Σ^1_n if

$$\theta(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m) \iff (\exists \boldsymbol{\beta}_1)(\forall \boldsymbol{\beta}_2)(\exists \boldsymbol{\beta}_3) \cdots (-\boldsymbol{\beta}_n)\varphi(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m, \boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_n),$$

where $\varphi(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m, \boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_n)$ has no quantifiers over $\mathcal{N}$. It is clear that we can interpret these formulas over standard models of ZF^-_g simply by putting (for $\alpha_1, \dots, \alpha_m \in M$),

$$M \models \theta(\alpha_1, \dots, \alpha_m) \iff (\omega, \mathcal{N} \cap M, +, \cdot, \mathrm{ap}, 0, 1) \models \theta(\alpha_1, \dots, \alpha_m),$$

i.e., by interpreting the quantifiers $\exists \boldsymbol{\beta}_i$, $\forall \boldsymbol{\beta}_i$ as ranging over the irrationals in M and using the standard interpretations for the operations $+$, $\cdot$, ap (which are ZF^-_g-absolute by **??**) and the quantifiers $\exists n$, $\forall n$ (since ω is also ZF^-_g-absolute and hence a member of M).

Theorem 8E.4 (Shoenfield's Theorem (II))**.** *[**??**] (i) If $\theta(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m)$ is a Σ^1_2 or Π^1_2 formula of second order arithmetic, then for every standard model M of ZF^-_g such that $\omega_1 \subseteq M$ and $\alpha_1, \dots, \alpha_m \in M$,*

$$V \models \theta(\alpha_1, \dots, \alpha_m) \iff M \models \theta(\alpha_1, \dots, \alpha_m);$$

in particular, if $\alpha_1, \ldots, \alpha_m \in L$*, then*

$$V \models \theta(\alpha_1, \ldots, \alpha_m) \iff L \models \theta(\alpha_1, \ldots, \alpha_m).$$

(ii) If we can prove a Σ^1_2 *or* Π^1_2 *sentence* θ *by assuming in addition to the axioms in* ZF^-_g *the hypothesis* $V = L$ *(and its consequences* **AC** *and* **GCH***), then* θ *is in fact true (i.e.,* $V \models \theta$*).*

Proof. Take a Σ^1_2 sentence for simplicity of notation

$$\theta \iff (\exists \boldsymbol{\alpha})(\forall \boldsymbol{\beta})\varphi(\boldsymbol{\alpha}, \boldsymbol{\beta}),$$

and let

$$P(\alpha, \beta) \iff \mathsf{A}^2 \models \varphi(\alpha, \beta)$$

be the arithmetical pointset defined by the matrix of θ so that

$$\begin{aligned} V \models \theta &\iff (\exists \alpha)(\forall \beta)P(\alpha, \beta) \\ M \models \theta &\iff (\exists \alpha \in M)(\forall \beta \in M)P(\alpha, \beta). \end{aligned}$$

Using the Basis Theorem for Σ^1_2, **??**,

$$\begin{aligned} V \models \theta &\Longrightarrow (\exists \alpha)(\forall \beta)P(\alpha, \beta) \\ &\Longrightarrow (\exists \alpha \in \Delta^1_2)(\forall \beta)P(\alpha, \beta) && \text{(by \textbf{??})} \\ &\Longrightarrow (\exists \alpha \in M)(\forall \beta)P(\alpha, \beta) && \text{(by 8E.3)} \\ &\Longrightarrow (\exists \alpha \in M)(\forall \beta \in M)P(\alpha, \beta) && \text{(obviously)} \\ &\Longrightarrow M \models \theta. \end{aligned}$$

Conversely, assuming that $M \models \theta$, choose some $\alpha_0 \in M$ such that

$$(\forall \beta \in M)P(\alpha_0, \beta)$$

and assume towards a contradiction that

$$(\exists \beta)\neg P(\alpha_0, \beta);$$

by the Basis Theorem **??** again, we then have

$$\big(\exists \beta \in \Delta^1_2(\alpha_0)\big)\neg P(\alpha_0, \beta)$$

so that by 8E.3,

$$(\exists \beta \in M)\neg P(\alpha_0, \beta)$$

contradicting our assumption end establishing $(\forall \beta)P(\alpha_0, \beta)$, i.e., $V \models \theta$.

The second assertion follows immediately because if we can prove θ using the additional hypothesis $V = L$, then we know that $L \models \theta$ by 8C.2 and hence $V \models \theta$ by the first assertion. $\dashv$

This theorem is quite startling because so many of the propositions that we consider in ordinary mathematics are expressible by Σ^1_2 sentences—including all propositions of elementary or analytic number theory and most of the propositions of "hard analysis". The techniques in the proof of 8C.1 allow us to prove that many set theoretic propositions are also equivalent to Σ^1_2 sentences. Theorem 8E.2 assures us then that the truth or falsity of these "basic" propositions does not depend on the answers to difficult and delicate questions about the nature of sets like the continuum hypothesis; we might as well assume that $V = L$ in attempting to prove or disprove them.

Of course, in descriptive set theory we worry about propositions much more complicated than Σ^1_2 which may well have different truth values in L and in V.

8F. Problems for Chapter 8

Problem x8.1 (ZFC, The Countable Reflection Theorem)**.** Prove that for any sentence θ,

$$\theta \Longrightarrow (\exists M)[M \text{ is countable, transitive and } M \models \theta].$$

Hint: Use the Downward Skolem-Löwenheim Theorem 2B.1

Problem x8.2* (ZF_g)**.** None of the following notions is ZFC-absolute: $\mathcal{P}(\omega)$, $\mathrm{Card}(\kappa)$, $\mathbb{R}$, $x \mapsto \mathrm{Power}(x)$, $x \mapsto |x|$.

Hint: This follows quite easily in ZFC from the preceding problem. It can also be proved in ZF^-_g, with just a little more work.

Let us take up first a few simple exercises which will help clarify the definability notions we have been using.

Problem x8.3. Show that if $R(x_1, \dots, x_n)$ is definable by a Σ_0 formula, then the condition

$$R^*(k_1, \dots, k_n) \iff k_1 \in \omega \,\&\, \cdots \,\&\, k_n \in \omega \,\&\, R(k_1, \dots, k_n)$$

is recursive.

A little thinking is needed for the next one.

Problem x8.4. Prove that the condition of satisfaction in #38 of 8A.1 is not definable by a Σ_0 formula.

Problem x8.5 (ZF)**.** Suppose that M is a grounded class, i.e., (by our definition) $M \subseteq V$. Prove that

$$(\forall x \subseteq M)(\exists s \in M)(\forall t \in s)[t \notin x].$$

Note. This is trivial if we assume the Axiom of Foundation by which $\mathcal{V} = V$, so what is needed is to prove it without assuming foundation.

Problem x8.6 (ZF_g^-)**.** Show that for each infinite ordinal ξ, $|L_\xi| = |\xi|$.

Problem x8.7. Prove that

$$\mathsf{ZFC} \nvdash \text{“there exists a weakly inaccessible cardinal”}.$$

Problem x8.8 (ZF_g)**.** Prove that the set $E = \{\xi \in \omega_1 : L_\xi \prec L_{\omega_1}\}$ is closed and unbounded in ω_1.

Hint: Check first that if $\eta < \xi$ and $\eta, \xi \in E$, then $L_\eta \prec L_\xi$.

Definition 8F.1. For each cardinal κ, we set

$$\text{HC}(\kappa) = \{x : |\text{TC}(x)| < \kappa\}. \tag{4}$$

So the sets of hereditarily finite and hereditarily countable sets introduced in Definition 7C.8 are respectively $\text{HC}(\aleph_0)$ and $\text{HC}(\aleph_1)$ with this notation. The sets in $\text{HC}(\kappa)$ are *hereditarily of cardinality* $< \kappa$.

Problem x8.9 (ZFC)**.** Prove that if κ regular, then $\text{HC}(\kappa) \models \mathsf{ZF}_g^-$.

Problem x8.10 (ZF_g)**.** (a) Prove that for every cardinal κ,

$$L_\kappa = \text{HC}(\kappa) \cap L.$$

Infer that if κ is regular, then $L_\kappa \models \mathsf{ZF}_g^-$.

(b) Prove that $\mathsf{ZF}_g \nvdash (L_{\aleph_\omega} \vdash \mathsf{ZF}_g^-)$.

Problem x8.11 (ZF)**.** Prove that for every infinite ordinal ξ,

$$(\xi \to L_{\xi^+}) \cap L \subset L_{\xi^+}.$$

Problem x8.12 (Ordinal pairing functions)**.** Define a binary operation

$$(\eta, \zeta) \mapsto \langle \eta, \zeta \rangle \in \text{ON}$$

on pairs of ordinal to ordinals with the following properties:

(1) $\langle \eta, \zeta \rangle = \langle \eta', \zeta' \rangle \iff \eta = \eta' \ \&\ \zeta = \zeta'$, i.e., $\langle\ \rangle$ is injective.
(2) Every ordinal is $\langle \eta, \zeta \rangle$ for some η, ζ, i.e., $\langle\ \rangle$ is surjective.
(3) For every infinite cardinal κ, if $\eta, \zeta < \kappa$ then $\langle \eta, \zeta \rangle < \kappa$.
(4) For all η, ζ, $\eta \leq \langle \eta, \zeta \rangle$, $\zeta \leq \langle \eta, \zeta \rangle$.

We denote the inverse functions by $(\ )_0, (\ )_1$ so that for every ξ,

$$\xi = \langle (\xi)_0, (\xi)_1 \rangle.$$

Hint: For each cardinal κ, define on $\kappa \times \kappa$ the relation

$$\begin{aligned}(\eta, \zeta) \leq_\kappa (\eta', \zeta') \iff\ & \max(\eta, \zeta) < \max(\eta', \zeta') \\ & \vee \max(\eta, \zeta) = \max(\eta', \zeta')\ \&\ \eta < \eta' \\ & \vee \max(\eta, \zeta) = \max(\eta', \zeta')\ \&\ \eta = \eta'\ \&\ \zeta \leq \zeta',\end{aligned}$$

check that it is a wellordering with rank κ and let

$$\langle\ \rangle_\kappa : \kappa \times \kappa \rightarrowtail\!\!\!\!\rightarrow \kappa$$

be the (unique) similarity. Let $\langle\ \rangle = \bigcup_{\kappa \in \mathrm{Card}} \langle\ \rangle_\kappa$. Only (4) requires some thinking.

Problem x8.13. Prove that there is no guessing sequence $\{t_\xi\}_{\xi \in \omega_1}$ such that for every $f : \omega_1 \to \omega$ the set $\{\xi : f \restriction \xi = t_\xi\}$ is closed and unbounded in ω_1.

Problem x8.14 ($\mathsf{ZFC} + V = L$)**.** Suppose U is a non-principal ultrafilter on ω_1. Prove that there is no guessing sequence $\{t_\xi\}_{\xi \in \omega_1}$ such that for every $f : \omega_1 \to \omega_1$, $\{\xi : f \restriction \xi = t_\xi\} \in U$.

Problem x8.15* (ZFC)**.** Prove that if $\diamondsuit$ holds, then there is a guessing sequence $\{t_\xi\}_{\xi \in \omega_1}$ such that for every $f : \omega_1 \to \omega_1$, the set $\{\xi : f \restriction \xi = t_\xi\}$ is stationary (Theorem 8D.5).

Hint: Take $t_\xi(\eta) = (s_\xi(\eta))_0$, where $\{s_\xi\}_{\xi \in \omega_1}$ is supplied by $\diamondsuit$ and $(\zeta)_0$ is the first projection of a coding of triples below ω_1, i.e., some $\langle\ \rangle : \omega_1^3 \rightarrowtail\!\!\!\!\rightarrow \omega_1$ such that for all ξ, $\xi = \langle (\xi)_0, (\xi)_1), (\xi)_2 \rangle$ and $(\xi)_i \leq \xi$. (There are many other proofs.)

Definition 8F.2 (Σ_1)**.** A formula is Σ_1 if it is of the form

$$(\exists \mathbf{y})\phi \text{ where } \phi \text{ is } \Sigma_0,$$

and a condition $R(x_1, \ldots, x_n)$ is Σ_1 in a theory T if it is defined by a full extended formula $\phi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ such that for some Σ_1 full extended formula $\phi^*(\mathbf{x}_1, \ldots, \mathbf{x}_n)$,

$$T \vdash \phi(\mathbf{x}_1, \ldots, \mathbf{x}_n) \leftrightarrow \phi^*(\mathbf{x}_1, \ldots, \mathbf{x}_n).$$

An operation $F : V^n \to V$ is Σ_1 in a theory T if

$$F(x_1, \ldots, x_n) = w \iff V \models \phi[x_1, \ldots, x_n, w]$$

with a formula $\phi(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{w})$ which is Σ_1 in T and such that

$$T \vdash (\forall \vec{\mathbf{x}})(\exists! \mathbf{w})\phi(\vec{\mathbf{x}}, \mathbf{w}).$$

A condition R is Δ_1 in a theory T if both R and $\neg R$ are Σ_1 in T.

Problem x8.16. Prove that the conditions $x \in L$ and $x \leq_L y$ are both Σ_1 in ZF_g^-.

Problem x8.17. Prove that if $F : V^n \to V$ is Σ_1 in a theory T, then the condition

$$R(\vec{x}, w) \iff F(x_1, \ldots, x_n) = w$$

is Δ_1 in T.

Definition 8F.3 (Collection)**.** An instance of the *Collection Scheme* is any formula of the form

$$(\forall x \in z)(\exists y)\phi \Longrightarrow (\exists w)(\forall x \in z)(\exists y \in w)\phi$$

where w is chosen so that it does not occur free in ϕ. It is an instance of Σ_1-*Collection* if ϕ is a Σ_1 formula.

Problem x8.18. Prove the Collection Scheme in ZF_g.

Problem x8.19. Prove that the collection of conditions which are Σ_1 in ZF_g^- + Collection contains all Σ_0 conditions and is closed under the positive propositional operations $\&, \vee$, the restricted quantifiers $(\forall x \in y), (\exists x \in y)$, existential quantification $(\exists x)$, and the substitution of operations which are Σ_1 in ZF_g^- + Collection, i.e., the scheme

$$P(\vec{x}) \iff R(F_1(\vec{x}), \dots, F_m(\vec{x})).$$

Show also that the collection of operations which are Σ_1 in ZF_g^- + Collection is closed under composition,

$$F(\vec{x}) = G(F_1(\vec{x}), \dots, F_m(\vec{x})).$$

Infer the same closure properties for the collection of notions which are Σ_1 in ZF_g.

Problem x8.20. Prove that all the notions #1 − #40 defined in Theorems 7C.2, 8A.1 are Σ_1 in ZF_g^- + Collection, and so also Σ_1 in ZF_g.