Foundations of Mathematics

Stephen G. Simpson

October 1, 2009

Department of Mathematics
The Pennsylvania State University
University Park, State College PA 16802

simpson@math.psu.edu

This is a set of lecture notes for my course, Foundations of Mathematics I, offered as Mathematics 558 at the Pennsylvania State University, most recently in Fall 2009.

Contents

List of Figures

List of Tables

Chapter 1

Computable Functions

We use $\mathbb{N}$ to denote the set of natural numbers,

$$\mathbb{N} = \{0, 1, 2, \ldots\}\,.$$

For $k \geq 1$, the k-fold Cartesian product

$$\underbrace{\mathbb{N} \times \ldots \times \mathbb{N}}_{k}$$

is denoted $\mathbb{N}^k$. A *k-place function* is a function $f : \mathbb{N}^k \to \mathbb{N}$ and is sometimes indicated with the *lambda-notation*,

$$f = \lambda x_1 \cdots x_k\,[\,f(x_1, \ldots, x_k)\,]\,.$$

A *number-theoretic function* is a k-place function for some $k \geq 1$.

The purpose of this chapter is to define and study an important class of number-theoretic functions, the recursive functions (sometimes called the computable functions). We begin with a certain subclass known as the primitive recursive functions.

1.1 Primitive Recursive Functions

Loosely speaking, a *recursion* is any kind of inductive definition, and a *primitive recursion* is an especially straightforward kind of recursion, in which the value of a number-theoretic function at argument $x + 1$ is defined in terms of the value at argument x. For example, the factorial function $\lambda x\,[\,x!\,]$ is defined by the primitive recursion equations $0! = 1$, $(x + 1)! = x!(x + 1)$. A number-theoretic function is said to be *primitive recursive* if it can be built up by means of primitive recursions. This concept is made precise in the following definition.

Definition 1.1.1 (Primitive Recursive Functions)**.** The class **PR** of primitive recursive functions is the smallest class **C** of number-theoretic functions having the following closure properties.

1. The constant zero function $Z = \lambda x\,[\,0\,]$ belongs to $\mathbf{C}$.

2. The successor function $S = \lambda x\,[\,x+1\,]$ belongs to $\mathbf{C}$.

3. For each $k \geq 1$ and $1 \leq i \leq k$, the projection function $P_{ki} = \lambda x_1 \cdots x_k\,[\,x_i\,]$ belongs to $\mathbf{C}$.

4. $\mathbf{C}$ is closed under generalized composition. This means that whenever the k-place functions

$$\lambda x_1 \cdots x_k\,[\,g_1(x_1,\ldots,x_k)\,],\ldots,\lambda x_1 \cdots x_k\,[\,g_m(x_1,\ldots,x_k)\,]$$

and the m-place function $\lambda y_1 \cdots y_m\,[\,h(y_1,\ldots,y_m)\,]$ all belong to $\mathbf{C}$, then the k-place function

$$f = \lambda x_1 \cdots x_k\,[\,h(g_1(x_1,\ldots,x_k),\ldots,g_m(x_1,\ldots,x_k))\,]$$

also belongs to $\mathbf{C}$. Here f is defined by

$$f(x_1,\ldots,x_k) = h(g_1(x_1,\ldots,x_k),\ldots,g_m(x_1,\ldots,x_k))\,.$$

5. $\mathbf{C}$ is closed under primitive recursion. This means that whenever the k-place function $\lambda x_1 \cdots x_k\,[\,g(x_1,\ldots,x_k)\,]$ and the $(k{+}2)$-place function

$$\lambda y z x_1 \cdots x_k\,[\,h(y,z,x_1,\ldots,x_k)\,]$$

belong to $\mathbf{C}$, then the $(k{+}1)$-place function $\lambda y x_1 \cdots x_k\,[\,f(y,x_1,\ldots,x_k)\,]$ defined by

$$\begin{aligned} f(0,x_1,\ldots,x_k) &= g(x_1,\ldots,x_k) \\ f(y+1,x_1,\ldots,x_k) &= h(y,f(y,x_1,\ldots,x_k),x_1,\ldots,x_k) \end{aligned}$$

also belongs to $\mathbf{C}$.

We now list some examples of primitive recursive functions.

Examples 1.1.2.

1. The recursion equations

$$\begin{aligned} x+0 &= x \\ x+(y+1) &= (x+y)+1 \end{aligned}$$

show that the addition function $\lambda x y\,[\,x+y\,]$ is primitive recursive.

2. The recursion equations

$$\begin{aligned} x\cdot 0 &= 0 \\ x\cdot(y+1) &= (x\cdot y)+x \end{aligned}$$

show that the multiplication function $\lambda x y\,[\,x\cdot y\,]$ is primitive recursive.

3. The recursion equations

$$\begin{aligned} x^0 &= 1 \\ x^{y+1} &= x^y \cdot x \end{aligned}$$

show that the exponentiation function $\lambda xy\,[\,x^y\,]$ is primitive recursive.

4. As already mentioned, the recursion equations

$$\begin{aligned} 0! &= 1 \\ (x+1)! &= x! \cdot (x+1) \end{aligned}$$

show that the factorial function $\lambda x\,[\,x!\,]$ is primitive recursive.

We now proceed to further enlarge our library of primitive recursive functions. First, the recursion equations $P(0) = 0$, $P(x+1) = x$ show that the "predecessor" function

$$P(x) = \begin{cases} x-1 & \text{if } x > 0\,, \\ 0 & \text{if } x = 0 \end{cases}$$

is primitive recursive. We can then obtain the *truncated subtraction* function

$$x \dot{-} y = \begin{cases} x-y & \text{if } x \geq y\,, \\ 0 & \text{if } x < y \end{cases}$$

using primitive recursion equations $x \dot{-} 0 = x$, $x \dot{-} (y+1) = P(x \dot{-} y)$. (Truncated subraction is useful because ordinary subtraction is not a function from $\mathbb{N}^2$ into $\mathbb{N}$.) We shall also have use for

$$|x-y| = (x \dot{-} y) + (y \dot{-} x)$$

and $\alpha(x) = 1 \dot{-} x$. Note that

$$\alpha(x) = \begin{cases} 0 & \text{if } x > 0\,, \\ 1 & \text{if } x = 0\,. \end{cases}$$

The following exercise will become easy after we have developed a little more machinery.

Exercise 1.1.3. Show that the Fibonacci function, defined by

$$\begin{aligned} \mathrm{fib}(0) &= 0\,, \\ \mathrm{fib}(1) &= 1\,, \\ \mathrm{fib}(x+2) &= \mathrm{fib}(x) + \mathrm{fib}(x+1) \end{aligned}$$

is primitive recursive. (The first few values of this function are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...)

In addition to primitive recursive functions, we shall want to consider primitive recursive predicates. By a *k-place predicate* we mean a subset of $\mathbb{N}^k$. If $R \subseteq \mathbb{N}^k$ is a k-place predicate and $x_1, \ldots, x_k$ are elements of $\mathbb{N}$, we say that $R(x_1, \ldots, x_k)$ is *true* if $\langle x_1, \ldots, x_k \rangle \in R$, otherwise *false*. A *number-theoretic predicate* is a k-place predicate for some $k \geq 1$.

Definition 1.1.4. A k-place predicate $R \subseteq \mathbb{N}^k$ is said to be *primitive recursive* if its characteristic function

$$\chi_R(x_1, \ldots, x_k) = \begin{cases} 1 & \text{if } R(x_1, \ldots, x_k) \text{ is true} \\ 0 & \text{if } R(x_1, \ldots, x_k) \text{ is false} \end{cases}$$

is primitive recursive.

For example, the 2-place predicates $x = y$ and $x < y$ are primitive recursive, since $\chi_=(x, y) = \alpha(|x - y|)$ and $\chi_<(x, y) = \alpha(\alpha(y \dot{-} x))$.

Lemma 1.1.5 (Boolean Connectives)**.** If P and Q are primitive recursive predicates, then so are $\neg P$, $P \wedge Q$, and $P \vee Q$. (Here $\neg$, $\wedge$, and $\vee$ denote negation, conjunction, and (nonexclusive) disjunction, respectively.)

Proof. We have $\chi_{\neg P} = \alpha(\chi_P)$ and $\chi_{P \wedge Q} = \chi_P \cdot \chi_Q$. Also

$$\chi_{P \vee Q} = \alpha(\alpha(\chi_P) \cdot \alpha(\chi_Q))$$

since $P \vee Q \equiv \neg((\neg P) \wedge (\neg Q))$ (de Morgan's law). □

Lemma 1.1.6 (Iterated Sums and Products)**.** If $f(x, y, z_1, \ldots, z_k)$ is a primitive recursive function, then so are

$$g(y, z_1, \ldots, z_k) = \sum_{x=0}^{y-1} f(x, y, z_1, \ldots, z_k) \quad (= 0 \text{ if } y = 0)$$

and

$$h(y, z_1, \ldots, z_k) = \prod_{x=0}^{y-1} f(x, y, z_1, \ldots, z_k) \quad (= 1 \text{ if } y = 0)\,.$$

Proof. We have $g(y, z_1, \ldots, z_k) = g^*(y, y, z_1, \ldots, z_k)$ where

$$g^*(w, y, z_1, \ldots, z_k) = \sum_{x=0}^{w-1} f(x, y, z_1, \ldots, z_k)\,.$$

The recursion equations

$$\begin{aligned} g^*(0, y, z_1, \ldots, z_k) &= 0 \\ g^*(w+1, y, z_1, \ldots, z_k) &= g^*(w, y, z_1, \ldots, z_k) + f(w, y, z_1, \ldots, z_k) \end{aligned}$$

show that g^* is primitive recursive, hence g is primitive recursive. The treatment of h is similar. □

Lemma 1.1.7 (Finite Conjuction and Disjunction)**.** If $R(x, y, z_1, \ldots, z_k)$ is a primitive recursive predicate, then so are

$$P(y, z_1, \ldots, z_k) \equiv \bigwedge_{x=0}^{y-1} R(x, y, z_1, \ldots, z_k)$$

and

$$Q(y, z_1, \ldots, z_k) \equiv \bigvee_{x=0}^{y-1} R(x, y, z_1, \ldots, z_k)\,.$$

Proof. We have

$$\chi_P(y, z_1, \ldots, z_k) = \prod_{x=0}^{y-1} \chi_R(x, y, z_1, \ldots, z_k)$$

and

$$\chi_Q(y, z_1, \ldots, z_k) = \alpha\left(\prod_{x=0}^{y-1} \alpha(\chi_R(x, y, z_1, \ldots, z_k))\right)$$

so our result follows from the previous lemma. □

Note that $\bigwedge_{x=0}^{y-1}$ and $\bigvee_{x=0}^{y-1}$ can be paraphrased as "for all x in the range $0 \leq x < y$" and "there exists x in the range $0 \leq x < y$", respectively. These operators are sometimes called *bounded quantifiers*.

The above lemmas make it easy to show that many familiar predicates are primitive recursive. For example, the set (i.e., 1-place predicate) of prime numbers is primitive recursive, since

$$\begin{aligned} \text{Prime}\,(x) &\equiv x \text{ is a prime number} \\ &\equiv x > 1 \wedge \neg \bigvee_{u<x} \bigvee_{v<x} (x = u \cdot v \wedge u > 1 \wedge v > 1)\,. \end{aligned}$$

Similarly, the following lemma can be used to show that many familiar functions are primitive recursive.

Lemma 1.1.8 (Bounded Least Number Operator)**.** If $R(x, y, z_1, \ldots, z_k)$ is a primitive recursive predicate, then the function

$$f(y, z_1, \ldots, z_k) = \begin{cases} \text{least } x < y \text{ such that } R(x, y, z_1, \ldots, z_k) \text{ holds}\,, \\ \qquad \text{if such } x \text{ exists}\,, \\ y \text{ otherwise} \end{cases}$$

is primitive recursive.

Proof. We have

$$\begin{aligned} f(y, z_1, \ldots, z_k) &= \sum_{x=0}^{y-1} \left(x \cdot \chi_R(x, y, z_1, \ldots, z_k) \cdot \prod_{w=0}^{x-1} \alpha(\chi_R(w, y, z_1, \ldots, z_k))\right) \\ &\qquad + y \cdot \prod_{x=0}^{y-1} \alpha(\chi_R(x, y, z_1, \ldots, z_k))\,, \end{aligned}$$

so f is primitive recursive. □

For example, consider the function $\lambda n\,[\,p_n\,]$ which enumerates the prime numbers in increasing order. (The first few values of this function are $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, ...) We want to use the bounded least number operator to show that $\lambda n\,[\,p_n\,]$ is primitive recursive. First, recall a famous theorem of Euclid which gives the bound $p_{n+1} \leq p_n! + 1$. We can then write $p_0 = 2$, $p_{n+1} =$ least $x \leq p_n! + 1$ such that $\mathrm{Prime}\,(x)$ and $x > p_n$. Thus $\lambda n\,[\,p_n\,]$ is primitive recursive.

As another application of the bounded least number operator, note that the functions

$$\begin{aligned} \mathrm{Quotient}\,(y,x) &= \lfloor y/x \rfloor = q\,, \\ \mathrm{Remainder}\,(y,x) &= (y \bmod x) = r\,, \end{aligned}$$

where $y = q \cdot x + r$, $0 \leq r < x$, $0 \leq q$, are primitive recursive, in view of

$$\begin{aligned} \mathrm{Quotient}\,(y,x) &= \text{least } q \leq y \text{ such that } \bigvee_{r<x}(y = q \cdot x + r)\,, \\ \mathrm{Remainder}\,(y,x) &= \text{least } r < x \text{ such that } \bigvee_{q\leq y}(y = q \cdot x + r)\,. \end{aligned}$$

Using the bounded least number operator, we can obtain a primitive recursive method of encoding ordered pairs of natural numbers as single numbers. For our pairing function we use $\lambda uv\,[\,2^u 3^v\,]$. The unpairing functions are then $\lambda z\,[\,(z)_0\,]$ and $\lambda z\,[\,(z)_1\,]$, where

$$\begin{aligned} (z)_n &= \text{least } w < z \text{ such that } \mathrm{Remainder}(z, p_n^{w+1}) \neq 0 \\ &= \text{the exponent of } p_n \text{ in the prime power factorization of } z\,. \end{aligned}$$

Note that $(2^u 3^v)_0 = u$ and $(2^u 3^v)_1 = v$.

More generally, we can encode variable-length finite sequences of natural numbers as single numbers. The sequence $\langle a_0, a_1, \ldots, a_{m-1}\rangle$ is encoded by

$$a = \prod_{x<m} p_x^{a_x}\,,$$

and for decoding we can use the primitive recursive function $\lambda zx\,[\,(z)_x\,]$, since $(a)_x = a_x$. This method of *prime power coding* will be used extensively in the proof of the Enumeration Theorem, below.

The pairing and unpairing functions make it easy to show that the Fibonacci function is primitive recursive (cf. Exercise 1.1.3). Namely, we first note that the auxiliary function $\lambda x\,[\,\mathrm{fibpair}(x)\,]$, defined by

$$\mathrm{fibpair}(x) = 2^{\mathrm{fib}(x)} 3^{\mathrm{fib}(x+1)}\,,$$

is primitive recursive in view of

$$\begin{aligned} \mathrm{fibpair}(0) &= 2^0 3^1\,, \\ \mathrm{fibpair}(x+1) &= 2^{(\mathrm{fibpair}(x))_1} 3^{(\mathrm{fibpair}(x))_0 + (\mathrm{fibpair}(x))_1}\,. \end{aligned}$$

Then $\lambda x\,[\,\mathrm{fib}(x)\,]$ is primitive recursive since $\mathrm{fib}(x) = (\mathrm{fibpair}(x))_0$.

Exercise 1.1.9. Show that the 2-place number-theoretic functions $\mathrm{GCD}(x,y)$ and $\mathrm{LCM}(x,y)$, the greatest common divisor and least common multiple of x and y, are primitive recursive.

Solution. $\mathrm{LCM}(x,y) = \text{least } z \leq x{\cdot}y \text{ such that } \mathrm{Remainder}(z,x) = \mathrm{Remainder}(z,y) = 0$. $\mathrm{GCD}(x,y) = xy/\mathrm{LCM}(x,y)$.

Exercise 1.1.10. Show that the 1-place number-theoretic function $f(n)$ given by

$$f(n) \;=\; 1 + \sum_{k=0}^{n-1} f(k)^n$$

is primitive recursive.

Solution. Consider the so-called *course-of-values function*

$$\widetilde{f}(n) = \prod_{k=0}^{n-1} p_k^{f(k)}\,,$$

i.e., $\widetilde{f}(n)$ encodes the variable-length finite sequence $\langle f(0), f(1), \ldots, f(n-1)\rangle$ via prime power coding. Then $\widetilde{f}(n)$ is primitive recursive, in view of the recursion equations $\widetilde{f}(0) = 1$ and

$$\widetilde{f}(n+1) = \widetilde{f}(n) \cdot p_n^{h(n,\widetilde{f}(n))}\,,$$

where $h(n,z) = 1 + \sum_{k=0}^{n-1}((z)_k)^n$. It now follows that $f(n) = (\widetilde{f}(n+1))_n$ is primitive recursive. This general technique is known as *course-of-values recursion*.

Exercise 1.1.11. Show that the function $\lambda n\,\big(n\text{th digit of } \sqrt{2}\,\big)$ is primitive recursive.

Solution. The nth digit of $\sqrt{2}$ is $f(n) = \mathrm{Remainder}(g(n), 10)$, where $g(n) =$ the least $x < 4 \cdot 10^{2n}$ such that $(x+1)^2 > 2 \cdot 10^{2n}$.

Exercise 1.1.12. Show that the 1-place number-theoretic function

$$f(n) = \text{the } n\text{th decimal digit of } \pi = 3.141592\cdots$$

is primitive recursive.

Hint: You may want to use the fact that $|\pi - a/b| > 1/b^{42}$ for all integers $a, b > 1$. This result is due to K. Mahler, On the approximation of π, Nederl. Akad. Wetensch. Proc. Ser. A., 56, Indagationes Math., 15, 30–42, 1953.

Solution. We use the well-known series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1}\,,$$

i.e.,

$$\pi = 4 - \frac{4}{3} + \frac{4}{5} - \frac{4}{7} + \frac{4}{9} - \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n 4}{2n+1}\,.$$

Let S_k be the kth partial sum of this series. We have $S_k = a(k)/b(k)$ where the functions $a(k)$ and $b(k)$ are primitive recursive, namely

$$a(k) = \sum_{n=0}^{k} \frac{(-1)^n 4(2k+1)!}{2n+1}$$

and $b(k) = (2k+1)!$. Note also that the functions

$$g(n,a,b) = (\mu i < 10^n b)\,(10^i a \geq 10^n b)$$

and

$$h(n,a,b) = \mathrm{Rem}(\mathrm{Quot}(10^{g(n,a,b)}a, b), 10) = \text{the } n\text{th digit of } a/b$$

is primitive recursive. By Mahler's result, for each n there exists $k < 10^{50n}$ such that S_k and S_{k+1} have the same first n digits. Since π lies between S_k and S_{k+1}, it follows that S_k and π have the same first n digits, so in particular $f(n) =$ the nth digit of S_k. Using the bounded least number operator, we have $f(n) = h(n, a(k(n)), b(k(n)))$ where $k(n) =$ the least $k < 10^{50n}$ such that $\bigwedge_{m=0}^{n} g(m, a(k), b(k)) = g(m, a(k+1), b(k+1))$. Clearly this is primitive recursive.

1.2 The Ackermann Function

In this section we present an example of a function which is not primitive recursive, yet is clearly computable in some intuitive sense. The precise concept of computability which we have in mind will be explained in the next section.

Definition 1.2.1. We define a sequence of 1-place functions A_n, $n \in \mathbb{N}$, as follows:

$$\begin{aligned} A_0(x) &= 2x, \\ A_{n+1}(x) &= \underbrace{A_n A_n \cdots A_n}_{x}(1)\,. \end{aligned}$$

Thus $A_0(x) = 2x$, $A_1(x) = 2^x$, $A_2(x) = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height x), etc.

Exercise 1.2.2 (the Ackermann hierarchy)**.**

1. Show that, for each n, $\lambda x\,[\,A_n(x)\,]$ is primitive recursive.
2. Show that
   (a) $A_n(x+1) > A_n(x) > x$ for all $x \geq 1$ and all n.

(b) $A_{n+1}(x) \geq A_n(x+1)$ for all $x \geq 3$ and all n.

3. Show that for each k-place primitive recursive function

$$\lambda x_1 \ldots x_k \, [\, f(x_1, \ldots, x_k) \,]$$

there exists n such that

$$f(x_1, \ldots, x_k) \leq A_n(\max(3, x_1, \ldots, x_k))$$

for all $x_1, \ldots, x_k$.

4. Show that the 2-place function $\lambda nx \, [\, A_n(x) \,]$ is not primitive recursive. This is known as *the Ackermann function*.

5. Show that the 3-place relation $\lambda nxy \, [\, A_n(x) = y \,]$ is primitive recursive. Use this to show that the Ackermann function is computable, i.e., recursive, in the sense of Section 1.3.

Solutions.

1. Show that $A_n(1) = 2$, $A_n(2) = 4$, and $A_{n+1}(3) = A_n(4)$ for all n. Compute $A_n(x)$ for all n, x with $n + x \leq 8$.

   Solution. For all n we have $A_{n+1}(1) = A_n(1)$, hence by induction $A_n(1) = A_0(1) = 2$. Also $A_{n+1}(2) = A_n(A_n(1)) = A_n(2)$, hence by induction $A_n(2) = A_0(2) = 4$. Also, for all n and x we have $A_{n+1}(x+1) = A_n(A_{n+1}(x))$, in particular $A_{n+1}(3) = A_n(A_{n+1}(2)) = A_n(4)$. Table 1.1 shows $A_n(x)$ for small values of n, x.

Table 1.1: The Ackermann branches.

	0	1	2	3	4	5
A_0	0	2	4	6	8	10
A_1	1	2	4	8	16	32
A_2	1	2	4	16	2^{16}	$2^{2^{16}}$
A_3	1	2	4	2^{16}	$2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height 2^{16})	$2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height 2^{16}))
A_4	1	2	4	$2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height 2^{16})	$A_3(2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height 2^{16}))	
A_5	1	2	4	$A_3(2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (height 2^{16}))		
A_6	1	2	4			

2. Prove the following:

(a) $A_n(x+1) > A_n(x) > x$ for all $x \geq 1$ and all n.

(b) $A_{n+1}(x) \geq A_n(x+1)$ for all $x \geq 3$ and all n.

(c) For each primitive recursive function $f(x_1, \ldots, x_k)$ there exists n such that A_n *covers* f, i.e.,

$$f(x_1, \ldots, x_k) \leq A_n(\max(3, x_1, \ldots, x_k))$$

for all $x_1, \ldots, x_k$.

(d) The 1-place function $\lambda x\,(A_x(x))$ is not primitive recursive.

(e) The 2-place function $\lambda xy\,(A_x(y))$ is not primitive recursive.

Solution. First we prove $A_n(x+1) > A_n(x) > x$ for $x \geq 1$, by induction on n. For $n = 0$ we have $A_0(x+1) = 2x+2 > 2x = A_0(x)$ for all x, and $A_0(x) = 2x > x$ for $x \geq 1$. For $n+1$ and $x \geq 1$ we have $A_{n+1}(x+1) = A_n(A_{n+1}(x)) > A_{n+1}(x)$ by inductive hypothesis. Thus A_{n+1} is strictly monotone. Since $A_{n+1}(0) > 0$, it follows that $A_{n+1}(x) > x$ for all x.

Next we prove $A_{n+1}(x) \geq A_n(x+1)$ for $x \geq 3$, by induction on x. For $x = 3$ we have $A_{n+1}(3) = A_n(4)$ as noted above, and inductively $A_{n+1}(x+1) = A_n(A_{n+1}(x)) \geq A_n(A_n(x+1)) \geq A_n(x+2)$, since A_n is strictly monotone and $A_n(x+1) \geq x+2$ by what has already been proved.

Next we prove that each primitive recursive function is covered by A_n for some n. We prove this by induction on the class of primitive recursive functions. We begin by noting that the initial functions are covered by A_0.

Suppose f is obtained by generalized composition, say

$$f(x_1, \ldots, x_k) = h(g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k)).$$

Let n be such that A_n covers h and A_{n+1} covers $g_1, \ldots, g_m$. We then have

$$\begin{array}{rcl} f(x_1, \ldots, x_k) & = & h(g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k)) \\ & \leq & A_n(\max(3, g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k))) \\ & \leq & A_n(A_{n+1}(\max(3, x_1, \ldots, x_k))) \\ & = & A_{n+1}(\max(3, x_1, \ldots, x_k) + 1) \\ & \leq & A_{n+2}(\max(3, x_1, \ldots, x_k)), \end{array}$$

i.e., A_{n+2} covers f.

Suppose f is obtained by primitive recursion, say

$$\begin{array}{rcl} f(0, x_1, \ldots, x_k) & = & g(x_1, \ldots, x_k), \\ f(y+1, x_1, \ldots, x_k) & = & h(y, f(y, x_1, \ldots, x_k), x_1, \ldots, x_k). \end{array}$$

Let n be such that A_n covers h and A_{n+1} covers g. We first claim that

$$f(y, x_1, \ldots, x_k) \leq A_{n+1}(y + \max(3, x_1, \ldots, x_k))$$

for all $y, x_1, \ldots, x_k$. We prove this by induction on y. For $y = 0$ we have $f(0, x_1, \ldots, x_k) = g(x_1, \ldots, x_k) \leq A_{n+1}(\max(3, x_1, \ldots, x_k))$. For the inductive step we have

$$\begin{aligned} f(y+1, x_1, \ldots, x_k) &= h(y, f(y, x_1, \ldots, x_k), x_1, \ldots, x_k) \\ &\leq A_n(\max(3, y, f(y, x_1, \ldots, x_k), x_1, \ldots, x_k) \\ &\leq A_n(\max(3, y, A_{n+1}(y + \max(3, x_1, \ldots, x_k)), x_1, \ldots, x_k) \\ &= A_n(A_{n+1}(y + \max(3, x_1, \ldots, x_k))) \\ &= A_{n+1}(y + 1 + \max(3, x_1, \ldots, x_k)) \end{aligned}$$

and this proves our claim. We then have

$$\begin{aligned} f(y, x_1, \ldots, x_k) &\leq A_{n+1}(y + \max(3, x_1, \ldots, x_k)) \\ &\leq A_{n+1}(2 \max(3, y, x_1, \ldots, x_k)) \\ &\leq A_{n+1}(A_{n+2}(\max(3, y, x_1, \ldots, x_k))) \\ &= A_{n+2}(\max(3, y, x_1, \ldots, x_k) + 1) \\ &\leq A_{n+3}(\max(3, y, x_1, \ldots, x_k)), \end{aligned}$$

i.e., A_{n+3} covers f. This completes the proof that each primitive recursive function is covered by A_n for some n.

Now, if $A_x(x)$ were primitive recursive, then $A_x(x)+1$ would be primitive recursive, hence covered by A_n for some $n \geq 3$. But then in particular $A_n(n) + 1 \leq A_n(\max(3, n)) = A_n(n)$, a contradiction. Thus the 1-place function $A_x(x)$ is not primitive recursive. It follows immediately that the 2-place function $A_x(y)$ is not primitive recursive.

3. Show that the 3-place relation

$$\{\langle x, y, z\rangle \mid A_x(y) = z\}$$

is primitive recursive. Use this to prove that $\lambda xy\,(A_x(y))$ is recursive. Hence $\lambda x\,(A_x(x))$ is recursive.

Solution. For all $x, y > 0$ we have

$$0 < y < A_x(y) = A_{x-1}(A_x(y-1)) = A_{x-1}(y')$$

where $y' = A_x(y-1)$. Since $A_{x-1}(y') = A_x(y) \geq 2$, it follows that $0 < y' < A_{x-1}(y') = A_x(y)$. Repeating this step x times, we obtain a finite sequence $y_0, y_1, y_2, \ldots, y_x$ starting with y such that

$$A_x(y) = A_x(y_0) = A_{x-1}(y_1) = A_{x-2}(y_2) = \cdots = A_0(y_x) = 2y_x,$$

and each of $y_0, y_1, \ldots, y_x$ is > 0 and $< A_x(y)$. Moreover, if $y > 2$ then we also have $x < A_x(y)$. Thus the 3-place predicate $A_x(y) = z$ can be defined

by course-of-values recursion on z as follows:

$$
\begin{aligned}
&A_x(y) = z \text{ if and only if} \\
&(x = 0 \wedge z = 2y) \vee \\
&(x > 0 \wedge y = 0 \wedge z = 1) \vee \\
&(x > 0 \wedge y = 1 \wedge z = 2) \vee \\
&(x > 0 \wedge y = 2 \wedge z = 4) \vee \\
&(x > 0 \wedge y > 2 \wedge x < z \wedge \exists y_0, y_1, \ldots, y_x < z \\
&(y_0 = y \wedge \forall i < x\, (y_{i+1} = A_{x-i}(y_i - 1)) \wedge z = 2y_x)).
\end{aligned}
$$

Actually, the function being defined by primitive recursion is

$$a(w) = \prod\{p_{2^x 3^y 5^z} \mid A_x(y) = z \wedge x, y, z < w\}.$$

In any case, it follows that the 3-place predicate $A_x(y) = z$ is primitive recursive.

Applying the least number operator, we see that the 2-place function $A_x(y)$ is recursive. It follows immediately that the 1-place function $A_x(x)$ is recursive.

1.3 Computable Functions

In this section we define the class of computable (i.e., recursive) number-theoretic functions. We show that the primitive recursive functions form a proper subclass of the computable functions.

Our definition will be given in terms of a *register machine*. We assume the existence of infinitely many registers R_1, R_2, ..., R_i, ... At any given time, each register contains a natural number. If the number contained in R_i is 0, we say that R_i is *empty*. At any given time, all but finitely many of the registers are empty. The basic actions that the machine can perform are to *increment* or *decrement* a register, i.e., add or subtract 1 from the number contained in it.

A *register machine program* consists of finitely many instructions linked together in a flow diagram indicating the order in which the instructions are to be executed. There are four types of instructions: R_i^+, R_i^-, *start*, and *stop*. Each program contains exactly one start instruction, which is executed first. An R_i^+ instruction is executed by incrementing R_i and then proceeding to another, specified, instruction. An R_i^- instruction is executed by testing R_i for emptiness. If R_i is empty, we proceed to one of two specified instructions. If R_i is nonempty, we decrement it and then proceed to the other of the two specified instructions. A stop instruction causes execution of the program to halt. See Figure 1.1.

For example, consider the *addition program* depicted in Figure 1.2. If we run this program starting with natural numbers x and y in R_1 and R_2 respectively, the run will eventually halt with $x + y$ in R_3.

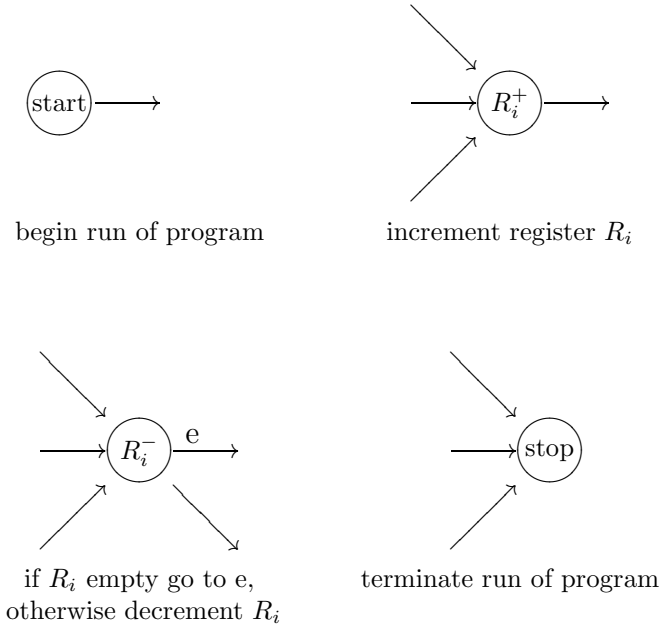


Figure 1.1: Register Machine Instructions

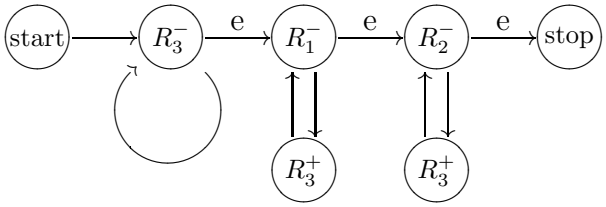


Figure 1.2: An Addition Program

Let $\mathcal{P}$ be a register machine program, and let $x_1, \ldots, x_k$ be natural numbers, i.e., elements of $\mathbb{N}$. We write $\mathcal{P}(x_1, \ldots, x_k)$ to denote the unique run of $\mathcal{P}$ starting with x_1 in R_1, ..., x_k in R_k, and all other registers empty. Uniqueness follows from the fact that the register machine operates deterministically.

Definition 1.3.1 (Computable Functions)**.** A k-place number-theoretic function

$$\lambda x_1 \ldots x_k \, [\, f(x_1, \ldots, x_k) \,]$$

is said to be *computable* if there exists a register machine program $\mathcal{P}$ which computes it, *i*.e. for all $x_1, \ldots, x_k \in \mathbb{N}$, $\mathcal{P}(x_1, \ldots, x_k)$ eventually halts with $y = f(x_1, \ldots, x_k)$ in R_{k+1}.

For example, the addition program of Figure 1.2 shows that $\lambda x_1 x_2 \, [\, x_1 + x_2 \,]$ is computable.

We shall now prove that all primitive recursive functions are computable.

Lemma 1.3.2. The initial functions Z, S, and P_{ki}, $1 \leq i \leq k$, are computable.

Proof. The functions $Z = \lambda x \, [\, 0 \,]$, $S = \lambda x \, [\, x + 1 \,]$, and $P_{ki} = \lambda x_1 \ldots x_k \, [\, x_i \,]$ are computed by the register machine programs given in Figure 1.3. □

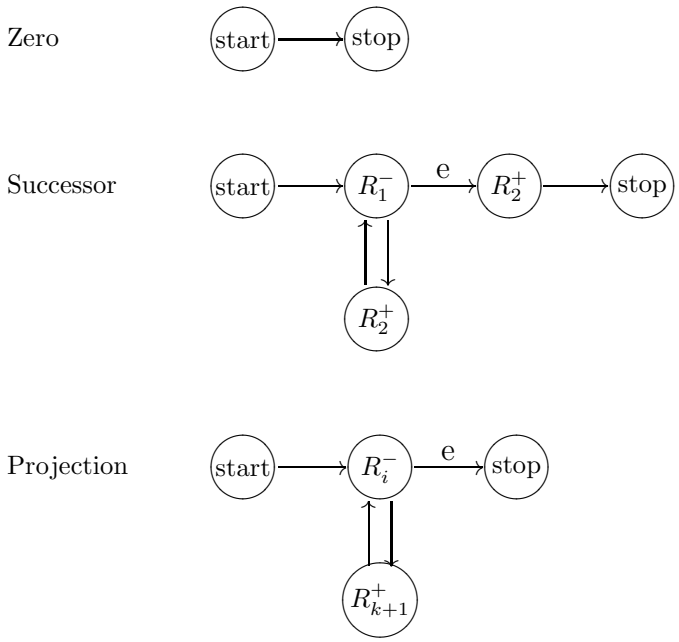


Figure 1.3: The Initial Functions

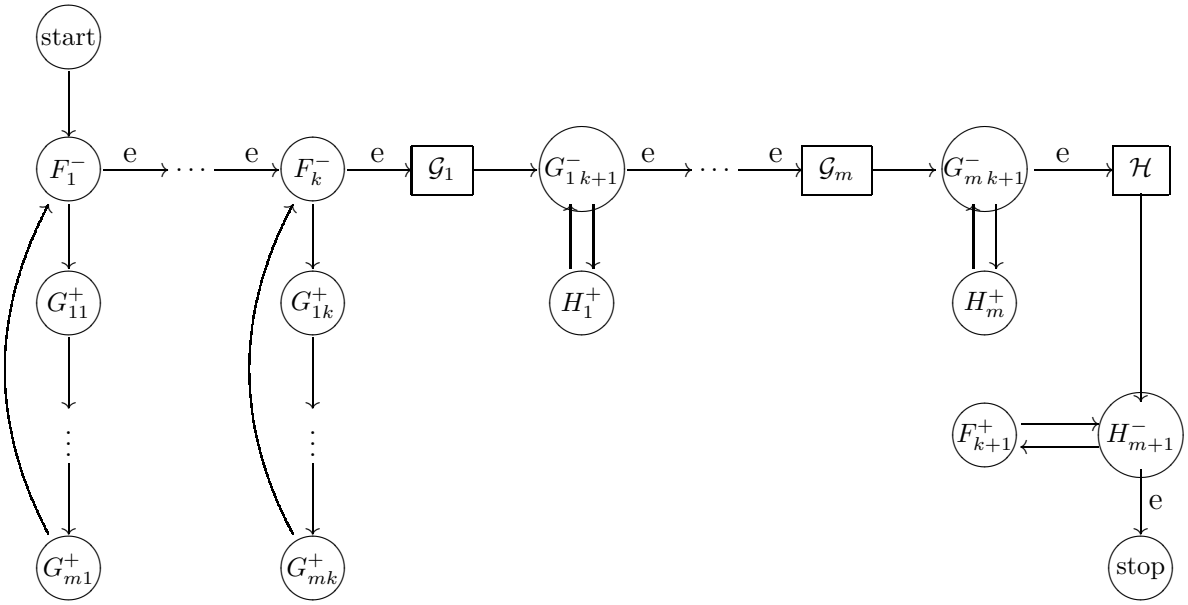


Figure 1.4: Generalized Composition

Lemma 1.3.3. The class of computable functions is closed under generalized composition.

Proof. Assume that

$$\lambda x_1 \dots x_k \, [\, g_1(x_1, \dots, x_k) \,] \, , \; \dots , \; \lambda x_1 \dots x_k \, [\, g_m(x_1, \dots, x_k) \,]$$

and $\lambda y_1 \dots y_m \, [\, h(y_1, \dots, y_m) \,]$ are computed by register machine programs $\mathcal{G}_1$, $\dots$, $\mathcal{G}_m$, $\mathcal{H}$ respectively. For convenience we regard these programs as being executed on pairwise disjoint sets of registers. We use G_{j1}, $\dots$, G_{jk}, $G_{j,k+1}$, $\dots$ to denote the registers on which $\mathcal{G}_j$ is executed, $1 \leq j \leq m$. We use H_1, $\dots$, H_m, H_{m+1}, $\dots$ to denote the registers on which $\mathcal{H}$ is executed.

To compute $\lambda x_1 \dots x_k \, [\, f(x_1, \dots, x_k) \,]$ where

$$f(x_1, \dots, x_k) = h(g_1(x_1, \dots, x_k), \dots, g_m(x_1, \dots, x_k)) \, .$$

we shall use a register machine program $\mathcal{F}$ which we regard as being executed on registers F_1, $\dots$, F_k, F_{k+1}, $\dots$. In order to make it easy for $\mathcal{F}$ to call $\mathcal{G}_1$, $\dots$, $\mathcal{G}_m$, $\mathcal{H}$, the registers of $\mathcal{G}_1$, $\dots$, $\mathcal{G}_m$, $\mathcal{H}$ will be among the auxiliary registers of $\mathcal{F}$. (The auxiliary registers of $\mathcal{F}$ are the registers F_i, $i \geq k+2$.) Actually, the auxiliary registers of $\mathcal{F}$ consist precisely of the registers of $\mathcal{G}_1$, $\dots$, $\mathcal{G}_m$, $\mathcal{H}$. Our program $\mathcal{F}$ is given in Figure 1.4. □

Lemma 1.3.4. The class of computable functions is closed under primitive recursion.

In proving this lemma, the idea will be to write a program containing a loop which repeatedly calls the iterator h. Let us first illustrate this idea with a simple example.

Example 1.3.5. The multiplication function $\lambda x_1 x_2 [\, x_1 \cdot x_2 \,]$ is computed by iterated addition, using the program given in Figure 1.5.

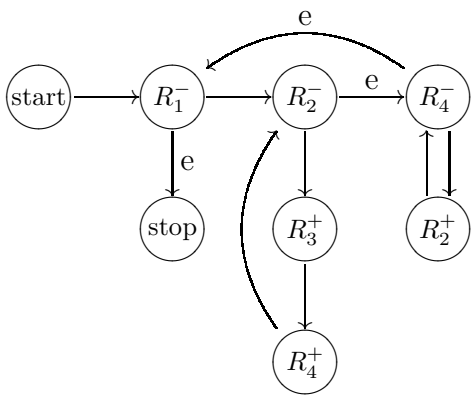


Figure 1.5: A Multiplication Program

Exercise 1.3.6. Write a register machine program which computes the *exponential function*, i.e., the 2-place number-theoretic function $\exp(x, y) = x^y$. Note that $x^0 = 1$ for all x.

Proof of Lemma 1.3.4. Assume that $\lambda x_1 \ldots x_k [\, g(x_1, \ldots, x_k) \,]$ and

$$\lambda y z x_1 \ldots x_k [\, h(y, z, x_1, \ldots, x_k) \,]$$

are computed by register machine programs $\mathcal{G}$ and $\mathcal{H}$ with registers G_1, ..., G_k, G_{k+1}, ... and H_1, H_2, H_3, ..., H_{k+2}, H_{k+3}, ... respectively. To compute $\lambda y x_1 \ldots x_k [\, f(y, x_1, \ldots, x_k) \,]$ where

$$\begin{aligned} f(0, x_1, \ldots, x_k) &= g(x_1, \ldots, x_k)\,, \\ f(y+1, x_1, \ldots, x_k) &= h(y, f(y, x_1, \ldots, x_k), x_1, \ldots, x_k)\,, \end{aligned}$$

we use a register machine program $\mathcal{F}$ with registers F_1, F_2, ..., F_{k+1}, F_{k+2}, ... See Figure 1.6. The auxiliary registers F_i, $i \geq k+3$ of $\mathcal{F}$ consist of the registers of $\mathcal{G}$ and $\mathcal{H}$ plus two additional registers, U and V. □

Theorem 1.3.7. Every primitive recursive function is computable.

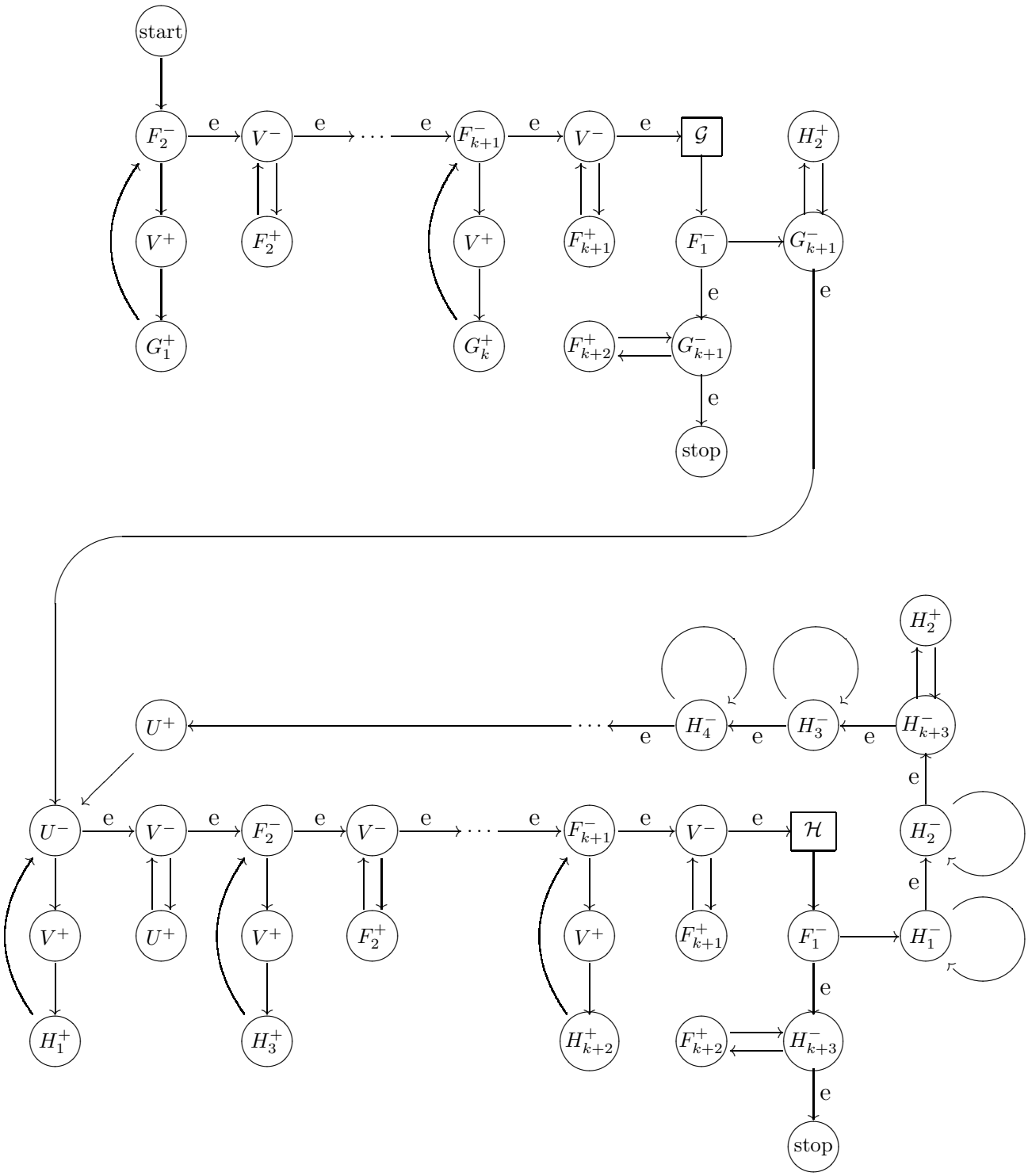


Figure 1.6: Primitive Recursion

Proof. The above lemmas show that the computable functions form a class which contains the initial functions and is closed under generalized composition and primitive recursion. Since the primitive recursive functions were defined as the smallest such class, our theorem follows. □

1.4 Partial Recursive Functions

A *k-place partial function* is a function $\psi : \mathrm{dom}(\psi) \to \mathbb{N}$ where $\mathrm{dom}(\psi) \subseteq \mathbb{N}^k$. We sometimes abbreviate this as $\psi : \mathbb{N}^k \xrightarrow{P} \mathbb{N}$. We use $\mathrm{dom}(\psi)$ and $\mathrm{rng}(\psi)$ to denote the domain and range of ψ, respectively. If $\mathrm{dom}(\psi) = \mathbb{N}^k$, we say that ψ is *total*. Thus a total k-place function is just what we have previously called a k-place function.

The use of partial functions leads to expressions which may or may not have a numerical value. (For example, $\psi(x_1, \ldots, x_k) + 3$ has a numerical value if and only if $\langle x_1, \ldots, x_k \rangle \in \mathrm{dom}(\psi)$). If E is such an expression, we say that E is *defined* or *convergent* (abbreviated $E \downarrow$) if E has a numerical value. We say that E is *undefined* or *divergent* (abbreviated $E \uparrow$) if E does not have a numerical value. We write $E_1 \simeq E_2$ to mean that E_1 and E_2 are both defined and equal, or both undefined.

Definition 1.4.1 (Recursive Functions and Predicates)**.** A k-place (total) function is said to be *recursive* if and only if it is computable. A k-place predicate is said to be *recursive* if its characteristic function is recursive.

Definition 1.4.2 (Partial Recursive Functions)**.** A k-place partial function ψ is said to be *partial recursive* if it is computed by some register machine program $\mathcal{P}$. This means that, for all $x_1, \ldots, x_k \in \mathbb{N}$,

$$\psi(x_1, \ldots, x_k) \simeq \text{ the number in } R_{k+1} \text{ if and when } \mathcal{P}(x_1, \ldots, x_k) \text{ stops}.$$

In particular, $\psi(x_1, \ldots, x_k)$ is defined if and only if $\mathcal{P}(x_1, \ldots, x_k)$ eventually stops.

Partial recursive functions arise because a particular run of a register machine program may or may not eventually stop. One way this can happen is because of an unbounded search, as in the following lemma.

Lemma 1.4.3 (Unbounded Least Number Operator)**.** Let $P(x_1, \ldots, x_k, y)$ be a $(k+1)$-place recursive predicate. Then the k-place partial function ψ defined by

$$\psi(x_1, \ldots, x_k) \simeq \text{ least } y \text{ such that } P(x_1, \ldots, x_k, y) \text{ holds}$$

is partial recursive.

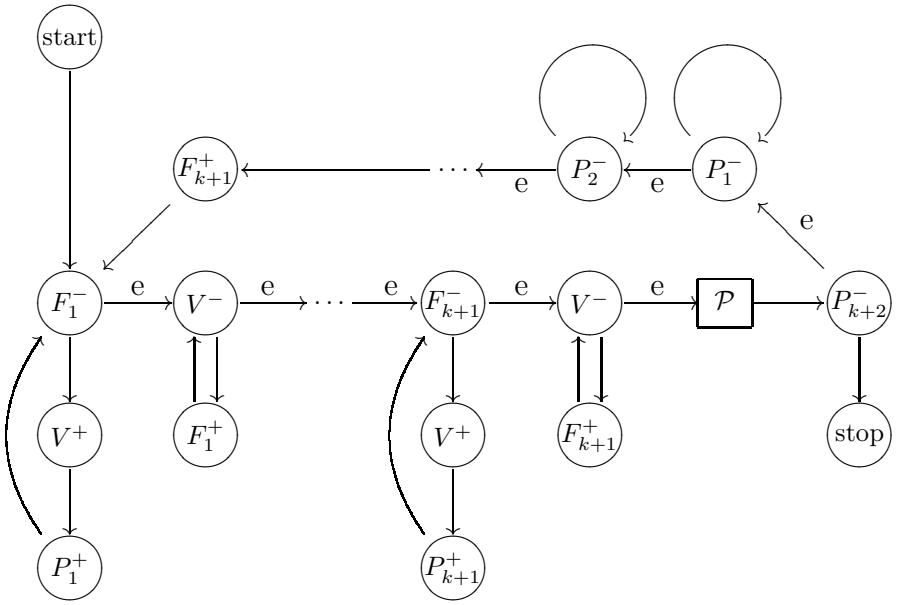


Figure 1.7: Minimization

Proof. Assume that χ_P is computed by a register machine program $\mathcal{P}$ with registers $P_1, \ldots, P_k, P_{k+1}, P_{k+2}, \ldots$. To compute ψ we use a register machine program $\mathcal{F}$ with registers $F_1, F_2, \ldots, F_{k+1}, \ldots$. The auxiliary registers F_i, $i \geq k+2$, of $\mathcal{F}$ are the registers of $\mathcal{P}$ plus an additional register V. See Figure 1.7. □

The unbounded least number operator is sometimes called the *minimization* operator. As a byproduct of the work in the next section, we shall see that all partial recursive functions can be obtained from primitive recursive functions by composition and minimization.

Exercise 1.4.4. Show that the function $f(n) = n$th digit of π is recursive.

Hint: Use an infinite series such as

$$\frac{\pi}{4} \;=\; 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots$$

plus the fact that π is irrational.

Solution. This follows from Exercise 1.1.12. A solution not using Mahler's result is as follows.

Let S_k be the kth partial sum of the alternating series

$$\pi = 4 - \frac{4}{3} + \frac{4}{5} - \frac{4}{7} + \frac{4}{9} - \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n 4}{2n+1}\,,$$

We have $S_k = a(k)/b(k)$ where $a(k)$ and $b(k)$ are primitive recursive. Since π is irrational, it follows that for each n there exists k such that S_k and S_{k+1} have the same first n digits. Since π lies between S_k and S_{k+1}, it follows that S_k and π have the same first n digits, so in particular $f(n) =$ the nth digit of S_k. Note also that the function

$$h(n, a, b) = n\text{th digit of } a/b$$

is primitive recursive. Using the least number operator, we have $f(n) = h(n, a(k(n)), b(k(n)))$ where $k(n) =$ the least k such that $\bigwedge_{m=0}^{n} h(m, a(k), b(k)) = h(m, a(k+1), b(k+1))$. Clearly this is recursive.

Exercise 1.4.5. Show that there exists a computable function which is not primitive recursive. (By 1.2.2 it suffices to show that the Ackermann function $\lambda nx\,[\,A_n(x)\,]$ is computable.)

Exercise 1.4.6. Let $f : \mathbb{N} \overset{1-1 \text{ onto}}{\longrightarrow} \mathbb{N}$ be a permutation of $\mathbb{N}$, the set of natural numbers. Show that if f is recursive, then the inverse permutation f^{-1} is also recursive.

Solution. Using the least number operator, we have $f^{-1}(y) =$ the least x such that $f(x) = y$.

Exercise 1.4.7. Give an example of a primitive recursive permutation of $\mathbb{N}$ whose inverse is not primitive recursive.

Solution. From our study of the Ackermann function in Section 1.2, we know that the predicate $\{\langle x, y\rangle \mid A_x(x) = y\}$ is primitive recursive, although the one-to-one increasing function $x \mapsto A_x(x)$ is not. Let B be the range of $x \mapsto A_x(x)$, i.e., $B = \{y \mid \exists x\,(A_x(x) = y)\}$. Then B is primitive recursive, because $y \in B \Leftrightarrow \bigvee_{x=0}^{y-1} A_x(x) = y$. Note also that B is infinite and coinfinite.

For any infinite set $S \subseteq \mathbb{N}$, let $\pi_S : \mathbb{N} \to \mathbb{N}$ be the *principal function* of S, i.e.,

$$S = \{\pi_S(0) < \pi_S(1) < \cdots < \pi_S(n) < \pi_S(n+1) < \cdots\}$$

where $\pi_S(n) =$ the nth element of S. Let f be the permutation of $\mathbb{N}$ defined by

$$f(y) = \begin{cases} 2\pi_B^{-1}(y) & \text{if } y \in B, \\ 2\pi_{\mathbb{N}\setminus B}^{-1}(y) + 1 & \text{if } y \in \mathbb{N} \setminus B. \end{cases}$$

By course-of-values recursion, f is primitive recursive. However, f^{-1} is not primitive recursive, because $f^{-1}(2x) = \pi_B(x) = A_x(x)$.

1.5 The Enumeration Theorem

To each register machine program $\mathcal{E}$ we shall assign a unique number $e = \#(\mathcal{E})$. This number will be called the *Gödel number* of $\mathcal{E}$ and will also be called an *index* of the k-place partial recursive function which is computed by $\mathcal{E}$

Recall that our register machine is equipped with infinitely many registers R_i, $i \geq 1$. Initially all of the registers are empty except for $R_1, \ldots, R_k$ which contain the arguments $x_1, \ldots, x_k$. We assume that our program $\mathcal{E}$ is given as a numbered sequence of instructions $I_1, \ldots, I_l$. By convention our machine starts by executing I_1 and stops when it attempts to execute the nonexistent instruction I_0. Each instruction I_m, $1 \leq m \leq l$, is of the form

$$\text{increment } R_i \text{ then go to instruction } I_{n_0}, \tag{1.0}$$

or

$$\begin{array}{c}\text{if } R_i \text{ is empty go to } I_{n_0}\text{, otherwise}\\ \text{decrement } R_i \text{ then go to instruction } I_{n_1}.\end{array} \tag{1.1}$$

Here n_0 and n_1 are in the range $0 \leq n \leq l$. To each instruction I_m we assign a Gödel number $\#(I_m)$, where

$$\#(I_m) = \begin{cases} 3^i \cdot 5^{n_0} & \text{for } I_m \text{ as in (1.0)}, \\ 2 \cdot 3^i \cdot 5^{n_0} \cdot 7^{n_1} & \text{for } I_m \text{ as in (1.1)}. \end{cases}$$

The Gödel number of the entire program $\mathcal{E}$ is then defined as

$$\#(\mathcal{E}) = \prod_{m=1}^{l} p_m^{\#(I_m)} \ ,$$

where p_0, p_1, p_2, ... are the prime numbers 2, 3, 5, ... in increasing order.

Example 1.5.1. Let $\mathcal{E}$ be the program in Figure 1.8, which computes $\lambda x\,[\,x{+}1\,]$. Listing the instructions I_1, I_2, I_3 as shown in the figure, we have

$$\begin{aligned} \#(I_1) &= 2 \cdot 3^1 \cdot 5^3 \cdot 7^2 = 2 \cdot 3 \cdot 125 \cdot 49 = 36750\,, \\ \#(I_2) &= 3^2 \cdot 5^1 = 45\,, \\ \#(I_3) &= 3^2 \cdot 5^0 = 9\,, \end{aligned}$$

so that

$$\#(\mathcal{E}) \ = \ 3^{\#(I_1)} \cdot 5^{\#(I_2)} \cdot 7^{\#(I_3)} \ = \ 3^{36750} \cdot 5^{45} \cdot 7^9\,.$$

Lemma 1.5.2. The 1-place predicate

$$\text{Program}\,(e) \ \equiv \ (e \text{ is the Gödel number of some register machine program})$$

is primitive recursive.

Proof. We have

$$\text{Program}\,(e) \quad \equiv \quad \bigvee_{l=0}^{e} \text{Program}\,(e, l)$$

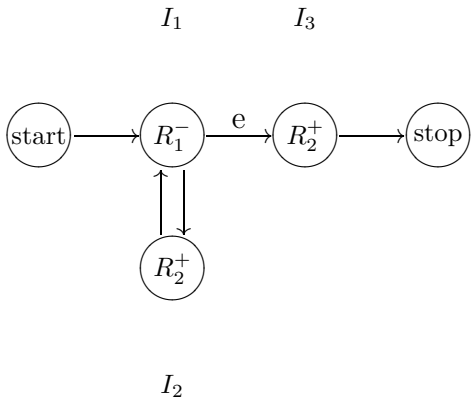


Figure 1.8: A Program with Labeled Instructions

where Program (e, l) says that e is the Gödel number of a register machine program consisting of l instructions $I_1, \ldots, I_l$. We then have

$$\text{Program}\,(e,l) \quad \equiv \quad e = \prod_{m=1}^{l} p_m^{(e)_m} \quad \wedge$$

$$\bigwedge_{m=1}^{l} \bigvee_{i=1}^{e} \bigvee_{n_0=0}^{l} \bigvee_{n_1=0}^{l} \left[\, (e)_m = 3^i \cdot 5^{n_0} \;\vee\; (e)_m = 2 \cdot 3^i \cdot 5^{n_0} \cdot 7^{n_1} \,\right] ,$$

the idea being that $(e)_m = \#(I_m)$. This proves the lemma. □

Definition 1.5.3. We denote by $\varphi_e^{(k)}$ the k-place partial computable function which is computed by the register machine program $\mathcal{E}$ whose Gödel number is e. In more detail, we define

$$\varphi_e^{(k)}(x_1, \cdots, x_k) \simeq \quad \begin{array}{l} \text{the number in } R_{k+1} \text{ if and when } \mathcal{E}(x_1, \cdots, x_k) \\ \text{stops, where } e = \#(\mathcal{E}), \text{ and undefined otherwise.} \end{array}$$

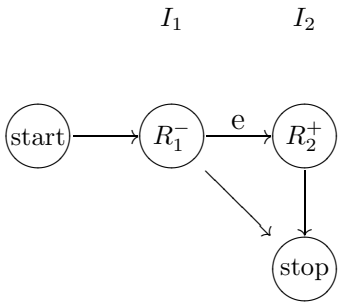
Note that if e is not the Gödel number of a register machine program, then $\varphi_e^{(k)}(x_1, \cdots, x_k)$ is undefined for all $x_1, \ldots, x_k$, so in this case $\varphi_e^{(k)}$ is the empty function.

If ψ is a k-place partial recursive function, an *index* of ψ is any number e such that $\psi = \varphi_e^{(k)}$, i.e., e is the Gödel number of a program which computes ψ. Clearly ψ has many different indices, since there are many different programs which compute ψ.

Exercise 1.5.4. Find an index of the function

$$\alpha(x) = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{if } x > 0. \end{cases}$$

Solution. Clearly the labeled program



computes α. We have $\#(I_1) = 2 \cdot 3^1 \cdot 5^2 \cdot 7^0 = 150$ and $\#(I_2) = 3^2 \cdot 5^0 = 9$, so an index of α is $e = 3^{\#(I_1)} \cdot 5^{\#(I_2)} = 3^{150} \cdot 5^9$. In other words, $\varphi_e^{(1)} = \alpha$.

The main theorem on indices reads as follows.

Theorem 1.5.5 (The Enumeration Theorem)**.** For each $k \geq 1$, the $(k+1)$-place partial function

$$\lambda e x_1 \ldots x_k \, [\, \varphi_e^{(k)}(x_1, \ldots, x_k) \,]$$

is partial recursive.

Remark 1.5.6. The Enumeration Theorem entails the existence of a "universal" program, i.e., a register machine program which can emulate the action of any other register machine program. This concept underlies the stored program digital computer.

In the proof of the Enumeration Theorem, the following easy lemma will be useful.

Lemma 1.5.7 (Definition by Cases)**.** Let P_1 and P_2 be k-place primitive recursive predicates and let f_1 and f_2 be k-place primitive recursive functions. Assume that P_1 and P_2 are mutually exclusive and exhaustive, i.e., for each k-tuple $\langle x_1, \ldots, x_k \rangle \in \mathbb{N}^k$, either $P_1(x_1, \ldots, x_k)$ or $P_2(x_1, \ldots, x_k)$ holds but not both. Then the k-place function f defined by

$$f(x_1, \ldots, x_k) = \begin{cases} f_1(x_1, \ldots, x_k) & \text{if } P_1(x_1, \ldots, x_k) \text{ holds} \\ f_2(x_2, \ldots, x_k) & \text{if } P_2(x_1, \ldots, x_k) \text{ holds} \end{cases}$$

is primitive recursive.

Proof. This is clear since $f = f_1 \cdot \chi_{P_1} + f_2 \cdot \chi_{P_2}$. The extension to more than two cases is also easy. □

Proof of the Enumeration Theorem.

The idea of the proof is to represent the state of $\mathcal{E}(x_1, \ldots, x_k)$ after executing n instructions by a single number

$$\begin{aligned} z &= \text{State}\,(e, x_1, \ldots, x_k, n) \\ &= p_0^m \cdot \textstyle\prod_{i=1}^{\infty} p_i^{z_i}\,, \end{aligned}$$

where z_i is the number in register R_i, and I_m is the next instruction to be executed. Note that $(z)_0 = m$ and, for all $i \geq 1$, $(z)_i = z_i$.

We first show that the State function is primitive recursive. We have

$$\begin{aligned} \text{State}\,(e, x_1, \ldots, x_k, 0) &= p_0^1 \cdot p_1^{x_1} \cdot \ldots \cdot p_k^{x_k} \\ &\quad (\text{begin by executing } I_1)\,, \\ \text{State}\,(e, x_1, \ldots, x_k, n+1) &= \text{NextState}\,(e, \text{State}\,(e, x_1, \ldots, x_k, n))\,, \end{aligned}$$

$$\text{NextState}\,(e, z) = \begin{cases} z \cdot p_i \cdot p_0^{-m+n_0} & \text{if } ((e)_m)_0 = 0\,, \\ z \cdot p_0^{-m+n_0} & \text{if } ((e)_m)_0 = 1 \text{ and } (z)_i = 0\,, \\ z \cdot p_i^{-1} \cdot p_0^{-m+n_1} & \text{if } ((e)_m)_0 = 1 \text{ and } (z)_i > 0\,, \\ z & \text{otherwise}\,, \end{cases}$$

where

$$m = (z)_0\,, \quad i = ((e)_m)_1\,, \quad n_0 = ((e)_m)_2\,, \quad n_1 = ((e)_m)_3\,.$$

We are now ready to prove the theorem. We use the least number operator to obtain

$$\begin{aligned} \text{Stop}\,(e, x_1, \ldots, x_k) \simeq\ & \text{least } n \text{ such that } (\text{State}\,(e, x_1, \ldots, x_k, n))_0 = 0 \\ & \wedge\ \text{Program}\,(e)\,. \end{aligned}$$

(The idea is that our machine stops if and when it is about to execute I_0. Note that $\text{Stop}\,(e, x_1, \ldots, x_k)$ is undefined if e is not the Gödel number of a register machine program.) We then use composition to get

$$\text{FinalState}\,(e, x_1, \ldots, x_k) \simeq \text{State}\,(e, x_1, \ldots, x_k, \text{Stop}\,(e, x_1, \ldots, x_k))$$

(the state of our machine if and when it stops)

and

$$\text{Output}\,(e, x_1, \ldots, x_k) \simeq (\text{FinalState}\,(e, x_1, \ldots, x_k))_{k+1}$$

(the number that is finally in register R_{k+1})\,.

Since the Output function was obtained by composition, primitive recursion and the least number operator, it is partial recursive. Moreover, for all e and x_1, $\ldots$, x_k, we clearly have

$$\varphi_e^{(k)}(x_1, \ldots, x_k) \simeq \text{Output}\,(e, x_1, \ldots, x_k)\,.$$

This completes the proof of the Enumeration Theorem. □

Exercise 1.5.8. Let $f : \mathbb{N}^k \to \mathbb{N}$ be a k-place total recursive function. Show that f is primitive recursive if and only if there exists an index e of f such that

$$\lambda x_1 \ldots x_k \, [\, \mathrm{Stop}\,(e, x_1, \ldots, x_k)\,]$$

is majorized by some primitive recursive function. (See also Exercise 1.2.2.)

Exercise 1.5.9. Fix $k \geq 1$. Construct a $k{+}1$-place total recursive function $\Phi_k : \mathbb{N}^{k+1} \to \mathbb{N}$ with the following properties:

1. for each $e \in \mathbb{N}$, the k-place function $\lambda x_1 \ldots x_k \, [\, \Phi_k(e, x_1, \ldots, x_k)\,]$ is primitive recursive;
2. for each k-place primitive recursive function $f : \mathbb{N}^k \to \mathbb{N}$, there exists an e such that $f = \lambda x_1 \ldots x_k \, [\, \Phi_k(e, x_1, \ldots, x_k)\,]$.

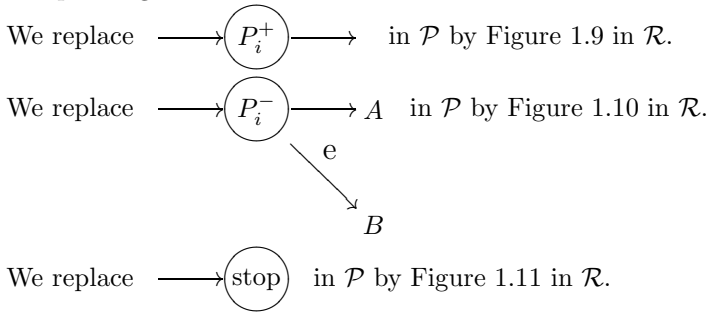
Exercise 1.5.10. Given a k-place partial recursive function $\psi(x_1, \ldots, x_k)$, show that there is a 1-place partial recursive function $\psi^*(x)$ such that

$$\psi^*(p_1^{x_1} \cdots p_k^{x_k}) \simeq p_{k+1}^{\psi(x_1,\ldots,x_k)}$$

for all $x_1, \ldots, x_k$, and ψ^* is computable by a register machine program which uses only two registers, R_1 and R_2.

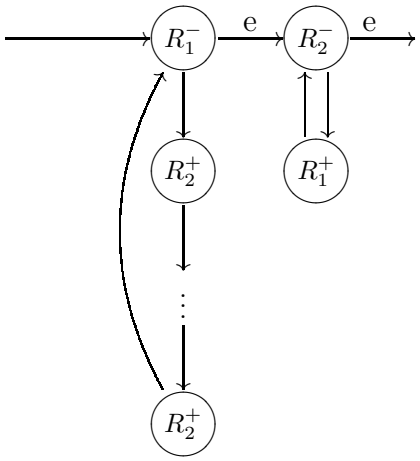
Solution. We begin with a register machine program $\mathcal{P}$ which computes $\psi(x_1, \ldots, x_k)$. Let $P_1, \ldots, P_k, P_{k+1}, \ldots, P_s$ be the registers used in $\mathcal{P}$. We may safely assume that, whenever $\mathcal{P}(x_1, \ldots, x_k)$ halts, it leaves all registers except P_{k+1} empty.

We transform $\mathcal{P}$ into a program $\mathcal{R}$ which uses only two registers, R_1 and R_2. The idea is that, if $P_1, \ldots, P_s$ contain $z_1, \ldots, z_s$ respectively, then R_1 contains $z = p_1^{z_1} \cdots p_s^{z_s}$, while R_2 contains 0. Incrementing (decrementing) P_i corresponds to multiplication (division) by p_i. Each instruction in $\mathcal{P}$ is replaced by a corresponding set of instructions in $\mathcal{R}$.



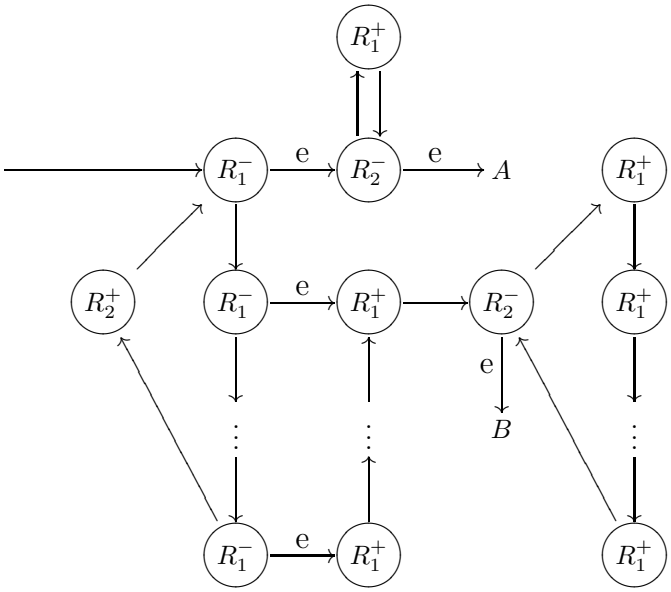
1.6 Consequences of the Enumeration Theorem

In this section we present some important consequences of the Enumeration Theorem.



The number of R_2^+ instructions is p_i.

Figure 1.9: Incrementing P_i



The number of R_1^- instructions is p_i.

Figure 1.10: Decrementing P_i

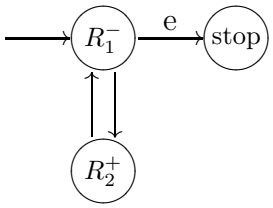


Figure 1.11: Stopping

Theorem 1.6.1. All partial recursive functions can be obtained from primitive recursive functions by composition and minimization.

Proof. This is immediate from the proof of the Enumeration Theorem. The State function is primitive recursive, the Stop function is obtained from the State function by minimization, and the FinalState and Output functions are obtained by composing the Stop and State functions with the primitive recursive function $\lambda z\,[\,(z)_{k+1}\,]$. □

The following characterizations of the class of partial recursive functions do not involve register machines and are similar to our definition of the class of primitive recursive functions.

Corollary 1.6.2. The class of partial recursive functions is the smallest class of functions containing the primitive recursive functions and closed under composition and minimization.

Corollary 1.6.3. The class of partial recursive functions is the smallest class of functions containing the initial functions and closed under composition, primitive recursion, and minimization.

Proof. Both corollaries are immediate from the previous theorem and Lemmas 1.3.2, 1.3.3, 1.3.4, 1.4.3. □

Next we present an interesting example showing that the consideration of partial functions is in some sense unavoidable or inherent in recursive function theory.

Example 1.6.4. We present an example of a partial recursive function $\psi : \mathbb{N} \xrightarrow{P} \mathbb{N}$ which cannot be extended to a total recursive function $f : \mathbb{N} \to \mathbb{N}$. Namely, we define

$$\psi(x) \simeq \varphi_x^{(1)}(x) + 1\,.$$

By the Enumeration Theorem, ψ is a partial recursive function. Suppose ψ were extendible to a total recursive function f. Let e be an index of f. Then $\psi(e) \simeq \varphi_e^{(1)}(e) + 1 \simeq f(e) + 1$ is defined, hence $f(e) \simeq \psi(e) \simeq f(e) + 1$, a contradiction.

Definition 1.6.5. A set $A \subseteq \mathbb{N}$ is said to be recursive if its characteristic function $\chi_A : \mathbb{N} \to \mathbb{N}$ is recursive. More generally, a k-place predicate $R \subseteq \mathbb{N}^k$ is said to be recursive if its characteristic function $\chi_R : \mathbb{N}^k \to \mathbb{N}$ is recursive.

Example 1.6.6. We present an example of a nonrecursive set. Let K be the subset of $\mathbb{N}$ consisting of all $x \in \mathbb{N}$ such that $\varphi_x^{(1)}(x)$ is defined. Thus $K = \mathrm{dom}(\psi)$ where ψ is as in the previous example. We claim that K is not recursive. If K were recursive, then the total function $f : \mathbb{N} \to \mathbb{N}$ defined by

$$f(x) = \begin{cases} \psi(x) & \text{if } x \in K, \\ 0 & \text{if } x \notin K \end{cases}$$

would be recursive, contradicting the fact that ψ is not extendible to a total recursive function.

Definition 1.6.7. A pair of sets $A, B \subseteq \mathbb{N}$ is said to be *recursively inseparable* if there is no recursive set X such that $A \subseteq X$ and $X \cap B = \emptyset$.

Exercise 1.6.8. Letting $K_n = \{x \in \mathbb{N} \mid \varphi_x^{(1)}(x) \simeq n\}$, show that K_0 and K_1 are recursively inseparable.

Exercise 1.6.9. Show that there exists a set $A \subseteq \mathbb{N}$ which is recursive but not primitive recursive.

(Caution: It can be shown that the 3-place predicate $z = A_x(y)$ is primitive recursive, even though the 2-place function $\lambda xy\,[\,A_x(y)\,]$ is not primitive recursive. See Exercises 1.2.2, 1.4.5, 1.5.8, 1.5.9.)

Remark 1.6.10 (Church's Thesis)**.** Perhaps the most important consequence of the proof of the Enumeration Theorem is that it provides strong evidence for Church's Thesis. We shall first explain what Church's Thesis says, and then we shall present the evidence for it.

The context of Church's Thesis is that, as mathematicians, we have an intuitive notion of what it means for a function $f : \mathbb{N}^k \to \mathbb{N}$ to be algorithmically computable. Since recursive functions are register machine computable, they are obviously algorithmically computable in the intuitive sense. Church's Thesis states the converse: All functions $f : \mathbb{N}^k \to \mathbb{N}$ which are algoritmically computable in the intuitive sense are in fact recursive.

To present our evidence for Church's thesis, assume that we are given a function $f : \mathbb{N}^k \to \mathbb{N}$ which is algorithmically computable in the intuitive sense. We want to show that f is recursive. Since the given algorithm for f is presumably deterministic, the execution of the algorithm should be describable as a sequence of states with deterministic transition from one state to the next. The precise nature of the states depends on the nature of the algorithm, but no matter what the states actually consist of, it should be possible to view them as finite strings of symbols and to assign Gödel numbers to them. Once this has been done, the transition from the Gödel number of one state to the Gödel number of the next state should be very simple, in particular primitive recursive. Thus we should

be able to carry out an analysis similar to what is in the proof of Theorem 1.5.5 (State, NextState, Stop, etc.). Such an analysis will show that f is obtained from primitive recursive functions by means of composition and minimization. It will then follow by Corollary 1.6.2 that f is recursive.

The argument in the previous paragraph is of necessity nonrigorous. However, it can be specialized to provide rigorous proofs that various models of computation (similar to but differing in details from register machine computability) give rise to exactly the same class of functions, the recursive functions. Some of the models of computation that have been analyzed in this way are: Turing machines, Markov algorithms, Kleene's equation calculus. There is no reason to think that the same analysis could not be carried out for any similar model. This constitutes very strong evidence for Church's thesis.

Note that the same arguments and evidence apply more generally in case f is a partial rather than a total function. From now on, we shall take Church's Thesis for granted and identify the class of partial recursive functions with the class of partial functions from $\mathbb{N}^k$ into $\mathbb{N}$ that are algorithmically computable in the intuitive sense.

The fact that the intuitive notion of algorithmic computability is captured by a rigorous mathematical notion of recursiveness is one of the successes of modern mathematical logic.

1.7 Unsolvable Problems

The purpose of this section is twofold: (1) to discuss and make precise the concept of an unsolvable mathematical problem, and (2) to present some important examples of such problems.

We begin with a preliminary clarification. In certain contexts, the word *problem* refers to a mathematical statement which has a definite truth value, True or False, but whose truth value is unknown at the present time. (An example of a problem in this sense is the Riemann Hypothesis.) However, we shall not deal with this type of problem now. Instead, we consider a somewhat different concept. For us in this section, a *problem* is any mathematical statement that involves a parameter. A solution of such a problem would be an algorithm which would enable us to compute the truth value of the problem statement for any given value of the parameter. The problem is said to be *solvable* if there exists such an algorithm, otherwise *unsolvable*. An *instance* of a problem is the specialization of the problem statement to a particular parameter value.

As an example of a solvable problem, we mention:

Example 1.7.1. The statement "n is prime" represents the problem of deciding whether an arbitrary number $n \in \mathbb{N}$ is prime or composite. Here the parameter is the variable n. For any particular n (*e.g.* $n = 123456789$), the question of whether this particular n is prime or composite is an instance (i.e., special case) of the general "primality problem". Since the set of prime numbers

$$\{n \in \mathbb{N} \mid n \text{ is prime}\}$$

is primitive recursive, the general primality problem is solvable.

On the other hand, we have the following example of an unsolvable problem.

Example 1.7.2. The set K defined in Example 1.6.6 is nonrecursive. Hence by Church's Thesis there is no algorithm to decide whether or not a given number n belongs to K. It is therefore appropriate to describe the membership problem for K (i.e., the problem of computing the truth value of $n \in K$ for any given n) as an unsolvable problem.

The ability to distinguish solvable problems from unsolvable ones is of basic importance for the mathematical enterprise. Among the most famous unsolvable mathematical problems are:

Example 1.7.3 (Hilbert's Tenth Problem)**.** Hilbert's Tenth Problem is to determine, for a given polynomial p in several variables with integral coeffients, $p \in \mathbb{Z}[X_1, \ldots, X_n]$, whether or not the equation $p(X_1, \ldots, X_n) = 0$ has a solution in integers $X_1, \ldots, X_n \in \mathbb{N}$. This problem encompasses the entire theory of Diophantine equations. A theorem of Matijasevič shows that Hilbert's Tenth Problem is unsolvable. Actually Matijasevič produced a particular polynomial

$$p(X_0, X_1, \ldots, X_9)$$

with 10 indeterminates, such that

$$\{n \in \mathbb{N} \mid p(n, a_1, \ldots, a_9) = 0 \text{ for some } a_1, \ldots, a_9 \in \mathbb{Z}\}$$

is nonrecursive. Once again, our notion of unsolvable problem is related to the existence of a nonrecursive set, namely the set of parameter values n for which the problem statement holds.

Example 1.7.4 (Word Problems)**.** Let G be a group presented by finitely many generators and relations. The *word problem* for G is the problem of determining, for a given word w in the generators of G and their inverses, whether or not $w = 1$ in G. In this case the parameter is w, and the word problem for G is solvable if and only if there exists an algorithm for determining whether or not a given word w is equal to 1 in G. It is known that the word problem is solvable for some groups G and not solvable for others. For example, the word problem for free groups or groups with one relation is solvable, but Boone and Novikov have exhibited groups G with finitely many relations such that the word problem for G is unsolvable.

Example 1.7.5 (The Halting Problem)**.**
Some famous unsolvable problems arise from computability theory itself. One of these is the Halting Problem: To determine whether or not a given register machine program $\mathcal{P}$ will eventually stop, if started with all registers empty. By Gödel numbering, we can identify the Halting Problem with the problem of deciding whether a given natural number e belongs to the set

$$H = \{e \in \mathbb{N} \mid \varphi_e^{(1)}(0) \text{ is defined}\}.$$

We shall prove below that H is nonrecursive, i.e., the Halting Problem is unsolvable.

In all of the above examples, the issue of solvability or unsolvability of a particular problem was rephrased as an issue of whether or not a particular subset of $\mathbb{N}$ is recursive. Such considerations based on Church's Thesis motivate the following definition:

Definition 1.7.6 (Unsolvability)**.** Recall that a set $A \subseteq \mathbb{N}$ is said to be recursive if and only if its characteristic function $\chi_A : \mathbb{N} \to \{0, 1\}$ is recursive. A *problem* is defined to be a subset of $\mathbb{N}$. If $A \subseteq \mathbb{N}$ is a problem in this sense, the problem A is said to be *solvable* if A is recursive, and *unsolvable* if A is nonrecursive.

We shall prove the unsolvability of the Halting Problem, i.e., the nonrecursiveness of the set H in Example 1.7.5 above. The proof will be accomplished by showing that the problem of membership in K is "reducible" to the problem of membership in H. In this context, reducibility of one problem to another means that each instance of the former problem can be effectively converted to an equivalent instance of the latter problem. Our precise notion of reducibility is given by:

Definition 1.7.7 (Reducibility)**.** Let A and B be subsets of $\mathbb{N}$ (i.e., problems, cf. Definition 1.7.6). We say that A *is reducible to* B if there exists a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that, for all $n \in \mathbb{N}$, $n \in A$ implies $f(n) \in B$, and $n \notin A$ implies $f(n) \notin B$.

Lemma 1.7.8. Suppose that A is reducible to B. If B is recursive, then A is recursive. If A is nonrecursive, then B is nonrecursive.

Proof. The first statement follows easily from the fact that $\chi_A(x) = \chi_B(f(x))$. The second statement follows since it is the contrapositive of the first. □

Exercise 1.7.9. Write $A \leq_{\mathrm{m}} B$ to mean that A is reducible to B. Show that

1. $A \leq_{\mathrm{m}} A$ for all $A \subseteq \mathbb{N}$.
2. $A \leq_{\mathrm{m}} B$ and $B \leq_{\mathrm{m}} C$ imply $A \leq_{\mathrm{m}} C$.
3. If $\emptyset \neq \mathrm{B} \neq \mathbb{N}$, then for every recursive set A we have $A \leq_{\mathrm{m}} B$.

In order to prove that the set H is nonrecursive, we shall need the following important technical result:

Theorem 1.7.10 (The Parametrization Theorem)**.** Let $\theta(x_0, x_1, \ldots, x_k)$ be a $(k+1)$-ary partial recursive function. Then we can find a unary primitive recursive function $f(x_0)$ such that, for all $x_0, x_1, \ldots, x_k \in \mathbb{N}$,

$$\varphi^{(k)}_{f(x_0)}(x_1, \ldots, x_k) \;\simeq\; \theta(x_0, x_1, \ldots, x_k)\,.$$

Proof. Let $\mathcal{T}$ be a register machine program which computes the $k+1$-ary partial recursive function θ. The idea of the proof is to let $f(x_0)$ be the Gödel number of a program which is similar to $\mathcal{T}$ but has x_0 hard-coded as the first argument of θ.

Formally, let $\mathcal{T}'$ be a register machine program which computes the $k+1$-ary partial recursive function

$$\theta'(x_1, \ldots, x_k, x_0) \;\simeq\; \theta(x_0, x_1, \ldots, x_k)\,.$$

Let $I_1, \ldots, I_l$ be the instructions of $\mathcal{T}'$, and let $\mathcal{T}''$ be the same as $\mathcal{T}'$ but modified so that the instructions are numbered $I_5, \ldots, I_{l+4}$ instead of $I_1, \ldots, I_l$. Then for any given $x_0 \in \mathbb{N}$, the program $\mathcal{T}'''_{x_0}$ depicted in Figure 1.12 computes the k-ary partial recursive function $\lambda x_1 \ldots x_k\,[\,\theta'(x_1, \ldots, x_k, x_0)\,]$, *i.e.* $\lambda x_1 \ldots x_k\,[\,\theta(x_0, x_1, \ldots, x_k)\,]$. The instructions of $\mathcal{T}'''_{x_0}$ are numbered as $I_1, \ldots, I_{l+x_0+5}$. Let $f(x_0)$ be the Gödel number of $\mathcal{T}'''_{x_0}$. Note that

$$\begin{aligned} f(x_0) &= \textstyle\prod_{m=1}^{l+x_0+5} p_m^{\#(I_m)} \\ &= \textstyle\prod_{m=1}^{l+4} p_m^{\#(I_m)} \cdot \prod_{m=l+5}^{l+x_0+4} p_m^{3^{k+1}\cdot 5^{m+1}} \cdot p_{l+x_0+5}^{2\cdot 3^{k+1}\cdot 5^5 \cdot 7^5} \end{aligned}$$

where the first factor $\prod_{m=1}^{l+4} p_m^{\#(I_m)}$ does not depend on x_0. Thus $f(x_0)$ is a primitive recursive function of x_0. This completes the proof. □

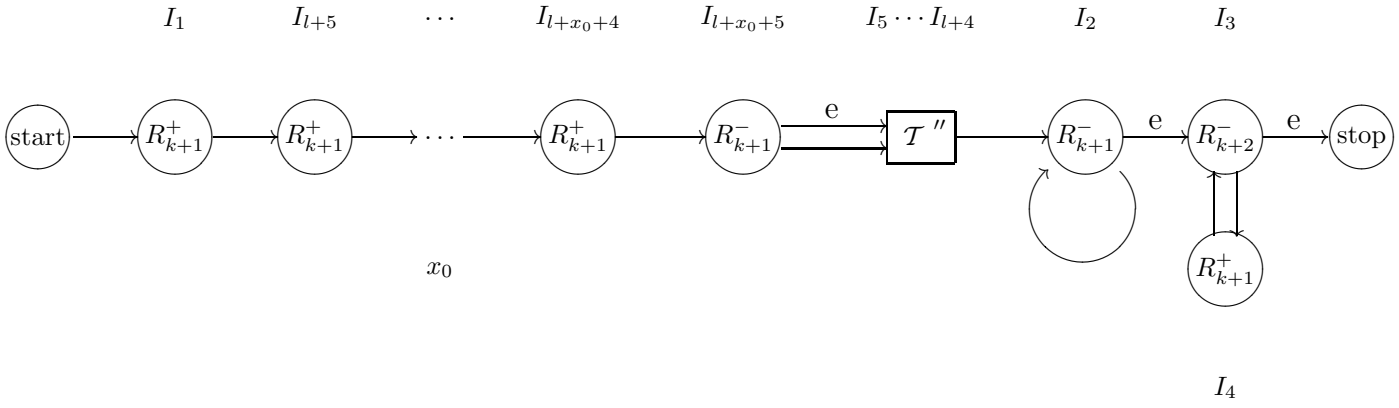


Figure 1.12: Parametrization

We can now prove that the Halting Problem is unsolvable.

Theorem 1.7.11 (Unsolvability of the Halting Problem)**.** The Halting Problem is unsolvable. In other words, the set

$$H = \{x \in \mathbb{N} \mid \varphi^{(1)}_x(0) \text{ is defined}\}$$

of Example 1.7.5 is nonrecursive.

Proof. Let H be as in Example 1.7.5 and let K be as in Example 1.6.6, i.e.,

$$K = \{x \in \mathbb{N} \mid \varphi_x^{(1)}(x) \text{ is defined}\}\,.$$

We shall prove that K is reducible to H. Since K is known to be nonrecursive (Example 1.6.6), it will follow by Lemma 1.7.8 that H is nonrecursive.

Consider the partial recursive function $\theta(x, y) \simeq \varphi_x^{(1)}(x)$. Note that θ is a 2-place function. By the Enumeration Theorem, θ is partial recursive. By the Parametrization Theorem applied with $k = 1$, we can find a primitive recursive function $f : \mathbb{N} \to \mathbb{N}$ such that

$$\varphi_{f(x)}^{(1)}(y) \;\simeq\; \theta(x, y)\,,$$

i.e.,

$$\varphi_{f(x)}^{(1)}(y) \;\simeq\; \varphi_x^{(1)}(x)$$

for all x and y. In particular, if $x \in K$ then $\varphi_x^{(1)}(x)$ is defined, hence $\varphi_{f(x)}^{(1)}(0)$ is defined, i.e., $f(x) \in H$. On the other hand, if $x \notin K$ then $\varphi_x^{(1)}(x)$ is undefined, hence $\varphi_{f(x)}^{(1)}(0)$ is undefined, i.e., $f(x) \notin H$. Thus K is reducible to H via f. This completes the proof. □

Exercise 1.7.12. Show that the following sets and predicates are nonrecursive:

1. $\{x \in \mathbb{N} \mid \varphi_x^{(1)} : \mathbb{N} \xrightarrow{P} \mathbb{N} \text{ is total}\}$.
2. $\{x \in \mathbb{N} \mid \varphi_x^{(1)} \text{ is the empty function}\}$.
3. $\{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid \varphi_x^{(1)} = \varphi_y^{(1)}\}$.
4. $\{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid y \in \mathrm{rng}(\varphi_x^{(1)})\}$.
5. $\{x \in \mathbb{N} \mid 0 \in \mathrm{rng}(\varphi_x^{(1)})\}$.
6. $\{x \in \mathbb{N} \mid \mathrm{rng}(\varphi_x^{(1)}) \text{ is infinite}\}$.

Exercise 1.7.13 (Rice's Theorem)**.** Let $\mathcal{P}$ be the class of 1-place partial recursive functions. For $\mathcal{C} \subseteq \mathcal{P}$, define $I_{\mathcal{C}}$ to be the set of indices of functions in $\mathcal{C}$, i.e.,

$$I_{\mathcal{C}} \;=\; \{x \in \mathbb{N} \mid \varphi_x^{(1)} \in \mathcal{C}\}\,.$$

Show that if $\emptyset \neq \mathcal{C} \neq \mathcal{P}$ then $I_{\mathcal{C}}$ is nonrecursive.

Solution. Let e_0 be an index of the empty function. Let e_1 be an index such that $\varphi_{e_1}^{(1)} \in \mathcal{C}$ if and only if $\varphi_{e_0}^{(1)} \notin \mathcal{C}$. By the Enumeration and Parametrization theorems, we can find a primitive recursive function f such that

$$\varphi_{f(x)}^{(1)}(y) \simeq \begin{cases} \varphi_{e_1}^{(1)}(y) & \text{if } \varphi_x^{(1)}(x)\downarrow, \\ \uparrow & \text{otherwise,} \end{cases}$$

for all x and y. Thus $x \in K$ implies $\varphi^{(1)}_{f(x)} = \varphi^{(1)}_{e_1}$, while $x \notin K$ implies $\varphi^{(1)}_{f(x)} = \varphi^{(1)}_{e_0}$. Thus f reduces K either to $I_{\mathcal{C}}$ (if $\varphi^{(1)}_{e_1} \in \mathcal{C}$) or to the complement of $I_{\mathcal{C}}$ (if $\varphi^{(1)}_{e_1} \notin \mathcal{C}$). In either case it follows that $I_{\mathcal{C}}$ is not recursive.

1.8 The Recursion Theorem

In this section we present an interesting and mysterious theorem known as the Recursion Theorem.

Theorem 1.8.1 (The Recursion Theorem)**.** Let $\theta(w, x_1, \ldots, x_k)$ be a partial recursive function. Then we can find an index e such that, for all $x_1, \ldots, x_k$,

$$\varphi^{(k)}_e(x_1, \ldots, x_k) \simeq \theta(e, x_1, \ldots, x_k) .$$

Proof. Applying the Parametrization Theorem and the Enumeration Theorem, we can find primitive recursive functions f and d such that, for all $w, u, x_1, \ldots, x_k$,

$$\varphi^{(k)}_{f(w)}(x_1, \ldots, x_k) \simeq \theta(w, x_1, \ldots, x_k) .$$

and

$$\varphi^{(k)}_{d(u)}(x_1, \ldots, x_k) \simeq \varphi^{(k)}_{\varphi^{(1)}_u(u)}(x_1, \ldots, x_k) .$$

Let v be an index of $f \circ d$, i.e., $\varphi^{(1)}_v(u) = f(d(u))$ for all u. Then

$$\begin{aligned} \varphi^{(k)}_{d(v)}(x_1, \ldots, x_k) &\simeq \varphi^{(k)}_{\varphi^{(1)}_v(v)}(x_1, \ldots, x_k) \\ &\simeq \varphi^{(k)}_{f(d(v))}(x_1, \ldots, x_k) \\ &\simeq \theta(d(v), x_1, \ldots, x_k) \end{aligned}$$

so we may take $e = d(v)$. This completes the proof. □

Example 1.8.2. As an example, if we take $\theta(w, x) = w + x$, then we obtain an index e such that $\varphi^{(1)}_e(x) = e + x$ for all x.

Example 1.8.3. As another illustration of the Recursion Theorem, we now use it to prove that the Ackermann function $\lambda n x [\, A_n(x) \,]$ (see Section 1.2) is computable. The recursion equations defining the Ackermann function can be written as

$$\begin{aligned} A_0(x) &= 2x \\ A_{n+1}(0) &= 1 \\ A_{n+1}(x+1) &= A_n(A_{n+1}(x)) . \end{aligned}$$

Writing $A(x, y) = A_x(y)$, this becomes

$$\begin{aligned} A(0, y) &= 2y \\ A(x+1, 0) &= 1 \\ A(x+1, y+1) &= A(x, A(x+1, y)) \end{aligned}$$

or in other words

$$A(x,y) \quad = \quad \begin{cases} 2y & \text{if } x = 0\,, \\ 1 & \text{if } x > 0 \text{ and } y = 0\,, \\ A(x \dot{-} 1, A(x, y \dot{-} 1)) & \text{if } x > 0 \text{ and } y > 0\,. \end{cases}$$

By the Enumeration Theorem together with the Recursion Theorem, we can find an index e such that

$$\varphi_e^{(2)}(x,y) \quad \simeq \quad \begin{cases} 2y & \text{if } x = 0\,, \\ 1 & \text{if } x > 0 \text{ and } y = 0\,, \\ \varphi_e^{(2)}(x \dot{-} 1, \varphi_e^{(2)}(x, y \dot{-} 1)) & \text{if } x > 0 \text{ and } y > 0\,. \end{cases}$$

It is then straightforward to prove by induction on x that, for all y, $\varphi_e^{(2)}(x,y) \simeq A(x,y)$. This completes the proof.

Exercise 1.8.4.

1. Find a primitive recursive function $f(x,y)$ such that, for all x and y,
$$\varphi^{(1)}_{f(x,y)} = \varphi^{(1)}_x \circ \varphi^{(1)}_y\,.$$
2. Find a primitive recursive function $g(x,y)$ such that, for all x and y,
$$\mathrm{dom}(\varphi^{(1)}_{g(x,y)}) = \mathrm{dom}(\varphi^{(1)}_x) \cap \mathrm{dom}(\varphi^{(1)}_y)\,.$$
3. Find a primitive recursive function $h(x,y)$ such that, for all x and y,
$$\mathrm{dom}(\varphi^{(1)}_{h(x,y)}) = \mathrm{dom}(\varphi^{(1)}_x) \cup \mathrm{dom}(\varphi^{(1)}_y)\,.$$

Solution.

1. By the Enumeration Theorem and the Parametrization Theorem, find a primitive recursive function $\widehat{f}(w)$ such that
$$\varphi^{(1)}_{\widehat{f}(w)}(z) \simeq \varphi^{(1)}_{(w)_1}(\varphi^{(1)}_{(w)_2}(z))$$
for all w, z. Then $f(x,y) = \widehat{f}(3^x 5^y)$ has the desired property.
2. By the Enumeration Theorem and the Parametrization Theorem, find a primitive recursive function $\widehat{g}(w)$ such that
$$\varphi^{(1)}_{\widehat{g}(w)}(z) \simeq \varphi^{(1)}_{(w)_1}(z) + \varphi^{(1)}_{(w)_2}(z)$$
for all w, z. Then $g(x,y) = \widehat{g}(3^x 5^y)$ has the desired property.

3. By the Parametrization Theorem, find a primitive recursive function $\widehat{h}(w)$ such that

   $$\varphi^{(1)}_{\widehat{h}(w)}(z) \simeq \text{ least } n \text{ such that } (\text{State}((w)_1, z, n))_0 \cdot (\text{State}((w)_2, z, n))_0 = 0$$

   for all w, z. Then $h(x, y) = \widehat{h}(3^x 5^y)$ has the desired property.

Exercise 1.8.5.

1. Find a primitive recursive function $f(x)$ such that for all x, if $\varphi^{(1)}_x$ is a permutation of $\mathbb{N}$, then $\varphi^{(1)}_{f(x)}$ is the inverse permutation.

2. What happens if $\varphi^{(1)}_x$ is assumed only to be partial and one-to-one, and not necessarily a permutation?

Solution. Consider the partial recursive function $\theta(x, y) \simeq$ least w such that $(\text{State}(x, (w)_1, (w)_2))_0 = 0$ and $(\text{State}(x, (w)_1, (w)_2))_2 = y$. By construction, if $\varphi^{(1)}_x(z) \simeq y$ then $(\theta(x, y))_1 \simeq z$. Therefore, by the Parametrization Theorem, let $f(x)$ be a primitive recursive function such that $\varphi^{(1)}_{f(x)}(y) \simeq (\theta(x, y))_1$. This works even if $\varphi^{(1)}_x$ is only assumed to be partial and one-to-one.

Exercise 1.8.6. Find m and n such that $m \neq n$ and $\varphi^{(1)}_m(0) = n$ and $\varphi^{(1)}_n(0) = m$.

Solution. By the Parametrization Theorem, let f be a 1-place primitive recursive function such that $\varphi^{(1)}_{f(x)}(y) = x$ for all x, y. The construction of f in the proof of the Parametrization Theorem shows that $f(x) > x$ for all x. By the Recursion Theorem, let e be such that $\varphi^{(1)}_e(y) \simeq f(e)$ for all y. In particular we have $\varphi^{(1)}_e(0) \simeq f(e)$, $\varphi^{(1)}_{f(e)}(0) = e$, and $f(e) > e$. So take $m = e$ and $n = f(e)$.

1.9 The Arithmetical Hierarchy

In this section we study some important classes of number-theoretic predicates: Σ^0_1, Π^0_1, Σ^0_2, Π^0_2, ... These classes collectively are known as *the arithmetical hierarchy*.

Definition 1.9.1 (The Arithmetical Hierarchy)**.** We define Σ^0_0 and Π^0_0 to be the class of primitive recursive predicates. For $n \geq 1$, we define Σ^0_n to be the class of k-place predicates $P \subseteq \mathbb{N}^k$ (for any $k \geq 1$) such that P can be written in the form

$$P(x_1, \ldots, x_k) \equiv \exists y\, R(x_1, \ldots, x_k, y)$$

where R is a k+1-place predicate belonging to the class Π^0_{n-1}. Similarly, we define Π^0_n to be the class of predicates that can be written in the form

$$P(x_1, \ldots, x_k) \equiv \forall y\, R(x_1, \ldots, x_k, y)$$

where R belongs to the class Σ^0_{n-1}.

For example, a predicate $P(x_1, \ldots, x_k)$ belongs to the class Σ_3^0 if and only if it can be written in the form

$$\exists y_1 \forall y_2 \exists y_3 \, R(x_1, \ldots, x_k, y_1, y_2, y_3)$$

where R is primitive recursive. Similarly, P belongs to the class Π_3^0 if and only if it can be written in the form

$$\forall y_1 \exists y_2 \forall y_3 \, R(x_1, \ldots, x_k, y_1, y_2, y_3)$$

where R is primitive recursive.

Theorem 1.9.2. We have:

1. The classes Σ_n^0 and Π_n^0 are included in the classes Σ_{n+1}^0 and Π_{n+1}^0.
2. The classes Σ_n^0 and Π_n^0 are closed under conjunction and disjunction.
3. The classes Σ_n^0 and Π_n^0 are closed under bounded quantification.
4. For $n \geq 1$, the class Σ_n^0 is closed under existential quantification.
5. For $n \geq 1$, the class Π_n^0 is closed under universal quantification.
6. A predicate P belongs to Σ_n^0 (respectively Π_n^0) if and only if $\neg P$ belongs to Π_n^0 (respectively Σ_n^0).

Proof. Straightforward. □

Theorem 1.9.3. A k-place predicate $P \subseteq \mathbb{N}^k$ belongs to the class Σ_1^0 if and only if $P = \mathrm{dom}(\psi)$ for some k-place partial recursive function $\psi : \mathbb{N}^k \xrightarrow{P} \mathbb{N}$.

Proof. If P is Σ_1^0, then we have

$$P(x_1, \ldots, x_k) \quad \equiv \quad \exists y \, R(x_1, \ldots, x_k, y)$$

where R is primitive recursive, hence $P = \mathrm{dom}(\psi)$ where

$$\psi(x_1, \ldots, x_k) \quad \simeq \quad \text{least } y \text{ such that } R(x_1, \ldots, x_k, y) \text{ holds}\,,$$

and clearly ψ is partial recursive. Conversely, if $P = \mathrm{dom}(\psi)$, then letting e be an index of ψ, we have as in the proof of the Enumeration Theorem

$$P(x_1 \ \ldots, x_k) \quad \equiv \quad \exists n \, (\mathrm{State}(e, x_1, \ldots, x_k, n))_0 = 0\,,$$

hence P is Σ_1^0. □

Corollary 1.9.4. $P \subseteq \mathbb{N}^k$ is Σ_1^0 if and only if

$$P(x_1, \ldots, x_k) \ \equiv \ \exists y \, R(x_1, \ldots, x_k, y)$$

where $R \subseteq \mathbb{N}^{k+1}$ is recursive (not only primitive recursive).

Remark 1.9.5. It follows that, in the definition of Σ^0_n and Π^0_n for $n \geq 1$, we may replace "primitive recursive" by "recursive".

Exercises 1.9.6. If ψ is a k-place partial function, the *graph* of ψ is the $(k{+}1)$-place predicate $G_\psi = \{\langle x_1, \ldots, x_k, y\rangle \mid \psi(x_1, \ldots, x_k) \simeq y\}$.

1. Show that ψ is partial recursive if and only if the graph of ψ is Σ^0_1.
2. Show that, for every $(k{+}1)$-place Σ^0_1 predicate $P(x_1, \ldots, x_k, y)$ there exists a k-place partial recursive function $\psi(x_1, \ldots, x_k)$ which *uniformizes* P, i.e., $G_\psi \subseteq P$ and $\mathrm{dom}(\psi) = \{\langle x_1, \ldots, x_k\rangle \mid \exists y\, P(x_1, \ldots, x_k, y)\}$.

Definition 1.9.7. Let A be an infinite subset of $\mathbb{N}$. The *principal function* of A is the one-to-one function $\pi_A : \mathbb{N} \to \mathbb{N}$ that enumerates the elements of A in increasing order.

Lemma 1.9.8. Let A be an infinite subset of $\mathbb{N}$. The set A is recursive if and only if the function π_A is recursive.

Proof. If A is recursive then the functions ν_A and π_A defined by

$$\begin{aligned} \nu_A(x) &= \text{least } y \text{ such that } y \geq x \text{ and } y \in A \\ \pi_A(0) &= \nu_A(0) \\ \pi_A(x+1) &= \nu_A(\pi_A(x) + 1) \end{aligned}$$

are obviously recursive. Conversely, if π_A is recursive then we have

$$y \in A \quad \text{if and only if} \quad \bigvee_{x=0}^{y} \pi_A(x) = y\,.$$

Since the class of recursive predicates is closed under bounded quantification, it follows that A is recursive. □

Theorem 1.9.9. For $A \subseteq \mathbb{N}$, the following are pairwise equivalent:

1. A is Σ^0_1;
2. $A = \mathrm{dom}(\psi)$ for some partial recursive function $\psi : \mathbb{N} \xrightarrow{P} \mathbb{N}$;
3. $A = \mathrm{rng}(\psi)$ for some partial recursive function $\psi : \mathbb{N} \xrightarrow{P} \mathbb{N}$;
4. $A = \emptyset$ or $A = \mathrm{rng}(f)$ for some total recursive function $f : \mathbb{N} \to \mathbb{N}$;
5. A is finite or $A = \mathrm{rng}(f)$ for some one-to-one total recursive function $f : \mathbb{N} \to \mathbb{N}$.

Proof. The equivalence of 1 and 2 is a special case of Theorem 1.9.3, and the fact that 3 implies 1 is proved similarly. It is easy to see that 5 implies 4 and 4 implies 3. To see that 1 implies 5, suppose that $A \subseteq \mathbb{N}$ is infinite and Σ_1^0, say

$$x \in A \;\equiv\; \exists y R(x,y)$$

where R is primitive recursive. Put

$$B \;=\; \left\{ 2^x 3^y \;\middle|\; R(x,y) \wedge \neg \bigvee_{z=0}^{y-1} R(x,z) \right\}.$$

Then B is an infinite primitive recursive set, so by Lemma 1.9.8, π_B is a one-to-one recursive function. Putting $f(n) = (\pi_B(n))_0$, we see that f is a one-to-one recursive function and $A = \mathrm{rng}(f)$. This completes the proof. □

Remark 1.9.10. A set A satisfying the conditions of Theorem 1.9.9 is sometimes called a *recursively enumerable* set.

Exercises 1.9.11.

1. Show that every nonempty recursively enumerable set is the range of a primitive recursive function.
2. Find an infinite primitive recursive set that is not the range of a one-to-one primitive recursive function.

Definition 1.9.12. For each $n \in \mathbb{N}$, the class Δ_n^0 is defined to be the intersection of the classes Σ_n^0 and Π_n^0.

Theorem 1.9.13. A k-place predicate $P \subseteq \mathbb{N}^k$ belongs to the class Δ_1^0 if and only if P is recursive.

Proof. If P is recursive, it follows easily by Theorem 1.9.3 that P is Δ_1^0. Conversely, if P is Δ_1^0, then we have

$$P(x_1,\ldots,x_k) \quad\equiv\quad \exists y\, R_1(x_1,\ldots,x_k,y) \quad\equiv\quad \forall y\, R_2(x_1,\ldots,x_k,y)$$

where R_1 and R_2 are primitive recursive. Define a total recursive function f by

$$f(x_1,\ldots,x_k) \quad=\quad \text{least } y \text{ such that } R_1(x_1,\ldots,x_k,y) \vee \neg\, R_2(x_1,\ldots,x_k,y)\,.$$

Then we have

$$P(x_1,\ldots,x_k) \quad\equiv\quad R_1(x_1,\ldots,x_k,f(x_1,\ldots,x_k))\,,$$

hence P is recursive. □

Exercise 1.9.14. A function $f : \mathbb{N}^k \to \mathbb{N}$ is said to be *limit-recursive* if there exists a recursive function $g : \mathbb{N}^{k+1} \to \mathbb{N}$ such that

$$f(x_1, \ldots, x_k) = \lim_y g(x_1, \ldots, x_k, y)$$

for all $x_1, \ldots, x_k \in \mathbb{N}$. Show that a predicate P is Δ_2^0 if and only if its characteristic function χ_P is limit-recursive.

Solution. For simplicity, let x be an abbreviation for $x_1, \ldots, x_k$.

First assume that χ_P is limit-recursive, say

$$\chi_P(x) \;=\; \lim_n f(n, x)$$

for all x, where $f(n, x)$ is a recursive function. Then we have

$$P(x) \;\equiv\; \exists m \, \forall n \, (n \geq m \Rightarrow f(n, x) = 1)$$

and

$$\neg\, P(x) \;\equiv\; \exists m \, \forall n \, (n \geq m \Rightarrow f(n, x) = 0)$$

so P is Δ_2^0.

For the converse, assume that P is Δ_2^0, say

$$P(x) \;\equiv\; \exists y \, \forall z \, R_1(x, y, z)$$

and

$$\neg\, P(x) \;\equiv\; \exists y \, \forall z \, R_0(x, y, z)$$

where R_1 and R_0 are primitive recursive predicates. Using the bounded least number operator, define $g(n, x) =$ the least $y < n$ such that either $\forall z < n \, R_1(x, y, z)$ or $\forall z < n \, R_0(x, y, z)$ or both, if such a y exists, and $g(n, x) = n$ otherwise. Thus $g(n, x)$ is a primitive recursive function, and it is easy to see that, for all x, $g(x) = \lim_n g(n, x)$ exists and is equal to the least y such that $\forall z \, R_1(x, y, z)$ or $\forall z \, R_0(x, y, z)$. Now define $h(n, x) = 1$ if $\forall z < n \, R_1(x, g(n, x), z)$, and $h(n, x) = 0$ otherwise. Thus $h(n, x)$ is again a primitive recursive function, and for all x, $h(x) = \lim_n h(n, x)$ exists. Moreover $P(x)$ implies $h(x) = 1$, and $\neg\, P(x)$ implies $h(x) = 0$. Thus χ_P is limit-recursive. This completes the proof.

Theorem 1.9.15 (Universal Σ_n^0 Predicate)**.** For each $n \geq 1$ and $k \geq 1$, we can find a predicate $U = U_{n,k}$ with the following properties:

1. U is a k+1-place predicate belonging to the class Σ_n^0; and
2. for any k-place predicate P belonging to the class Σ_n^0, there exists an $e \in \mathbb{N}$ such that
$$P(x_1, \ldots, x_k) \;\equiv\; U(e, x_1, \ldots, x_k)$$
for all $x_1, \ldots, x_k$.

Proof. This is a straightforward consequence of the Enumeration Theorem. The proof is by induction on n. For $n = 1$ we have

$$U_{1,k}(e, x_1, \ldots, x_k) \equiv \varphi_e^{(k)}(x_1, \ldots, x_k) \downarrow \equiv \exists s \, (\mathrm{State}(e, x_1, \ldots, x_k, s))_0 = 0$$

in view of Theorem 1.9.3. For $n > 1$ we have

$$U_{n,k}(e, x_1, \ldots, x_k) \equiv \exists y \, \neg U_{n-1,k+1}(e, x_1, \ldots, x_k, y) \, .$$

This completes the proof. □

Lemma 1.9.16. Let A, $B \subseteq \mathbb{N}$ and assume that A is reducible to B. Assume $n \geq 1$. If B belongs to Σ_n^0, then so does A. If B belongs to Π_n^0, then so does A.

Proof. Suppose for example that B belongs to Σ_3^0. Then we have

$$x \in B \quad \text{if and only if} \quad \exists y_1 \, \forall y_2 \, \exists y_3 \, R(x, y_1, y_2, y_3)$$

where $R \subseteq \mathbb{N}^4$ is a primitive recursive predicate. If A is reducible to B via the recursive function f, then we have

$$\begin{aligned} x \in A \qquad & \text{if and only if} \qquad f(x) \in B \\ & \text{if and only if} \qquad \exists y_1 \, \forall y_2 \, \exists y_3 \, R(f(x), y_1, y_2, y_3) \, . \end{aligned}$$

Note that the predicate $R(f(x), y_1, y_2, y_3)$ is recursive, hence Δ_1^0. It follows that the predicate $\exists y_3 \, R(f(x), y_1, y_2, y_3)$ is Σ_1^0. Hence A is Σ_3^0. □

Definition 1.9.17. Given $n \geq 1$, a set $B \subseteq \mathbb{N}$ is said to be *complete* Σ_n^0 if

1. B belongs to the class Σ_n^0; and
2. for any set $A \subseteq \mathbb{N}$ belonging to the class Σ_n^0, A is reducible to B.

The notion of complete Π_n^0 set is defined similarly.

Theorem 1.9.18. For each $n \geq 1$ there exists a complete Σ_n^0 set. For each $n \geq 1$ there exists a complete Π_n^0 set. For each $n \geq 1$, a complete Σ_n^0 set is not Π_n^0, and a complete Π_n^0 set is not Σ_n^0.

Proof. By Theorem 1.9.15 let $U(e, x)$ be a universal Σ_n^0 predicate. Obviously the set $\{2^e 3^x \mid U(e, x)\}$ is Σ_n^0 complete. To show that a Σ_n^0 complete set can never be Π_n^0, it suffices by Lemma 1.9.16 to show that there exists a Σ_n^0 set which is not Π_n^0. A simple diagonal argument shows that the Σ_n^0 set $\{x \mid U(x, x)\}$ is not Π_n^0. This completes the proof of the Σ_n^0 part of the theorem. The Π_n^0 part follows easily by taking complements. □

Corollary 1.9.19. For all $n \in \mathbb{N}$ we have

$$\Delta_n^0 \subseteq \Sigma_n^0 \, , \qquad \Delta_n^0 \subseteq \Pi_n^0 \, , \qquad \Sigma_n^0 \cup \Pi_n^0 \subseteq \Delta_{n+1}^0$$

and, except for $n = 0$, all of these inclusions are proper.

Proof. Given $n \geq 1$, let A be a complete Σ^0_n set. Then the complement $B = \mathbb{N} \setminus A$ is complete Π^0_n. Clearly A belongs to $\Sigma^0_n \setminus \Delta^0_n$ and B belongs to $\Pi^0_n \setminus \Delta^0_n$. Moreover it follows by Theorem 1.9.2 and Lemma 1.9.16 that the set

$$A \oplus B \quad = \quad \{2x \mid x \in A\} \cup \{2x+1 \mid x \in B\}$$

belongs to $\Delta^0_{n+1} \setminus (\Sigma^0_n \cup \Pi^0_n)$. □

Exercises 1.9.20.

1. Show that the sets

   $$H = \{x \mid \varphi^{(1)}_x(0) \text{ is defined}\}$$

   and

   $$K = \{x \mid \varphi^{(1)}_x(x) \text{ is defined}\}$$

   are complete Σ^0_1 sets.

2. Show that the set

   $$T = \{x \mid \varphi^{(1)}_x \text{ is total}\}$$

   is a complete Π^0_2 set.

Exercise 1.9.21. What reducibility and non-reducibility relations exist among the following sets? Note that H, T, E, and S are index sets.

$K = \{x \in \mathbb{N} \mid \varphi^{(1)}_x(x) \downarrow\}$,

$H = \{x \in \mathbb{N} \mid \varphi^{(1)}_x(0) \downarrow\}$,

$T = \{x \in \mathbb{N} \mid \varphi^{(1)}_x \text{ is total}\}$,

$E = \{x \in \mathbb{N} \mid \varphi^{(1)}_x \text{ is the empty function}\}$,

$S = \{x \in \mathbb{N} \mid \text{dom}(\varphi^{(1)}_x) \text{ is infinite}\}$.

Prove your answers.

Hint: Using the Parametrization Theorem as in the proof of Theorem 1.7.11, show that H and K are Σ^0_1 complete, S and T are Π^0_2 complete, and E is Π^0_1 complete. These completeness facts, together with Lemma 1.9.16 and Theorem 1.9.18, determine the reducibility relations among H, K, S, T, and E.

Chapter 2

Undecidability of Arithmetic

We are going to show that arithmetic is undecidable. This means that there is no algorithm to decide whether a given sentence in the language of arithmetic is true or false.

2.1 Terms, Formulas, and Sentences

By *arithmetic* we mean the set of sentences which are true in the structure $(\mathbb{N}, +, \cdot, 0, 1, =)$. Here $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of non-negative integers, $+$ and $\cdot$ denote the 2-place operations of addition and multiplication on $\mathbb{N}$, and $=$ denotes the 2-place relation of equality between elements of $\mathbb{N}$. For the benefit of the reader who has not previously studied mathematical logic, we shall now review the concept of a sentence being true in a structure. Since we are only interested in the particular structure $(\mathbb{N}, +, \cdot, 0, 1, =)$, we shall concentrate on that case.

It is first necessary to define a language appropriate for the structure

$$(\mathbb{N}, +, \cdot, 0, 1, =).$$

Our language contains infinitely many variables x_0, x_1, ..., x_n, ... which are usually denoted by letters such as x, y, z, ... Each of these variables is also a term of our language. In addition the symbols 0 and 1 are terms. Other terms are built up using the 2-place operation symbols $+$ and $\cdot$. Examples of terms are

$$1 + 1 + 1\,, \qquad x + 1\,, \qquad (x + y) \cdot z + x\,.$$

When writing terms, we may employ the usual abbreviations. For instance $1 + 1 + 1 = 3$ and $x \cdot x \cdot x = x^3$. Thus a term is essentially a polynomial in several variables with non-negative integer coefficients.

An atomic formula is a formula of the form $t_1 = t_2$ where t_1 and t_2 are terms. Examples of atomic formulas are

$$x + 1 = y\,, \qquad x = 3y^2 + 1\,.$$

Formulas are built from atomic formulas by using the Boolean propositional connectives $\wedge$, $\vee$, $\neg$ (and, or, not) and the quantifiers $\forall$, $\exists$ (for all, there exists). An example of a formula is

$$\exists z\,(x + z + 1 = y) \tag{2.1}$$

In this formula, x, y and z are to be interpreted as variables ranging over the set $\mathbb{N}$. Similarly the expression $\exists z \ldots$ is to be interpreted as "there exists a non-negative integer z in $\mathbb{N}$ such that $\ldots$." Thus the formula (2.1) expresses the assertion that x is less than y. From now on we shall write $x < y$ as an abbreviation for (2.1). This idea of introducing new relation symbols as abbreviations for formulas allows us to expand our language indefinitely.

Another example of a formula is

$$x > 1 \wedge \neg\,\exists y\,\exists z\,(y > 1 \wedge z > 1 \wedge x = y \cdot z)\,. \tag{2.2}$$

This formula expresses the assertion that x is a prime number. Thus we might choose to abbreviate (2.2) by some expression such as Prime(x) or "x is prime."

In any particular formula, a free variable is a variable which is not acted on by any quantifier in that formula. For example, the free variables of (2.1) are x and y, while in (2.2) the only free variable is x. A *sentence* is a formula with no free variables. Examples of sentences are

$$\forall x\,(\exists y\,(x = 2y) \vee \exists y\,(x = 2y + 1)) \tag{2.3}$$

and

$$\forall x\,\exists y\,(x = y + 1)\,. \tag{2.4}$$

When interpreting formulas or sentences in the structure $(\mathbb{N}, +, \cdot, 0, 1, =)$, please bear in mind that the quantifiers $\forall$ and $\exists$ range over the set of non-negative integers, $\mathbb{N}$. Thus $\forall x$ means "for all x in $\mathbb{N}$," and $\exists x$ means "for some x in $\mathbb{N}$" or "there exists x in $\mathbb{N}$ such that $\ldots$." With this understanding, we know what it means for a sentence of our language to be true or false in the structure $(\mathbb{N}, +, \cdot, 0, 1, =)$. For example (2.3) is true (because every element of $\mathbb{N}$ is either even or odd) and (2.4) is false (because not every element of $\mathbb{N}$ is the successor of some other element of $\mathbb{N}$).

Let $F(x_1, \ldots, x_k)$ be a formula whose free variables are $x_1, \ldots, x_k$. Then for any non-negative integers $a_1, \ldots, a_k \in \mathbb{N}$, we can form the sentence $F(a_1, \ldots, a_k)$ which is obtained by substituting ("plugging in") the constants $a_1, \ldots, a_k$ for the free occurrences of the variables $x_1, \ldots, x_k$. For example, let $F(x, y)$ be the formula

$$\exists z\,(x^2 + z = y)$$

with free variables x and y. Then for any particular non-negative integers m and n, $F(m,n)$ is a sentence which expresses the assertion that m^2 is less than or equal to n. For instance $F(5,40)$ is true and $F(5,20)$ is false.

This completes our review of the concept of a sentence being true or false in the structure $(\mathbb{N}, +, \cdot, 0, 1, =)$.

Exercise 2.1.1. Write a sentence expressing Goldbach's Conjecture: Every even number is the sum of two prime numbers.

2.2 Arithmetical Definability

We now present a key definition.

Definition 2.2.1 (Arithmetical Definability)**.** A k-place partial function

$$\lambda x_1 \cdots x_k \, [\, \psi(x_1, \ldots, x_k) \,]$$

is said to be *arithmetically definable* if there exists a formula

$$F(x_1, \ldots, x_k, x_{k+1})$$

with free variables x_1, ..., x_k, x_{k+1}, such that for all $m_1, \ldots, m_k, n \in \mathbb{N}$,

$$\psi(m_1, \ldots, m_k) \simeq n \quad \text{if and only if} \quad F(m_1, ..., m_k, n) \text{ is true.}$$

(Of course it doesn't matter whether we use the variables $x_1, \ldots, x_k$, x_{k+1} or some other set of $k+1$ distinct variables.)

For example, the 1-place function $\lambda x \, [\, 2x \,]$ is arithmetically definable, by the formula $y = 2x$. (Here we are using a formula with two free variables x and y.) As another example, note that the 2-place functions $\lambda xy \, [\, \text{Quotient}(y, x) \,]$ and $\lambda xy \, [\, \text{Remainder}(y, x) \,]$ (the quotient and remainder of y on division by x) are arithmetically definable, by the formulas

$$\exists u \, \exists v \, (y = u \cdot x + v \, \wedge \, v < x \, \wedge \, z = u)$$

and

$$\exists u \, \exists v \, (y = u \cdot x + v \, \wedge \, v < x \, \wedge \, z = v)$$

respectively. (Here we are using formulas with free variables x, y, and z.)

Exercise 2.2.2. Show that the function

$$\lambda xy \, [\, \text{least common multiple of } x \text{ and } y \,]$$

is arithmetically definable.

Remark 2.2.3. A more "mathematical" characterization of arithmetical definability, not involving formulas, may be given as follows. Let us say that a predicate $P \subseteq \mathbb{N}^k$ is *strongly Diophantine* if there exists a polynomial with integer coefficients, $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, such that

$$P = \{\langle a_1, \ldots, a_k \rangle \in \mathbb{N}^k \mid f(a_1, \ldots, a_k) = 0\}.$$

For $Q \subseteq \mathbb{N}^{k+1}$, the *projection* of Q is given as

$$\pi(Q) = \{\langle a_1, \ldots, a_k \rangle \in \mathbb{N}^k \mid \langle a_1, \ldots, a_k, a_{k+1} \rangle \in Q \text{ for some } a_{k+1} \in \mathbb{N}\}\,.$$

Then, the arithmetically definable predicates may be characterized as the smallest class of number-theoretic predicates which contains all strongly Diophantine predicates and is closed under union, complementation, and projection. Clearly each arithmetically definable predicate is obtained by applying these operations only a finite number of times.

Exercise 2.2.4. Show that the following number-theoretic predicates are arithmetically definable, by exhibiting formulas which define them over the structure $(\mathbb{N}, +, \cdot, 0, 1, =)$.

1. $\mathrm{GCD}(x, y) = z$.
2. $\mathrm{LCM}(x, y) = z$.
3. $\mathrm{Quotient}(x, y) = z$.
4. $\mathrm{Remainder}(x, y) = z$.
5. x is the largest prime number less than y.
6. x is the product of all the prime numbers less than y.

Remark 2.2.5. The principal result of this section, Theorem 2.2.21 below, is that all recursive functions and predicates are arithmetically definable. From this it will follow easily that there exists an arithmetically definable predicate which is not recursive (Corollary 2.2.22 below). In addition, we shall characterize the class of arithmetically definable predicates in terms of the arithmetical hierarchy (Theorem 2.2.23 below).

Lemma 2.2.6. The initial functions are arithmetically definable.

Proof. The constant zero function $\lambda x\,[\,0\,]$ is defined by the formula

$$x = x \wedge y = 0\,.$$

The successor function $\lambda x\,[\,x + 1\,]$ is defined by the formula

$$y = x + 1\,.$$

For $1 \leq i \leq k$, the projection function $\lambda x_1 \ldots x_k\,[\,x_i\,]$ is defined by the formula

$$x_1 = x_1 \wedge \ldots \wedge x_k = x_k \wedge y = x_i\,.$$

This completes the proof. □

Lemma 2.2.7. If the functions $g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k)$ and $h(y_1, \ldots, y_m)$ are arithmetically definable, then so is the function

$$f(x_1, \ldots, x_k) \quad = \quad h(g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k))$$

obtained by composition.

Proof. Let $g_1(x_1, \ldots, x_k)$, $\ldots$, $g_m(x_1, \ldots, x_k)$, $h(y_1, \ldots, y_m)$ be defined by the formulas

$$G_1(x_1, \ldots, x_k, y)\,, \ \ldots\ , G_m(x_1, \ldots, x_k, y)\,, H(y_1, \ldots, y_m, z)$$

respectively. Then $f(x_1, \ldots, x_k)$ is defined by the formula

$$\exists y_1 \cdots \exists y_m (G_1(x_1, \ldots, x_k, y_1) \wedge \ldots \wedge G_m(x_1, \ldots, x_k, y_m) \wedge H(y_1, \ldots, y_m, z))$$

which we may abbreviate as $F(x_1, \ldots, x_k, z)$. This proves the lemma. □

A k-place predicate $P(x_1, \ldots, x_k)$ is said to be *arithmetically definable* if it is definable over the structure $(\mathbb{N}, +, \cdot, 0, 1, =)$ by a formula with k free variables x_1, $\ldots$, x_k.

Lemma 2.2.8. If the k+1-place predicate $R(x_1, \ldots, x_k, y)$ is arithmetically definable, then so is the k-place partial function

$$\psi(x_1, \ldots, x_k) \quad \simeq \quad \text{least } y \text{ such that } R(x_1, \ldots, x_k, y) \text{ holds.}$$

Proof. Our $\lambda x_1 \ldots x_k[\psi(x_1, \ldots, x_k)]$ is arithmetically definable by the formula

$$R(x_1, \ldots, x_k, y) \wedge \neg\, \exists z\, (z < y \wedge R(x_1, \ldots, x_k, z))$$

which we may abbreviate as $F(x_1, \ldots, x_k, y)$. This proves the lemma. □

It remains to prove:

Lemma 2.2.9. If the total k-place function $g(y_1, \ldots, y_k)$ and the total k+2-place function $h(x, z, y_1, \ldots, y_k)$ are arithmetically definable, then so is the total k+1-place function

$$f(x, y_1, \ldots, y_k)$$

obtained by primitive recursion:

$$\begin{aligned} f(0, y_1, \ldots, y_k) &= g(y_1, \ldots, y_k)\,, \\ f(x+1, y_1, \ldots, y_k) &= h(x, f(x, y_1, \ldots, y_k), y_1, \ldots, y_k))\,. \end{aligned}$$

In order to prove Lemma 2.2.9, we need some definitions and lemmas from number theory. Two positive integers m and n are said to be *relatively prime* if they have no common factor greater than 1. A set of positive integers is said to be *pairwise relatively prime* if any two distinct integers in the set are relatively prime.

Lemma 2.2.10. Given a positive integer k, we can find infinitely many positive integers a such that the k integers in the set

$$a+1\,,\ 2a+1\,,\ \ldots\,,\ ka+1$$

are pairwise relatively prime.

Proof. Let a be any positive integer which is divisible by all of the prime numbers which are less than k. We claim that $a+1$, $2a+1$, $\ldots$, $ka+1$ are pairwise relatively prime. Suppose not. Let i and j be such that $1 \leq i < j \leq k$ and $ia+1$ and $ja+1$ are not relatively prime. Let p be a prime number which is a factor of both $ia+1$ and $ja+1$. Then p cannot be a factor of m. Hence p is greater than or equal to k. On the other hand p is a factor of $(ja+1)-(ia+1) = (j-i)a$. Hence p is a factor of $j-i$. But $j-i$ is less than k, hence p is less than k, a contradiction. □

Example 2.2.11. If $k = 5$, the primes less than k are 2 and 3, so we can take a to be any multiple of 6. Then the integers $a+1$, $2a+1$, $3a+1$, $4a+1$, $5a+1$ will be pairwise relatively prime. Taking $a = 6$ we see that 7, 13, 19, 25, 31 are paiwise relatively prime. Taking $a = 12$ we see that 13, 25, 37, 49, 61 are pairwise relatively prime. And taking $a = 600$ we see that 601, 1201, 1801, 2401, 3001 are pairwise relatively prime.

Lemma 2.2.12 (Chinese Remainder Theorem)**.** Let $m_1, \ldots, m_k$ be a set of k distinct positive integers which are pairwise relatively prime. Then for any given non-negative integers $r_i < m_i$, $1 \leq i \leq k$, we can find a non-negative integer r such that $\text{Remainder}(r, m_i) = r_i$ for all i.

Proof. Let m be the product of $m_1, \ldots, m_k$. For any non-negative integer r less than m, define the *remainder sequence of* r to be the sequence $\langle r_1, \ldots, r_k\rangle$ where $r_i = \text{Remainder}(r, m_i)$. We claim that any two distinct non-negative integers less than m have distinct remainder sequences. To see this, let r and s be non-negative integers less than m. If r and s have the same remainder sequence, then $r-s$ is divisible by each of $m_1, \ldots, m_k$. Since $m_1, \ldots, m_k$ are pairwise relatively prime, it follows that $r-s$ is divisible by m. Since r and s are both less than m, we must have $r = s$. This proves the claim. Define a *possible remainder sequence* to be any sequence $\langle r_1, \ldots, r_k\rangle$ with $0 \leq r_i < m_i$ for all i. The number of possible remainder sequences is exactly m. From this and the claim, we see that any possible remainder sequence must actually occur as the remainder sequence associated with some r in the range $0 \leq r < m$. The lemma follows immediately. □

Example 2.2.13. Continuing the previous example, we see that for any non-negative integers $r_1 < 7$, $r_2 < 13$, $r_3 < 19$, $r_4 < 25$, $r_5 < 31$, there must be a non-negative integer r less than $7 \cdot 13 \cdot 19 \cdot 25 \cdot 31$ such that $\text{Remainder}(r, 7) = r_1$, $\ldots$, $\text{Remainder}(r, 31) = r_5$. We may view the integer r as a "code" for the sequence $(r_1, r_2, r_3, r_4, r_5)$. The "decoding" is accomplished by means of the key integer 6, since $r_i = \text{Remainder}(r, 6i+1)$.

Definition 2.2.14. For any non-negative integers r, a, i, we define

$$\beta(r, a, i) \quad = \quad \text{Remainder}(r, a \cdot (i+1) + 1)\,.$$

This 3-place function is known as Gödel's β-function. Note that the β-function is arithmetically definable.

The significance of the β-function is that it can be used to encode an arbitrary sequence of non-negative integers $\langle r_0, r_1, \ldots, r_k \rangle$ by means of two non-negative integers r and a. We make this precise in the following lemma.

Lemma 2.2.15. Given a finite sequence of non-negative integers $r_0, r_1, \ldots, r_k$, we can find a pair of non-negative integers r and a such that $\beta(r, a, 0) = r_0$, $\beta(r, a, 1) = r_1$, $\ldots$, $\beta(r, a, k) = r_k$.

Proof. By Lemma 2.2.10 (replacing k by $k+1$), we can find a positive integer a such that $r_0 < a+1$, $r_1 < 2a+1$, $\ldots$, $r_k < (k+1)\cdot a+1$, and furthermore $a+1$, $2a+1$, $\ldots$, $(k+1)\cdot a+1$ are pairwise relatively prime. Then by Lemma 2.2.12 we can find a non-negative integer r such that $\text{Remainder}(r, a+1) = r_0$, $\text{Remainder}(r, 2a+1) = r_1$, $\ldots$, $\text{Remainder}(r, (k+1)\cdot a+1) = r_k$. This proves the lemma. □

Exercise 2.2.16. Find a pair of numbers r, a such that $\beta(r, a, 0) = 11$, $\beta(r, a, 1) = 19$, $\beta(r, a, 2) = 30$, $\beta(r, a, 3) = 37$, $\beta(r, a, 4) = 51$.

Hint: First find an appropriate a by hand. Then write a small computer program to find r by brute force.

We are now ready to prove Lemma 2.2.9.

Proof of Lemma 2.2.9. Let the total functions $g(y_1, \ldots, y_k)$ and $h(x, z, y_1, \ldots, y_k)$ be defined by the formulas $G(y_1, \ldots, y_k, w)$ and $H(x, z, y_1, \ldots, y_k, w)$ respectively. We wish to write down a formula $F(x, y_1, \ldots, y_k, w)$ which would say that there exists a finite sequence $r_0, r_1, \ldots, r_x$ such that $G(y_1, \ldots, y_k, r_0)$ holds, and $H(i, r_i, y_1, \ldots, y_k, r_{i+1})$ holds for all $i < x$, and finally $r_x = w$. If we could do this, then clearly $F(x, y_1, \ldots, y_k, w)$ would define the function $f(x, y_1, \ldots, y_k)$. This would prove the lemma. The only difficulty is that our language is not powerful enough to talk directly about finite sequences of variable length in the required way. Our language allows us to say things like "there exists a non-negative integer r such that $\ldots$," but it does not allow us to directly say things like "there exists a sequence of non-negative integers $r_0, r_1, \ldots, r_x$ (of variable length, x) such that $\ldots$." The way to overcome this difficulty is to use the β-function. Instead of saying "there exists a finite sequence r_0, r_1, $\ldots$, r_k," we can say "there exists a pair of non-negative integers r and a which encode the required sequence, via the β-function." Namely, we write down a formula $F(x, y_1, \ldots, y_k, w)$ which says, informally, there exist r and a such that $G(y_1, \ldots, y_k, \beta(r, a, 0))$ holds, and $H(i, \beta(r, a, i), y_1, \ldots, y_k, \beta(r, a, i+1))$ holds for all $i < x$, and finally $\beta(r, a, x) = w$. By Lemma 2.2.15 it is clear that this

formula defines the function $f(x, y_1, \ldots, y_k)$. Formally, let $B(r, a, i, w)$ be a formula which defines the β-function. We may then take $F(x, y_1, \ldots, y_k, w)$ to be the formula

$$\exists r\, \exists a\, (\, \exists u\, (B(r, a, 0, u) \wedge G(y_1, \ldots, y_k, u)) \;\wedge\; B(r, a, x, w) \wedge$$
$$\forall i\, (\, i \geq x \;\vee\; \exists u\, \exists v\, (B(r, a, i, u) \wedge B(r, a, i+1, v) \wedge H(i, u, y_1, \ldots, y_k, v))\,)\,)\,.$$

This completes the proof of Lemma 2.2.9. □

Example 2.2.17. The exponential function $\lambda xy\,[\,y^x\,]$ is arithmetically definable by the formula

$$\exists r\, \exists a\, (\, B(r, a, 0, 1) \;\wedge\; B(r, a, x, w) \wedge$$
$$\forall i\, (\, i \geq x \vee \exists u\, \exists v\, (B(r, a, i, u) \wedge B(r, a, i+1, v) \wedge v = u \cdot y)\,)\,)$$

which we may abbreviate as $\mathrm{Exp}(x, y, w)$, meaning that $y^x = w$.

Exercise 2.2.18. Consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 3n+1 & \text{if } n \text{ is odd.} \end{cases}$$

For each $k \in \mathbb{N}$ let

$$f^k = \underbrace{f \circ \cdots \circ f}_{k},$$

i.e., $f^0(n) = n$ and $f^{k+1}(n) = f(f^k(n))$.

Write a formula $F(x, y, z)$ in the language $+, \cdot, 0, 1, =, <$ which, when interpreted over the natural number system $\mathbb{N}$, defines the 3-place predicate $f^x(y) = z$.

Exercise 2.2.19. Show that the function $\lambda x\,[\,\text{the } x\text{th Fibonacci number}\,]$ is arithmetically definable.

Exercise 2.2.20. Which of the following number-theoretic predicates are arithmetically definable? Prove your answers.

1. x is the sum of all the prime numbers less than y.
2. $x^y = z$.
3. $x! = y$.

Theorem 2.2.21. Every partial recursive function is arithmetically definable.

Proof. Recall that the partial recursive functions have been characterized as the smallest class of functions which includes the initial functions and is closed under composition, primitive recursion, and the least-number operator. Lemma 2.2.6 says that the class of arithmetically definable functions includes the initial functions. Lemmas 2.2.7, 2.2.8, and 2.2.9 say that the class of arithmetically definable functions is closed under composition, the least-number operator, and primitive recursion, respectively. It follows that the arithmetically definable functions include the partial recursive functions. □

Corollary 2.2.22. There exists a set $K \subseteq \mathbb{N}$ which is arithmetically definable but not recursive.

Proof. Recall that

$$K = \{x \in \mathbb{N} \mid \varphi_x^{(1)}(x) \text{ is convergent}\}$$

is our basic example of a non-recursive set. By the Enumeration Theorem, the 2-place partial function $\lambda xy[\varphi_x^{(1)}(y)]$ is partial recursive. Hence, by Theorem 2.2.21 $\lambda xy[\varphi_x^{(1)}(y)]$ is arithmetically definable. Let $F(x, y, z)$ be a formula which defines this function. Then K is defined by the formula $\exists z F(x, x, z)$. This completes the proof. □

More generally, recall our discussion of the arithmetical hierarchy in Chapter 1, Section 1.9. The next theorem characterizes arithmetically definability (Definition 2.2.1) in terms of the arithmetical hierarchy (Definition 1.9.1).

Theorem 2.2.23. Let P be a k-place predicate, $P \subseteq \mathbb{N}^k$. The following are equivalent:

1. P is arithmetically definable;
2. P belongs to the arithmetical hierarchy, i.e., P belongs to the class Σ_n^0 for some $n \in \mathbb{N}$.

Proof. Theorem 2.2.21 implies that every predicate in the class Σ_0^0 $(= \Pi_0^0)$ is arithmetically definable. From this it is straightforward to prove by induction on $n \in \mathbb{N}$ that every predicate in the class $\Sigma_n^0 \cup \Pi_n^0$ is arithmetically definable. For the converse, put

$$\Sigma_\infty^0 \quad = \quad \bigcup_{n \in \mathbb{N}} \Sigma_n^0 \quad = \quad \bigcup_{n \in \mathbb{N}} \Pi_n^0 .$$

By Theorem 1.9.2, the class Σ_∞^0 is closed under Boolean connectives $\wedge$, $\vee$, $\neg$ and universal and existential quantification $\forall$ and $\exists$. From this it follows that every arithmetically definable predicate P belongs to the class Σ_∞^0; this is proved by induction on the number of symbols in a defining formula for P. □

Exercise 2.2.24. Let A and B be subsets of $\mathbb{N}$. Prove that if A is reducible to B and B is arithmetically definable, then A is arithmetically definable.

Exercise 2.2.25. For each $n \geq 1$ let C_n be a set which is Σ_n^0 complete. Consider the set $B = \{2^n 3^x \mid x \in C_n\}$. Prove that B is not arithmetically definable.

Remark 2.2.26 (Hilbert's Tenth Problem)**.** A refinement of Theorem 2.2.23 due to Matiyasevich 1967 is as follows. Let us say that $P \subseteq \mathbb{N}^k$ is *Diophantine* if $P = \pi^l(Q)$ for some $l \geq 0$ and some strongly Diophantine $Q \subseteq \mathbb{N}^{k+l}$. Thus

$$P = \{\langle a_1, \ldots, a_k \rangle \in \mathbb{N}^k \mid \exists \langle b_1, \ldots, b_l \rangle \in \mathbb{N}^l \, (f(a_1, \ldots, a_k, b_1, \ldots, b_l) = 0)\}$$

where $f(x_1, \ldots, x_k, y_1, \ldots, y_l)$ is a polynomial with integer coefficients. Matiyasevich's Theorem states that P is Diophantine if and only if P is Σ_1^0.

A corollary of Matiyasevich's Theorem is that, for example, the sets K and H are Diophantine. Thus, we can find a polynomial $f(z, x_1, \ldots, x_l)$ with integer coefficients, such that the set of $a \in \mathbb{N}$ for which $f(a, x_1, \ldots, x_l) = 0$ has a solution in $\mathbb{N}$ is nonrecursive. Here it is known that one can take $l = 9$, but $l = 8$ is an open question.

Hilbert's Tenth Problem, as stated in Hilbert's famous 1900 problem list, reads as follows:

> To find an algorithm which allows us, given a polynomial equation in several variables with integer coefficients, to decide in a finite number of steps whether or not the equation has a solution in integers.

From Matiyasevich's Theorem plus the unsolvability of the Halting Problem, it follows that there is no such algorithm. In other words, Hilbert's Tenth Problem is unsolvable.

A full exposition of Hilbert's Tenth Problem and the proof of Matiyasevich's Theorem is in my lecture notes for Math 574, Spring 2005, at

`http://www.math.psu.edu/simpson/notes/.`

Exercise 2.2.27. Recall that $\mathbb{N} = \{0, 1, 2, \ldots\}$ = the natural numbers, while $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ = the integers. In our formulation of Matiyasevich's Theorem, we have spoken of solutions in $\mathbb{N}$. What happens if we replace "solution in $\mathbb{N}$" by "solution in $\mathbb{Z}$"?

Hint: Use the following well-known theorem of Lagrange: For each $n \in \mathbb{N}$ there exist $a, b, c, d \in \mathbb{N}$ such that $n = a^2 + b^2 + c^2 + d^2$.

2.3 Gödel Numbers of Formulas

For each formula F in the language of arithmetic, we shall define a unique positive integer $\#(F)$, which will be called *the Gödel number of* F. The number $\#(F)$ will serve as a "code" for the formula F.

Before assigning Gödel numbers to formulas, we shall first assign Gödel numbers to terms. We define

$$\begin{aligned} \#(0) &= 1 \\ \#(1) &= 3 \\ \#(x_i) &= 3^2 \cdot 5^i \\ \#(t_1 + t_2) &= 3^3 \cdot 5^{\#(t_1)} \cdot 7^{\#(t_2)} \\ \#(t_1 \cdot t_2) &= 3^4 \cdot 5^{\#(t_1)} \cdot 7^{\#(t_2)} \end{aligned}$$

For example, the Gödel number of the term $1 + x_0$ is

$$\#(1 + x_0) = 3^3 \cdot 5^3 \cdot 7^9$$

since $\#(1) = 3$ and $\#(x_0) = 9$.

We now define the Gödel numbers of formulas:

$$\begin{aligned}
\#(t_1 = t_2) &= 2 \cdot 5^{\#(t_1)} \cdot 7^{\#(t_2)} \\
\#(F \wedge G) &= 2 \cdot 3 \cdot 5^{\#(F)} \cdot 7^{\#(G)} \\
\#(F \vee G) &= 2 \cdot 3^2 \cdot 5^{\#(F)} \cdot 7^{\#(G)} \\
\#(\neg F) &= 2 \cdot 3^3 \cdot 5^{\#(F)} \\
\#(\forall x_i F) &= 2 \cdot 3^4 \cdot 5^i \cdot 7^{\#(F)} \\
\#(\exists x_i F) &= 2 \cdot 3^5 \cdot 5^i \cdot 7^{\#(F)}
\end{aligned}$$

For example, the Gödel number of the formula $\exists x_1(x_1 = 1)$ is

$$\#(\exists x_1(x_1 = 1)) \quad = \quad 2 \cdot 3^5 \cdot 5^1 \cdot 7^{2 \cdot 5^{45} \cdot 7^3}$$

since $\#(x_1) = 45$, $\#(1) = 3$, and $\#(x_1 = 1) = 2 \cdot 5^{45} \cdot 7^3$.

If $\mathcal{F}$ is any collection of formulas, we denote by $\#(\mathcal{F})$ the collection of all Gödel numbers of formulas in $\mathcal{F}$. Let

$$\mathsf{Fml} = \#(\text{all formulas}),$$

$$\mathsf{Snt} = \#(\text{all sentences}),$$

and

$$\mathsf{TrueSnt} = \#(\text{all true sentences}).$$

Note that Fml, Snt, and TrueSnt are subsets of $\mathbb{N}$.

Theorem 2.3.1. The sets Fml and Snt are primitive recursive.

Proof. The proof is straightforward and we omit it. □

We are going to prove that the set TrueSnt is nonrecursive. In other words, the problem of deciding whether a given sentence of the language of arithmetic is true or false is unsolvable. This result may be paraphrased as "arithmetical truth is undecidable," or simply, "arithmetic is undecidable."

Theorem 2.3.2. Every arithmetically definable set $A \subseteq \mathbb{N}$ is reducible to TrueSnt.

Proof. Given an arithmetically definable set A, let $F(x_1)$ be a formula with one free variable x which defines A, i.e.,

$$A \quad = \quad \{m \in \mathbb{N} \mid F(m) \text{ is true}\}.$$

Define

$$f(m) \quad = \quad \#(\exists x_1(x_1 = m \wedge F(x_1))).$$

Thus for all $m \in \mathbb{N}$ we have that $m \in A$ if and only if $f(m) \in \mathsf{TrueSnt}$. We claim that the function $f : \mathbb{N} \to \mathbb{N}$ is primitive recursive. This is clear since

$$f(m) = 2 \cdot 3^3 \cdot 7^{2 \cdot 3 \cdot 5^{\#(x_1 = m)} \cdot 7^{\#(F(x_1))}}$$

where

$$\#(x_1 = m) = 2 \cdot 5^{45} \cdot 7^{\#(m)} ,$$

and $\#(m) = \#(\underbrace{1 + \ldots + 1}_{m})$ can be defined primitive recursively by

$$\begin{aligned} \#(0) &= 1 , \\ \#(m+1) &= 3^3 \cdot 5^{\#(m)} \cdot 7^3 . \end{aligned}$$

Thus A is reducible to $\mathsf{TrueSnt}$ via f. This proves the theorem. □

Theorem 2.3.3. $\mathsf{TrueSnt}$ is not recursive.

Proof. By Corollary 2.2.22 we have an arithmetically definable set K which is not recursive. By the previous theorem K is reducible to $\mathsf{TrueSnt}$. Hence by Lemma 1.7.8 $\mathsf{TrueSnt}$ is not recursive. □

More generally we have the following theorem, which may be paraphrased as "arithmetical truth is not arithmetically definable."

Theorem 2.3.4 (Tarski)**.** $\mathsf{TrueSnt}$ is not arithmetically definable.

Proof. Suppose that $\mathsf{TrueSnt}$ were arithmetically definable. Then by Theorem 2.2.23 we would have that $\mathsf{TrueSnt}$ belongs to the class Σ^0_n for some n. By Theorem 1.9.18, let C be a complete Σ^0_{n+1} set. By Theorem 2.2.23 C is arithmetically definable. Hence by Theorem 2.3.2 C is reducible to $\mathsf{TrueSnt}$. Hence by Lemma 1.9.16 C belongs to the class Σ^0_n. This contradicts that fact (Theorem 1.9.18) that a complete Σ^0_{n+1} set can never belong to the class Σ^0_n. This completes the proof. □

Exercise 2.3.5. Prove that the set Fml of all Gödel numbers of formulas is primitive recursive.

Exercise 2.3.6. Prove that the set Snt of all Gödel numbers of sentences is primitive recursive.

Chapter 3

The Real Number System

In Chapter 2 we have shown that $\mathsf{TrueSnt}_{\mathbb{N}}$ is nonrecursive, i.e., the theory of the natural number system is undecidable. In this Chapter we shall show that, by contrast, $\mathsf{TrueSnt}_{\mathbb{R}}$ is recursive, i.e., the theory of the real number system is decidable.

3.1 Quantifier Elimination

Let $\mathcal{L}_{OR}$ be the language of ordered rings, i.e.,

$$\mathcal{L}_{OR} = (+, -, \cdot, 0, 1, <, =)$$

where $+$ and $\cdot$ are 2-ary operation symbols, $-$ is a 1-ary operation symbol, $<$ and $=$ are 2-place predicate symbols, and 0 and 1 are constant symbols. We consider the $\mathcal{L}_{OR}$-structure

$$\mathcal{R} = (\mathbb{R}, +_{\mathbb{R}}, -_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, <_{\mathbb{R}}, =_{\mathbb{R}}),$$

i.e., the real number system, the ordered field of real numbers. Formulas of $\mathcal{L}_{OR}$ are interpreted with reference to $\mathcal{R}$, i.e., $\exists x \ldots$ means "there exists $x \in \mathbb{R}$ such that $\ldots$," etc.

Two $\mathcal{L}_{OR}$-formulas F and G are said to be *equivalent* if they have the same free variables $x_1, \ldots, x_k$ and define the same k-place predicate $P \subseteq \mathbb{R}^k$. An equivalent condition is that the sentence

$$\forall x_1 \cdots \forall x_k \, (F(x_1, \ldots, x_k) \Leftrightarrow G(x_1, \ldots, x_k))$$

is true in $\mathcal{R}$.

We are going to prove the following theorem, due originally to Tarski:

Theorem 3.1.1 (Quantifier Elimination)**.** For any $\mathcal{L}_{OR}$-formula F, we can find an equivalent quantifier-free $\mathcal{L}_{OR}$-formula F^*.

Example 3.1.2. The formula

$$\exists x\,(ax^2 + bx + c = 0)$$

is equivalent to the quantifier-free formula

$$(a = 0 \wedge b = 0 \wedge c = 0) \vee (a = 0 \wedge b \neq 0) \vee (a \neq 0 \wedge b^2 - 4ac \geq 0)\,.$$

Exercise 3.1.3. Find quantifier-free formulas in the language $+, -, \cdot, 0, 1, <, =$ which are equivalent, over the real number system $\mathbb{R}$, to:

1. $\exists x\,(ax^2 + bx + c > 0)$.
2. $\exists x\,(ax^3 + bx^2 + cx + d > 0)$.
3. $\exists x\,(ax^4 + bx^3 + cx^2 + dx + e > 0)$.

Exercise 3.1.4. Does there exist a constant c such that the following holds?

> Given a formula $F(x)$ in the language $+, \cdot, 0, 1, =$ with exactly one free variable x, we can find a formula $F^*(x)$ in the same language which is equivalent to $F(x)$ over the natural number system $\mathbb{N}$, and which contains at most c quantifiers.

Prove your answer.

Remark 3.1.5. The only properties of $\mathcal{R}$ that will be used in the proof of Theorem 3.1.1 are: (1) $\mathcal{R}$ is a commutative ordered field; and (2) $\mathcal{R}$ has the intermediate value property for polynomials, i.e.,

$$(\,x < y \,\wedge\, p(x) < 0 < p(y)\,) \;\Rightarrow\; \exists z\,(\,x < z < y \,\wedge\, p(z) = 0\,)$$

for any polynomial $p(x) \in \mathbb{R}[x]$. An ordered field with these properties is called a real closed ordered field. This is related to Hilbert's 17th Problem.

Remark 3.1.6. The proof of Theorem 3.1.1 which we shall present below is due to P. J. Cohen. In order to present the proof, we shall define and study a class of functions called the *effective* functions. This notion of effectivity has no importance beyond the proof of Theorem 3.1.1. See also Corollary 3.1.21 below.

Definition 3.1.7. A predicate A on the reals, i.e., $A \subseteq \mathbb{R}^k$, is said to be *effective* if it is definable over $\mathcal{R}$ by a quantifier-free formula. That is, A is a Boolean combination of sets in $\mathbb{R}^k$ which are defined by equations and inequations $p(x_1, \ldots, x_k) = 0$, $p(x_1, \ldots, x_k) > 0$, where $p \in \mathbb{Z}[x_1, \ldots, x_k]$.

Remark 3.1.8. If we allow parameters from $\mathbb{R}$, we get semi-algebraic sets. Thus "effective = semi-algebraic with parameters from $\mathbb{Z}$".

Definition 3.1.9. A function $f : D \to \mathbb{R}$, $D \subseteq \mathbb{R}^k$ is said to be *effective* if

1. D is effective, and

2. for every effective predicate $A(x_1, \ldots, x_k, y, z_1, \ldots, z_n)$, the predicate

$$B(x_1, \ldots, x_k, z_1, \ldots, z_n) \;\equiv\; A(x_1, \ldots, x_k, f(x_1, \ldots, x_k), z_1, \ldots, z_n)$$

is effective.

Example 3.1.10. It can be shown that the function $\sqrt{x}$ is effective. This is because, first, the domain of $\sqrt{x}$ is the effective set $\{x \in \mathbb{R} \mid x \geq 0\}$, and second, for instance, $\sqrt{x} > 3 \equiv x > 9$.

In order to prove Theorem 3.1.1, we shall build up a library of effective functions. We shall use notations such as $\overline{x}$ and $\overline{y}$ to abbreviate sequences of variables such as $x_1, \ldots, x_k$ and $y_1, \ldots, y_m$.

Lemma 3.1.11. The functions $x + y$, $x \cdot y$, $-x$ and x/y are effective.

Proof. For $x+y$, $x \cdot y$ and $-x$ there is nothing to prove. For x/y, note first that the domain is $\{(x, y) \mid y \neq 0\}$ which is obviously effective. It remains to show that if $A(z, \ldots)$ is an effective predicate then so is $A(x/y, \ldots)$. The latter is a Boolean combination of predicates of the form

$$a_n \left(\frac{x}{y}\right)^n + \ldots + a_1 \left(\frac{x}{y}\right) + a_0 \;>\; 0$$

and this is equivalent to the atomic formula

$$a_n x^n + a_{n-1} x^{n-1} y + \ldots + a_1 x y^{n-1} + a_0 y^n \;>\; 0\,,$$

assuming as we may that n is even. □

Corollary 3.1.12. Any rational function

$$f(x_1, \ldots, x_k) \;\in\; \mathbb{Q}(x_1, \ldots, x_k)$$

is effective.

Lemma 3.1.13. The composition of effective functions is effective.

Proof. Consider for instance $f(g(x))$ where f and g are effective 1-place functions. If $D(y)$ is a quantifier-free formula defining the $\mathrm{dom}(f)$, then $D(g(x))$ defines the $\mathrm{dom}(fg)$, which is therefore effective. If $A(y, \overline{z})$ is any effective predicate, then clearly $A(f(y), \overline{z})$ is effective, hence $A(f(g(x)), \overline{z})$ is effective. □

Lemma 3.1.14. The function

$$\mathrm{sgn}(x) \;=\; \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0. \end{cases}$$

is effective.

Proof. Let $A(y, \overline{z})$ be an effective predicate. Then $A(\mathrm{sgn}(x), \overline{z})$ is equivalent to

$$(x > 0 \wedge A(1, \overline{z})) \vee (x = 0 \wedge A(0, \overline{z})) \vee (x < 0 \wedge A(-1, \overline{z}))$$

which is again effective. This proves the lemma. □

More generally we have:

Lemma 3.1.15. If a function $f(\overline{x})$ takes only finitely many values, all integers, then $f(\overline{x})$ is effective if and only if for each $j \in \mathbb{Z}$, the predicate $f(\overline{x}) = j$ is effective.

Proof. If: Let $j_1, \ldots, j_n$ be the finitely many values. For any effective predicate $A(y, \overline{z})$, the predicate $A(f(\overline{x}), \overline{z})$ is equivalent to

$$(f(\overline{x}) = j_1 \wedge A(j_1, \overline{z})) \vee \cdots \vee (f(\overline{x}) = j_n \wedge A(j_n, \overline{z}))$$

and is therefore effective.

Only if: Trivial. □

Lemma 3.1.16 (Definition by Cases)**.** If two functions $f_1(\overline{x})$ and $f_2(\overline{x})$ and a predicate $A(\overline{x})$ are effective, then the function

$$f(\overline{x}) = \begin{cases} f_1(\overline{x}) & \text{if } A(\overline{x}), \\ f_2(\overline{x}) & \text{if } \neg A(\overline{x}) \end{cases}$$

is effective.

Proof. We must show that, for each effective predicate $B(y, \overline{z})$, the predicate $C(\overline{x}, \overline{z}) \equiv B(f(\overline{x}), \overline{z})$ is effective. This is so because $C(\overline{x}, \overline{z})$ is equivalent to

$$(A(\overline{x}) \wedge B(f_1(\overline{x}), \overline{z})) \vee (\neg A(\overline{x}) \wedge B(f_2(\overline{x}), \overline{z}))\,.$$

Since $f_1(\overline{x})$ and $f_2(\overline{x})$ and $B(y, \overline{z})$ are effective, $B(f_1(\overline{x}), \overline{z})$ and $B(f_2(\overline{x}), \overline{z})$ are effective. Since $A(\overline{x})$ is effective, it follows that $C(\overline{x}, \overline{z})$ is effective. This proves the lemma. □

The extension of the previous lemma to more than two cases is obvious.

Lemma 3.1.17. A function $f(\overline{x})$ is effective if and only if for every positive integer $d \geq 1$ and every polynomial $q(y) \in \mathbb{R}[y]$ of degree d, $\mathrm{sgn}(q(f(\overline{x})))$ is an effective function of $\overline{x}$ and the $d + 1$ coefficients of $q(y)$.

Proof. Only if: Trivial, since for instance

$$\mathrm{sgn}(q(f(\overline{x}))) = 1 \quad \equiv \quad q(f(\overline{x})) > 0 \quad \equiv \quad A(f(\overline{x})),$$

where $A(y)$ is the predicate $q(y) > 0$.

If: We must show that if $A(y, \overline{z})$ is effective then $A(f(\overline{x}), \overline{z})$ is effective. Note that $A(y, \overline{z})$ can be viewed as a Boolean combination of atomic predicates of the

form $p(y, \overline{z}) > 0$, for various polynomials $p(y, \overline{z})$ with coefficients in $\mathbb{Z}$. It suffices to show that the predicates $p(f(\overline{x}), \overline{z}) > 0$ are effective. In order to show this, write $p(y, \overline{z}) = q(y) \in \mathbb{Z}[\overline{z}][y]$ i.e., $q(y)$ is a polynomial in y whose coefficients are polynomials in $\overline{z}$ with integer coefficients. Then

$$p(f(\overline{x}), \overline{z}) > 0 \quad \equiv \quad \mathrm{sgn}(q(f(\overline{x}))) = 1\,.$$

By assumption $\mathrm{sgn}(q(f(\overline{x})))$ is an effective function of $\overline{x}$ and the cofficients of q; hence by composition $\mathrm{sgn}(q(f(\overline{x})))$ is an effective function of $\overline{x}$ and $\overline{z}$. □

The next lemma says that the real roots of a polynomial are effective functions of the coefficients. For example, the quadratic formula

$$x \;=\; \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

shows that the roots of $ax^2 + bx + c$ are effective functions of a, b and c.

Lemma 3.1.18 (Main Lemma)**.** Let $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$. Write $\overline{a} = a_0, \ldots, a_n$. There are $n+1$ effective functions $\xi_1(\overline{a})$, $\ldots$, $\xi_n(\overline{a})$, and $k = k(\overline{a})$ such that

$$\xi_1(\overline{a}) < \cdots < \xi_k(\overline{a})$$

are all of the real roots of $p(x)$.

Proof. By induction on n. Let

$$p'(x) \quad = \quad n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

be the derivative of $p(x)$. This is of degree $\leq n-1$. By inductive hypothesis, the roots of $p'(x)$ are among $t_1 < \cdots < t_m$, $m = n-1$, where the t_i's are effective function of $\overline{a}$. Note that $p(x)$ is monotone on each of the open intervals

$$(-\infty, t_1)\,,\ (t_1, t_2)\,,\ \ldots\,,\ (t_{m-1}, t_m)\,,\ (t_m, +\infty)$$

So, in each of these intervals, there is at most one root of $p(x)$. In addition the t_i's could be roots of $p(x)$. Thus the number of roots is determined by $\mathrm{sgn}(p(t_i))$, $1 \leq i \leq n-1$ and $\mathrm{sgn}(p'(t_1 - 1))$ and $\mathrm{sgn}(p'(t_n + 1))$. We can therefore use definition by cases to obtain $k(\overline{a})$ as an effective function of $\overline{a}$.

It remains to show that the roots themselves are effective functions of $\overline{a}$. Consider for example a root $\xi = \xi(\overline{a})$ in the interval (t_1, t_2) where $p(t_1) > 0$ and $p(t_2) < 0$. By the previous lemma, it suffices to show that, for each $d \geq 1$ and polynomial $q(x)$ of degree d, $\mathrm{sgn}(q(\xi))$ is effective (as a function of $\overline{a}$ and the coefficients of q).

Replacing $q(x)$ by its remainder on division by $p(x)$, we may assume $\deg(q(x)) < n$. [Details: Long division gives $q(x) = p(x) \cdot f(x) + r(x)$, where $\deg(r(x)) < n$ and the coefficients of $r(x)$ are effective functions of the coefficients of $p(x)$ and $q(x)$. We can replace $q(x)$ by $r(x)$.]

By induction hypothesis, the roots of $q(x)$ can be found effectively. Let the roots of $q(x)$ be among $u_1 < \cdots < u_m$. Then the sign of $q(x)$ on the $m+1$ intervals

$$(-\infty, u_1)\,,\ (u_1, u_2)\,,\ \ldots\,,\ (u_{m-1}, u_m)\,,\ (u_m, +\infty)$$

is given by $m+1$ effective functions

$$\mathrm{sgn}(q(u_1{-}1))\,,\ \mathrm{sgn}\left(q\left(\frac{u_1+u_2}{2}\right)\right)\,,\ \ldots\,,\ \mathrm{sgn}\left(q\left(\frac{u_{m-1}+u_m}{2}\right)\right)\,,\ \mathrm{sgn}(q(u_m{+}1))\,.$$

Moreover the position of ξ relative to the u_i's is determined by the positions of t_1 and t_2 relative to the u_i's and by the $\mathrm{sgn}(p(u_i))$'s. Thus we can use definition by cases to obtain $\mathrm{sgn}(q(\xi))$ as an effective function. In view of the previous lemma characterizing effective functions, this shows that ξ is an effective function. The proof of the Main Lemma is now complete. □

Lemma 3.1.19. If $A(x_1, x_2, \ldots, x_k)$ is an effective predicate, then the predicate

$$B(x_2, \ldots, x_k) \quad \equiv \quad \exists x_1\, A(x_1, x_2, \ldots, x_k)$$

is effective.

Proof. The predicate $A(x_1, x_2, \ldots, x_k)$ may be viewed as a Boolean combination of polynomial inequalities of the form $p_i(x_1) > 0$, $1 \le i \le l$, where the coefficients of the $p_i(x)$'s are polynomials in $x_2, \ldots, x_k$ with integer coefficients. By the Main Lemma, the roots of the $p_i(x)$'s are effective function of $x_2, \ldots, x_k$. Let $\xi_1, \ldots, \xi_m$ be all of these roots. Hence the $p_i(x)$'s change sign only at $\xi_1, \ldots, \xi_m$. It follows that

$$\exists x_1\, A(x_1, x_2, \ldots, x_k)$$

is equivalent to a finite disjunction

$$A(\eta_1, x_2, \ldots, x_k) \vee \cdots \vee A(\eta_n, x_2, \ldots, x_k)\,,$$

where $\eta_1, \ldots, \eta_n$ is a list of all the ξ_i's and $(\xi_i + \xi_j)/2$'s and $\xi_i \pm 1$'s. Since the η_i's are effective functions of $x_2, \ldots, x_k$, it follows that the above disjunction is an effective predicate of $x_2, \ldots, x_k$. This proves the lemma. □

Theorem 3.1.20. Any predicate $A \subseteq \mathbb{R}^k$ which is definable over $\mathcal{R}$ is effective.

Proof. $A \subseteq \mathbb{R}^k$ is defined over $\mathcal{R}$ by a formula $F(x_1, \ldots, x_k)$ of $\mathcal{L}_{OR}$. Therefore, it suffices to show that any formula F of $\mathcal{L}_{OR}$ is equivalent over $\mathcal{R}$ to a quantifier-free formula F^*. We shall prove this by induction on the number of symbols in F.

If F is quantifier-free, we may take $F^* \equiv F$.

If $F \equiv \neg G$, then we may take $F^* \equiv \neg G^*$.

If $F \equiv G \wedge H$, then we may take $F^* \equiv G^* \wedge H^*$.

If $F \equiv \exists x\, G$, let $F(\overline{y}) \equiv \exists x\, G(x, \overline{y})$, where $\overline{y}$ is a list of the free variables of F. By the inductive hypothesis, $G(x, \overline{y})$ is equivalent to a quantifier-free formula $G^*(x, \overline{y})$. Then $G^*(x, \overline{y})$ defines an effective predicate $B(x, \overline{y})$. By the

previous lemma, the predicate $A(\overline{y}) \equiv \exists x\, B(x, \overline{y})$ is effective, i.e., is defined by a quantifier-free formula $F^*(\overline{y})$. Clearly F is equivalent to F^*. This completes the proof. □

Corollary 3.1.21. For a predicate $A \subseteq \mathbb{R}^k$ the following three conditions are equivalent:

1. A is effective.
2. A is definable over $\mathcal{R}$.
3. A is definable over $\mathcal{R}$ by a quantifier-free formula.

Similarly for functions $f : D \to \mathbb{R}$, $D \subseteq \mathbb{R}^k$.

Proof. For predicates this follows immediately from Theorem 3.1.20. Consider now a function f. Note first that if f is effective then the predicate $y = f(\overline{x})$ is effective, i.e., definable by a quantifier-free formula. Conversely, suppose that f is definable. Then for any effective predicate $A(y, \overline{z})$, the predicate $A(f(\overline{x}), \overline{z})$ is equivalent to the definable predicate $\exists y\, (y = f(\overline{x}) \wedge A(y, \overline{z}))$, which is therefore effective in view of what has already been proved. Thus f is effective. □

Theorem 3.1.22 (Quantifier Elimination)**.** If a predicate $A \subseteq \mathbb{R}^k$ is definable over $\mathcal{R}$, then it is definable over $\mathcal{R}$ by a quantifier-free formula.

Proof. This is merely a restatement of the previous corollary. □

Proof of Theorem 3.1.1. Theorem 3.1.1 is a restatement of the previous theorem. □

3.2 Decidability of the Real Number System

Theorem 3.2.1. Given a formula F of $\mathcal{L}_{OR}$, there is an algorithm to find an equivalent quantifier-free formula F^*.

Proof. The algorithm can be obtained by tracing back through the proof of Theorem 3.1.22. □

Theorem 3.2.2. Given a sentence S of $\mathcal{L}_{OR}$, there is an algorithm to determine whether or not $\mathcal{R}$ satisfies S, i.e., whether S is true in the real number system.

Proof. Given a sentence S, a special case of the previous theorem is that we can algorithmically compute S^*, an equivalent quantifier-free sentence. But then S^* is a Boolean combination of atomic sentences of the form $t_1 = t_2$ and $t_1 < t_2$ where t_1 and t_2 are variable-free terms, for example $1+(0+1) < (1+1)\cdot-(1+0)$, and the truth value of such sentences is easily computed. This completes the proof. □

Corollary 3.2.3. The set

$$\mathsf{TrueSnt}_{\mathbb{R}} \;=\; \{\#(S) \mid S \text{ is a sentence} \wedge\; S \text{ is true in } \mathcal{R}\}$$

is recursive.

Proof. This follows from the previous Theorem plus Church's Thesis. Alternatively, we can convert the proof of Theorem 3.1.1 into a rigorous proof that the function taking $\#(F)$ to $\#(F^*)$ is primitive recursive. □

Exercise 3.2.4. Recall that $\mathbb{N} = \{0, 1, 2, \ldots\}$ = the natural numbers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ = the integers, and $\mathbb{R} = (-\infty, \infty)$ = the real numbers.

Show that $\mathsf{TrueSnt}_{\mathbb{N}}$ and $\mathsf{TrueSnt}_{\mathbb{Z}}$ are not recursive. (This is in contrast to the fact that $\mathsf{TrueSnt}_{\mathbb{R}}$ is recursive.)

Theorem 3.2.5. The theory of the ordered ring of real numbers is decidable.

Proof. This is a restatement of the previous corollary. □

Corollary 3.2.6. Plane and solid geometry are decidable.

Proof. By the methods of Cartesian analytic geometry, the theory of points, lines and circles in the plane is interpretable into the theory of the real numbers. For example, a *point* is an ordered pair (x, y) where x and y are real numbers. A *line* is an ordered quadruple (a, b, u, v) where $(u, v) \neq (0, 0)$. A point (x, y) *lies on* a line (a, b, u, v) if and only if

$$\exists t\, (x = a + tu \wedge y = b + tv)\,.$$

Two lines are considered identical if and only if they contain the same points. A *circle* is an ordered triple (a, b, r) where $r > 0$. A point (x, y) *lies on* a circle (a, b, r) if and only if $(x - a)^2 + (y - b)^2 = r^2$. A *triangle* consists of three non-collinear points, the vertices of the triangle. Etc., etc.

Similarly for the theory of points, lines, planes, circles, and spheres in space. □

Exercise 3.2.7. Write sentences of the language $+, -, \cdot, 0, 1, <, =$ which, when interpreted over the real number system, express the following statements of Euclidean plane geometry.

1. For every two points, there is a unique line passing through them.
2. For every three non-collinear points, there is a unique circle passing through them.
3. For every line L and circle C, the intersection of L and C consists of at most two points.
4. Given a line L and a point P, among all points on L there is exactly one which is at minimum distance from P.

5. For every circle C and point P lying on C, there exists one and only one line L such that $L \cap C = P$. (I.e., a tangent line.)

6. Every line segment has a unique midpoint.

7. Every angle can be uniquely bisected.

Exercise 3.2.8. Explain in detail how you would translate the following statements of Euclidean plane geometry into sentences of the language $+, -, \cdot, 0, 1, <, =$ over the real number system.

1. The three angle bisectors of any triangle meet in a single point.

2. Every angle can be uniquely trisected.

Exercise 3.2.9. Recall that $\mathbb{N} = \{0, 1, 2, \ldots\}$ = the natural numbers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ = the integers, and $\mathbb{R} = (-\infty, \infty)$ = the real numbers. According to Matiyasevich's Theorem, we can find a polynomial

$$f(w, x_1, \ldots, x_k)$$

with integer coefficients, such that the set of $a \in \mathbb{N}$ for which the equation $f(a, x_1, \ldots, x_k) = 0$ has a solution in $\mathbb{N}$ is noncomputable.

1. Discuss the analogous question in which "solution in $\mathbb{N}$" is replaced by "solution in $\mathbb{Z}$".

2. Discuss analogous questions in which "solution in $\mathbb{N}$" is replaced by "solution in $\mathbb{R}$".

Chapter 4

Informal Set Theory

The purpose of this chapter is to develop set theory in an informal, preaxiomatic way. A good reference for this material is *Naïve Set Theory* by P. R. Halmos.

4.1 Operations on Sets

Informally, a *set* is any collection of objects which may be regarded as a completed totality. We use capital letters X, Y, ... to denote sets. If a is any object and X is any set, we write $a \in X$ to mean that a belongs to X, and $a \notin X$ to mean that a does not belong to X. Synonyms for "belongs to" are "is an element of", "is a member of", and "is contained in".

Since a set is nothing but a collection of elements, the set itself having no further structure, it follows that two sets are equal if and only if they contain exactly the same elements. Symbolically,

$$X = Y \quad \Leftrightarrow \quad \forall a \, (a \in X \Leftrightarrow a \in Y) \, .$$

This is known as the principle of extensionality. It can be taken as a definition of equality between sets.

If $P(a)$ is any definite property that an object a may or may not have, we use the notation $\{a \mid P(a)\}$ to denote the set of all objects a which have property P, if such a set exists. (If such a set exists, it will be unique in view of extensionality.)

In order to be a set, a collection of objects must be limited in size and definite. These requirements are rather vague, but we shall try to give some explanation of what they entail. Definiteness means that any object a either belongs or does not belong to the collection, i.e., there is no third possibility. Limitedness means that the collection is in some sense not too large. The need for some limitation-of-size requirement will be shown below in connection with the Russell paradox.

One of the most basic concepts in set theory is that of one set being included in another. We say that Y is a *subset* of X, symbolically $Y \subseteq X$, if every element

of Y is an element of X, i.e.,

$$\forall a\,(a \in Y \Rightarrow a \in X)\,.$$

If $P(a)$ is any definite property as above, and if X is any set, we can form a subset $Y = \{a \in X \mid P(a)\}$, consisting of all elements a of X which have property P. Thus

$$\forall a(a \in Y \Leftrightarrow (a \in X \wedge P(a)))\,.$$

Note that any set X is itself a mathematical object and as such can be an element of another set. Indeed, given a set X, we can form a set

$$\mathcal{P}(X) \;=\; \{Y \mid Y \subseteq X\}\,,$$

called the *power set* of X, whose elements are all possible subsets of X.

We now prove a theorem which implies that not all definite collections of mathematical objects are sets. This means that some limitation-of-size principle is needed.

Theorem 4.1.1 (Russell Paradox)**.** The collection of all sets is not itself a set.

Proof. Suppose to the contrary that there were a set S consisting of all sets. Form the subset D consisting of all sets which are not members of themselves. Symbolically,

$$D = \{X \in S \mid X \notin X\}\,.$$

Then $D \in D$ if and only if $D \notin D$, a contradiction. This completes the proof. □

The Russell Paradox shows that we cannot form sets with complete freedom. Nevertheless, a wide variety of sets can be formed. Some examples of sets are $\emptyset$ (the empty set, i.e., the unique set which has no elements), $\{\emptyset\}$ (the one-element set whose unique element is the empty set), $\{\emptyset, \{\emptyset\}\}$, etc. For any objects a, b, and c, we can form the set $\{a, b, c\}$ whose elements are exactly a, b, and c. The cardinality of this set will be one, two or three depending on which of a, b, and c are equal to each other. Some examples of infinite sets are $\mathbb{N}$ (the set of natural numbers), $\mathbb{R}$ (the set of real numbers), $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathbb{R}))$, etc. Another source of examples is subsets defined by properties, for example $\{n \in \mathbb{N} \mid n \text{ is prime}\}$ and $\{X \subseteq \mathbb{R} \mid X \text{ is countably infinite}\}$. Further sets can be obtained using the set operations discussed below.

Given two objects a and b, there is an object (a, b) called the *ordered pair* of a and b. The ordered pair operation is assumed to have the following property:

$$(a, b) = (a', b') \quad \Leftrightarrow \quad (a = a' \wedge b = b')\,.$$

Given two sets X and Y, the *Cartesian product* $X \times Y$ is the set of all ordered pairs (a, b) such that $a \in X$ and $b \in Y$.

For any set X, a *function* with *domain* X is a rule f associating to each object $a \in X$ a definite, unique object $f(a)$. In this case we write $\mathrm{dom}(f) = X$ and $\mathrm{rng}(f) = \{f(a) \mid a \in X\}$. The latter is again a set, called the *range* of F.

If f is a function and Z is a set, there is a unique function $f\restriction Z$, the *restriction* of f to Z, whose domain is $\mathrm{dom}(f) \cap Z$ and such that $(f\restriction Z)(a) = f(a)$ for all a in its domain.

We write $f : X \to Y$ to mean that f is a function, $\mathrm{dom}(f) = X$, and $\mathrm{rng}(f) \subseteq Y$. The set of all such functions is denoted Y^X.

Summarizing some of the above points, we have the following binary operations on sets:

$$\begin{aligned}
X \cup Y &= \{a \mid a \in X \vee a \in Y\} && \text{(union)}\,,\\
X \cap Y &= \{a \mid a \in X \wedge a \in Y\} && \text{(intersection)}\,,\\
X \setminus Y &= \{a \mid a \in X \wedge a \notin Y\} && \text{(difference)}\,,\\
X \times Y &= \{(a,b) \mid a \in X \wedge b \in Y\} && \text{(product)}\,,\\
X^Y &= \{f \mid f : Y \to X\} && \text{(exponential)}\,.
\end{aligned}$$

By an *indexed collection* with index set I, we mean simply a function f whose domain is I. In discussing indexed collections, we use notation such as $f = \langle a_i\rangle_{i\in I}$ where $a_i = f(i)$. For example, an ordered n-tuple $\langle a_1, \ldots, a_n\rangle$ is a function whose domain is $\{1, \ldots, n\}$, and a sequence $\langle a_n\rangle_{n\in\mathbb{N}}$ is a function whose domain is $\mathbb{N}$.

Given an indexed collection of sets $\langle X_i\rangle_{i\in I}$, the following operations are defined.

$$\begin{aligned}
\textstyle\bigcup_{i\in I} X_i &= \{a \mid \exists i \in I\,(a \in X_i)\} && \text{(union)}\,,\\
\textstyle\bigcap_{i\in I} X_i &= \{a \mid \forall i \in I\,(a \in X_i)\} && \text{(intersection)}\,,\\
\textstyle\prod_{i\in I} X_i &= \{\langle a_i\rangle_{i\in I} \mid \forall i \in I\,(a_i \in X_i)\} && \text{(product)}\,.
\end{aligned}$$

If in the latter operation we take all of the sets X_i to be the same set X, we get the Cartesian power

$$\textstyle\prod_{i\in I} X \;=\; X^I$$

which is the same as the previously mentioned exponential.

The *Axiom of Choice* is the assertion that, for any indexed collection of sets $\langle X_i\rangle_{i\in I}$, if $\forall i \in I\,(X_i \neq \emptyset)$ then $\prod_{i\in I} X_i \neq \emptyset$. This implies that it is possible to choose one element $a_i \in X_i$ for each $i \in I$. In the early years of set theory, there was some controversy about the Axiom of Choice. Nowadays the Axiom of Choice is accepted as being intuitively obvious, but we shall follow the custom of indicating which proofs use it.

4.2 Cardinal Numbers

A function f is said to be *one-to-one* if for all a, $a' \in \mathrm{dom}(f)$, $a \neq a'$ implies $f(a) \neq f(a')$. Note that in this case there is an inverse function f^{-1} with $\mathrm{dom}(f^{-1}) = \mathrm{rng}(f)$ and $\mathrm{rng}(f^{-1}) = \mathrm{dom}(f)$, defined by

$$f^{-1}(b) = a \quad \Leftrightarrow \quad f(a) = b\,.$$

Definition 4.2.1. If X and Y are sets, we say X is *equinumerous* with Y, written $X \approx Y$, if there exists a one-to-one correspondence between X and Y, i.e., a one-to-one function f with $\mathrm{dom}(f) = X$ and $\mathrm{rng}(f) = Y$.

Lemma 4.2.2.

1. $X \approx X$.
2. $X \approx Y$ if and only if $Y \approx X$.
3. $X \approx Y$ and $Y \approx Z$ imply $X \approx Z$.

Proof. Straightforward. □

Because of the preceding lemma, we can associate to any set X an object $\mathrm{card}(X)$, the *cardinality* or *cardinal number* of X, in such a way that

$$X \approx Y \quad \Leftrightarrow \quad \mathrm{card}(X) = \mathrm{card}(Y)\,.$$

If X is finite, we take $\mathrm{card}(X)$ to be the number of elements in X. For infinite sets X, it is not important at this stage what sort of object the cardinal number $\mathrm{card}(X)$ is, so long as the above property holds. We use Greek letters κ, λ, μ, ν, ... to denote cardinal numbers.

Definition 4.2.3. We write $X \preccurlyeq Y$ to mean that $X \approx X_1$ for some $X_1 \subseteq Y$.

Lemma 4.2.4.

1. If $X \approx X'$ and $Y \approx Y'$, then $X \preccurlyeq Y$ if and only if $X' \preccurlyeq Y'$.
2. $X \preccurlyeq X$.
3. $X \preccurlyeq Y$ and $Y \preccurlyeq Z$ imply $X \preccurlyeq Z$.
4. $X \preccurlyeq Y$ and $Y \preccurlyeq X$ imply $X \approx Y$.
5. For all sets X and Y, either $X \preccurlyeq Y$ or $Y \preccurlyeq X$.

Proof. Parts 1, 2, and 3 are straightforward. Parts 4 and 5 will be proved later, as consequences of the Well-Ordering Theorem. Part 4 is known as the Cantor-Schroeder-Bernstein Theorem. □

We can now make the following definition for cardinal numbers: $\kappa \leq \lambda$ if and only if $X \preccurlyeq Y$ where $\kappa = \mathrm{card}(X)$ and $\lambda = \mathrm{card}(Y)$. This does not depend on the choice of X and Y, as noted in part 1 of Lemma 4.2.4. The rest of Lemma 4.2.4 implies that $\leq$ is a linear ordering of the cardinal numbers, i.e., we have:

1. $\kappa \leq \kappa$.
2. $(\kappa \leq \lambda \wedge \lambda \leq \mu) \Rightarrow \kappa \leq \mu$.
3. $(\kappa \leq \lambda \wedge \lambda \leq \kappa) \Rightarrow \kappa = \lambda$.

4. $\forall\kappa\,\forall\lambda\,(\kappa \leq \lambda \vee \lambda \leq \kappa)$.

Definition 4.2.5 (Cardinal Arithmetic)**.** For cardinal numbers $\kappa = \mathrm{card}(X)$ and $\lambda = \mathrm{card}(Y)$, we define

1. $\kappa + \lambda = \mathrm{card}(X \cup Y)$.
2. $\kappa \cdot \lambda = \mathrm{card}(X \times Y)$.
3. $\kappa^{\lambda} = \mathrm{card}(X^{Y})$.

(In the definition of $\kappa + \lambda$, it is assumed that $X \cap Y = \emptyset$.)

For example, $2^{\kappa} = \mathrm{card}(\mathcal{P}(X))$ where $\kappa = \mathrm{card}(X)$.

Theorem 4.2.6. For cardinal numbers κ, λ, and μ, we have

1. $\kappa + \lambda = \lambda + \kappa$.
2. $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$.
3. $\kappa \cdot \lambda = \lambda \cdot \kappa$.
4. $(\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$.
5. $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.
6. $\kappa^{\lambda+\mu} = \kappa^{\lambda} \cdot \kappa^{\mu}$.
7. $\kappa^{\lambda \cdot \mu} = (\kappa^{\lambda})^{\mu}$.
8. $\kappa + 0 = \kappa$, $\kappa \cdot 0 = 0$, $\kappa \cdot 1 = \kappa$.

Proof. Straightforward. □

Later we shall prove that, for infinite cardinal numbers κ and λ,

$$\kappa + \lambda \quad = \quad \kappa \cdot \lambda \quad = \quad \max(\kappa, \lambda)\,.$$

Theorem 4.2.7 (Cantor's Theorem)**.** For any cardinal number κ, we have $2^{\kappa} > \kappa$. In other words, for any set X, we have $X \preccurlyeq \mathcal{P}(X)$ and $\mathcal{P}(X) \not\preccurlyeq X$.

Proof. We have $X \preccurlyeq \mathcal{P}(X)$ via the one-to-one function $f : X \to \mathcal{P}(X)$ where $f(a) = \{a\}$. Suppose now that $\mathcal{P}(X) \preccurlyeq X$ holds. Let $g : \mathcal{P}(X) \to X$ be one-to-one. Put

$$D = \{a \in X \mid a \in \mathrm{rng}(g) \wedge a \notin g^{-1}(a)\}\,.$$

Then $g(D) \in D$ if and only if $g(D) \notin D$, a contradiction. □

Exercise 4.2.8. Define $\aleph_0 = \text{card}(\mathbb{N})$. Without using the Cantor-Schroeder-Bernstein Theorem, prove that

$$\aleph_0 = \text{card}(\mathbb{Z}) = \text{card}(\mathbb{Q})$$

and

$$2^{\aleph_0} = \text{card}(\mathbb{R}) = \text{card}(\mathbb{C}) = \text{card}([0,1]) = \text{card}([0,1] \times [0,1]).$$

Definition 4.2.9. If $\langle \kappa_i \rangle_{i \in I}$ is an indexed set of cardinal numbers, we define

1. $\sum_{i \in I} \kappa_i = \text{card}(\bigcup_{i \in I} X_i)$
2. $\prod_{i \in I} \kappa_i = \text{card}(\prod_{i \in I} X_i)$

where $\kappa_i = \text{card}(X_i)$. In the definition of $\sum_{i \in I} \kappa_i$, it is assumed that $X_i \cap X_j = \emptyset$ for all i, $j \in I$ with $i \neq j$.

Exercise 4.2.10 (König's Theorem)**.** Suppose that $\langle \kappa_i \rangle_{i \in I}$ and $\langle \lambda_i \rangle_{i \in I}$ are indexed sets of cardinal numbers with the same index set I. Show that if $\kappa_i < \lambda_i$ for all $i \in I$, then

$$\sum_{i \in I} \kappa_i \; < \; \prod_{i \in I} \lambda_i \, .$$

Remark 4.2.11. Cantor's Theorem may be viewed as the special case of König's Theorem with $\kappa_i = 1$ and $\lambda_i = 2$. The Axiom of Choice may be viewed as the special case of König's Theorem with $\kappa_i = 0$ and $\lambda_i > 0$.

4.3 Well-Orderings and Ordinal Numbers

Definition 4.3.1. Given a set A, a relation on A is a set $R \subseteq A \times A$. A *relational structure* is an ordered pair (A, R) where A is a set and $R \subseteq A \times A$. We sometimes write aRa' instead of $(a, a') \in R$.

Definition 4.3.2. Given two relational structures (A, R) and (B, S), an *isomorphism* from (A, R) to (B, S) is a one-to-one function f such that $\text{dom}(f) = A$, $\text{rng}(f) = B$, and

$$aRa' \quad \Leftrightarrow \quad f(a)Sf(a')$$

for all $a, a' \in A$. We say that (A, R) is *isomorphic* to (B, S), symbolically $(A, R) \cong (B, S)$, if there exists an isomorphism from (A, R) to (B, S).

Lemma 4.3.3.

1. $(A, R) \cong (A, R)$.
2. $(A, R) \cong (B, S)$ if and only if $(B, S) \cong (A, R)$.
3. $(A, R) \cong (B, S)$ and $(B, S) \cong (C, T)$ imply $(A, R) \cong (C, T)$.

Proof. Straightforward. □

Because of the preceding lemma, we can associate to any relational structure (A, R) a mathematical object $\text{type}(A, R)$, the *isomorphism type* of (A, R), in such a way that

$$(A, R) \cong (B, S) \quad \Leftrightarrow \quad \text{type}(A, R) = \text{type}(B, S)\,.$$

It is not important at this stage exactly what sort of mathematical object $\text{type}(A, R)$ is, so long as the above property holds.

Definition 4.3.4. A relational structure (A, R) is said to be *well-founded* if for every nonempty set $X \subseteq A$, there exists $a \in X$ such that there is no $b \in X$ with bRa. Such an a might be called an R-*minimal* element of X.

Lemma 4.3.5. A relational structure (A, R) is well-founded if and only if there is no infinite descending R-sequence. (By an infinite descending R-sequence we mean a sequence $\langle a_n \rangle_{n\in\mathbb{N}}$ such that $a_{n+1}Ra_n$ for all $n \in \mathbb{N}$.)

Proof. If $\langle a_n \rangle_{n\in\mathbb{N}}$ is an infinite descending R-sequence, then $X = \{a_n \mid n \in \mathbb{N}\}$ is a counterexample to well-foundedness of (A, R). Conversely, suppose that $X \subseteq A$ is a counterexample to well-foundedness. Then we have $X \neq \emptyset$ and $\forall a \in X\, \exists b \in X\, bRa$. By the Axiom of Choice, there is a function $f : X \to X$ such that $f(a)Ra$ for all $a \in X$. Pick an element $a_0 \in X$ and define $\langle a_n \rangle_{n\in\mathbb{N}}$ recursively by putting $a_{n+1} = f(a_n)$ for all $n \in \mathbb{N}$. This is an infinite descending R-sequence. The lemma is proved. □

Definition 4.3.6. A *linear ordering* is a relational structure (A, R) with the following properties: aRb and bRc imply aRc; and for all $a, b \in A$ exactly one of aRb, $a = b$, bRa hold. A *well-ordering* is a linear ordering which is well-founded.

Note that if (A, R) is a well-ordering and X is a nonempty subset of A, then X has an R-least element, i.e., there is a unique $a \in X$ such that aRb holds for all $b \in X$, $b \neq a$.

Definition 4.3.7. An *ordinal number* is the isomorphism type of a well-ordering.

For $n \in \mathbb{N}$, we identify n with the ordinal number which is the order type of all n-element well-orderings. Another important ordinal number is ω, the order type of $\mathbb{N}$ itself (more precisely of $(\mathbb{N}, <) = (\mathbb{N}, \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid m < n\})$). The following definition and exercise show how to generate further examples of ordinal numbers.

Definition 4.3.8. Let $\alpha = \text{type}(A, R)$ and $\beta = \text{type}(B, S)$ be ordinal numbers. We define

1. $\alpha + \beta = \text{type}(A \cup B, R \cup S \cup (A \times B))$. Here we assume that $A \cap B = \emptyset$.
2. $\alpha \cdot \beta = \text{type}(A \times B, \{((a, b), (a', b')) \mid bSb' \vee (b = b' \wedge aRa')\})$.

Thus we have operations of *ordinal addition*, $\alpha + \beta$, and *ordinal multiplication*, $\alpha \cdot \beta$. (Later we shall define an analogous operation of *ordinal exponentiation*, α^β.) Note that the commutative laws fail, for example $1 + \omega = \omega \neq \omega + 1$ and $2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega$. However, we have the following properties.

Exercise 4.3.9. Prove the following laws of ordinal arithmetic.

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
2. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
3. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
4. $\alpha + 0 = 0 + \alpha = \alpha$, $\alpha \cdot 0 = 0 \cdot \alpha = 0$, $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$.

Give an example showing the failure of $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$.

Definition 4.3.10. If (A, R) is a linear ordering, an *initial segment* of (A, R) is any subset of A of the form $\{b \mid bRa\}$, where $a \in A$. Note that

$$(\{b \mid bRa\}, \{(c, b) \mid cRb \wedge bRa\})$$

is again a linear ordering, and we sometimes identify the initial segment with this ordering.

Theorem 4.3.11 (Comparability of Well-Orderings)**.** Let (A, R) and (B, S) be well-orderings. Then exactly one of the following holds.

1. $(A, R) \cong (B, S)$;
2. $(A, R) \cong$ some initial segment of (B, S);
3. $(B, S) \cong$ some initial segment of (A, R).

Moreover, in each case, the isomorphism is unique.

Proof. We first prove that the isomorphism is unique. Suppose for instance that f_1 and f_2 are two different isomorphisms from (A, R) to (B, S) or to some initial segment of (B, S). Then $\{a \in A \mid f_1(a) \neq f_2(a)\}$ is a nonempty subset of A, so let a be its R-least element. Then $f_1(a') = f_2(a')$ for all $a'Ra$ but $f_1(a) \neq f_2(a)$, say $f_1(a)Sf_2(a)$. Then $f_1(a) \notin \mathrm{rng}(f_2)$, contradicting the fact that $\mathrm{rng}(f_2)$ is B or an initial segment of B with respect to S.

Now let f be a function with $\mathrm{dom}(f) \subseteq A$ and $\mathrm{rng}(f) \subseteq B$, defined by putting $f(a) =$ the unique $b \in B$ such that

$$(\{a' \mid a'Ra\}, \{(a'', a') \mid a''Ra' \wedge a'Ra\}) \cong (\{b' \mid b'Sb\}, \{(b'', b') \mid b''Sb' \wedge b'Sb\}),$$

provided such a b exists. If for a given $a \in A$ no such b exists, $f(a)$ is undefined. If b exists, its uniqueness follows from what we have already proved. It is clear that $a'Ra$ and $a \in \mathrm{dom}(f)$ imply $a' \in \mathrm{dom}(f)$, and $b'Rb$ and $b \in \mathrm{rng}(f)$ imply $b' \in \mathrm{rng}(f)$.

We claim that $\mathrm{dom}(f) = A$ or $\mathrm{rng}(f) = B$ or both. If not, let a be the R-least element of $A \setminus \mathrm{dom}(f)$, and let b be the S-least element of $B \setminus \mathrm{rng}(f)$. Then f is an isomorphism from $(\{a' \mid a'Ra\}, \{(a'', a') \mid a''Ra' \wedge a'Ra\})$ to $(\{b' \mid b'Sb\}, \{(b'', b') \mid b''Sb' \wedge b'Sb\})$. This implies that $a \in \mathrm{dom}(f)$, a contradiction. The claim is proved.

If both $\mathrm{dom}(f) = A$ and $\mathrm{rng}(f) = B$, then we have $(A, R) \cong (B, S)$. If $\mathrm{dom}(f) \neq A$, then letting a be the R-least element of $A \setminus \mathrm{dom}(f)$, we see that f is an isomorphism from $(\{a' \mid a'Ra\}, \{(a'', a') \mid a''Ra' \wedge a'Ra\})$ to (B, S). If $\mathrm{rng}(f) \neq B$, then letting b be the S-least element of $B \setminus \mathrm{rng}(f)$, we see that f is an isomorphism from (A, R) to $(\{b' \mid b'Sb\}, \{(b'', b') \mid b''Sb' \wedge b'Sb\})$. This completes the proof of the theorem. □

Definition 4.3.12. For ordinal numbers α and β, we define $\alpha < \beta$ to mean that $(A, R) \cong$ some initial segment of (B, S), where $\alpha = \mathrm{type}(A, R)$ and $\beta = \mathrm{type}(B, S)$. We define $\alpha \leq \beta$ to mean $\alpha < \beta \vee \alpha = \beta$.

Lemma 4.3.13. For all ordinal numbers α and β, exactly one of $\alpha < \beta$, $\alpha = \beta$, and $\beta < \alpha$ holds. Moreover $\alpha < \beta$ and $\beta < \gamma$ imply $\alpha < \gamma$.

Proof. The first part follows from comparability of well-orderings. The second part is straightforward. □

Exercise 4.3.14. For ordinal numbers α, β, γ, prove that $\alpha < \beta$ if and only if $\alpha + \gamma = \beta$ for some $\gamma > 0$.

Lemma 4.3.15. If (A, R) is a well-ordering and $B \subseteq A$, then $(B, R \cap (B \times B))$ is a well-ordering, and

$$\mathrm{type}(B, R \cap (B \times B)) \ \leq \ \mathrm{type}(A, R)\,.$$

Proof. Straightforward, using comparability of well-orderings. □

The next theorem implies that any well-ordering is isomorphic to an initial segment of the ordinal numbers.

Theorem 4.3.16. For any ordinal number α, the relational structure

$$(\{\beta \mid \beta < \alpha\}, \{(\gamma, \beta) \mid \gamma < \beta < \alpha\})$$

is a well-ordering of type α.

Proof. Let (A, R) be some fixed well-ordering of type α. Define $f : A \to \{\beta \mid \beta < \alpha\}$ by

$$f(b) \ = \ \mathrm{type}(\{c \in A \mid cRb\}, \{(d, c) \mid dRc \wedge cRb\})\,.$$

It is straightforward to verify that f is an isomorphism from (A, R) onto

$$(\{\beta \mid \beta < \alpha\}, \{(\gamma, \beta) \mid \gamma < \beta < \alpha\})\,.$$

This proves the theorem. □

Corollary 4.3.17. For any ordinal number α, there is a set $\{\beta \mid \beta < \alpha\}$ consisting of all smaller ordinal numbers.

Proof. This follows from the previous theorem. □

Lemma 4.3.18. Let X be a set of ordinal numbers. Then there is an ordinal number $\gamma = \sup X$ which is the least upper bound of X under $<$, i.e., $\forall\alpha\,(\alpha \in X \Rightarrow \alpha \leq \gamma)$ and $\forall\beta\,(\beta < \gamma \Rightarrow \exists\alpha\,(\alpha \in X \wedge \beta < \alpha))$.

Proof. Put

$$A = \{\alpha \mid \exists\beta\,(\beta \in X \wedge \alpha < \beta)\} = \bigcup_{\beta \in X} \{\alpha \mid \alpha < \beta\}\,.$$

It is straightforward to verify that

$$(A, \{(\alpha, \beta) \in A \times A \mid \alpha < \beta\})$$

is a well-ordering. Let γ be the type of this well-ordering. It is straightforward to verify that $A = \{\alpha \mid \alpha < \gamma\}$ and that $\gamma = \sup X$. □

Exercise 4.3.19. If α is an ordinal number and X is a nonempty set of ordinal numbers, show that $\alpha + \sup X = \sup\{\alpha + \beta \mid \beta \in X\}$ and $\alpha \cdot \sup X = \sup\{\alpha \cdot \beta \mid \beta \in X\}$.

Lemma 4.3.20. Let X be a nonempty set of ordinal numbers. Then X has a smallest element under $<$.

Proof. Put $\alpha = \sup X$. Then X is a nonempty subset of $\{\beta \mid \beta \leq \alpha\}$. The latter set of ordinal numbers is well-ordered under $<$, hence X has a least element. □

Theorem 4.3.21 (Burali-Forti Paradox)**.** The class Ord of all ordinal numbers is not a set.

Proof. If Ord were a set, then by the above lemmas, $(\mathrm{Ord}, <)$ would be a well-ordering. Letting α be the type of this well-ordering, we see that $(\mathrm{Ord}, <)$ would be isomorphic to an initial segment of itself, namely $(\{\beta \mid \beta < \alpha\}, \{(\gamma, \beta) \mid \gamma < \beta < \alpha\})$. This contradiction completes the proof. □

4.4 Transfinite Recursion

By a *class* we mean a collection of objects which is not necessarily a set. Every set is a class, but not every class is a set. Examples of classes which are not sets are $\mathrm{Set} = \{X \mid X \text{ is a set}\}$ and $\mathrm{Ord} = \{\alpha \mid \alpha \text{ is an ordinal}\}$. These classes are "too big" to be sets. We have seen this in connection with the Russell Paradox and the Burali-Forti Paradox.

If C is a class, then by a *function with domain* C we mean a rule F which associates to each element a of C a uniquely defined object $F(a)$. For example, although the class Ord of all ordinal numbers is not a set, we shall be interested in functions with domain Ord. The next theorem gives us a powerful method for defining such functions.

Theorem 4.4.1 (Transfinite Recursion)**.** Let $\mathcal{F}$ be the class of all functions whose domain is an initial segment of Ord. Suppose that G is a function with domain $\mathcal{F}$. Then there is a unique function F with domain Ord such that, for all ordinal numbers α,

$$F(\alpha) = G(F{\restriction}\{\beta \mid \beta < \alpha\})\,.$$

Proof. Let us say that $f \in \mathcal{F}$ is *good* if for all $\beta \in \mathrm{dom}(f)$, $f(\beta) = G(f{\restriction}\{\gamma \mid \gamma < \beta\})$. We claim that for all ordinal numbers α, there is at most one good f with $\mathrm{dom}(f) = \{\beta \mid \beta < \alpha\}$. If not, let $f_1 \neq f_2$ be two such f's. Let γ be the smallest $\beta < \alpha$ such that $f_1(\beta) \neq f_2(\beta)$. Then $f_1{\restriction}\{\beta \mid \beta < \gamma\} = f_2{\restriction}\{\beta \mid \beta < \gamma\}$, hence

$$f_1(\gamma) \;=\; G(f_1{\restriction}\{\beta \mid \beta < \gamma\}) \;=\; G(f_2{\restriction}\{\beta \mid \beta < \gamma\}) \;=\; f_2(\gamma)\,,$$

a contradiction.

Using the above claim, let f_α be the unique good f with $\mathrm{dom}(f) = \{\beta \mid \beta < \alpha\}$, if it exists. We claim that f_α exists for all α. If not, let α be the smallest counterexample. Then f_β exists for all $\beta < \alpha$, and it is easy to check that $\{(\beta, G(f_\beta)) \mid \beta < \alpha\}$ is good. This contradicts the choice of α. Thus f_α exists for all α. Define F by putting $F(\alpha) = G(f_\alpha)$ for all α. It is easy to check that $F{\restriction}\{\beta \mid \beta < \alpha\} = f_\alpha$ and that F satisfies the desired conclusions. This completes the proof. □

As an example of transfinite recursion, we define the following operations of ordinal arithmetic.

Definition 4.4.2.

1. $\alpha + \beta = \sup\{\alpha, (\alpha + \gamma) + 1 \mid \gamma < \beta\}$.
2. $\alpha \cdot \beta = \sup\{(\alpha \cdot \gamma) + \alpha \mid \gamma < \beta\}$.
3. $\alpha^\beta = \sup\{1, \alpha^\gamma \cdot \alpha \mid \gamma < \beta\}$ (assuming $\alpha > 0$).

Exercise 4.4.3. Show that parts 1 and 2 of Definition 4.4.2 agree with parts 1 and 2 of Definition 4.3.8. In the next exercise we show how to extend Definition 4.3.8 to encompass part 3 of Definition 4.4.2.

Exercise 4.4.4. Let $\alpha = \mathrm{type}(A, R)$ and $\beta = \mathrm{type}(B, S)$ be ordinal numbers. Show that $\alpha^\beta = \mathrm{type}(C, T)$ where C is the set of all $f : B \to A$ such that, for all but finitely many $b \in B$, $f(b) = a_0$, where a_0 is the R-least element of A. Here T is the set of all $(f_1, f_2) \in C \times C$ such that $f_1(b')Rf_2(b')$, where b' is the S-greatest $b \in B$ such that $f_1(b) \neq f_2(b)$.

Exercise 4.4.5. If α is an ordinal number and X is a nonempty set of ordinal numbers, show that

1. $\alpha + \sup X = \sup\{\alpha + \beta \mid \beta \in X\}$,

2. $\alpha \cdot \sup X = \sup\{\alpha \cdot \beta \mid \beta \in X\}$, and
3. $\alpha^{\sup X} = \sup\{\alpha^\beta \mid \beta \in X\}$.

Exercise 4.4.6. For ordinal numbers α, β, and γ, show that

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
2. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
3. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
4. $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$.
5. $\alpha^{\beta \cdot \gamma} = (\alpha^\beta)^\gamma$.
6. $\alpha + 0 = 0 + \alpha = \alpha$, $\alpha \cdot 0 = 0 \cdot \alpha = 0$, $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$.
7. $\alpha^0 = 1$.
8. $0^\alpha = 0$ provided $\alpha > 0$.
9. $\alpha^1 = \alpha$, $1^\alpha = 1$.

Exercise 4.4.7. Show that $\beta < \gamma$ implies the following:

1. $\alpha + \beta < \alpha + \gamma$;
2. $\alpha \cdot \beta < \alpha \cdot \gamma$ provided $\alpha > 0$;
3. $\alpha^\beta < \alpha^\gamma$ provided $\alpha > 1$.

Definition 4.4.8. A *successor ordinal* is an ordinal number of the form $\alpha + 1$. A *limit ordinal* is an ordinal number δ such that $\delta > 0$ and $\alpha + 1 < \delta$ for all $\alpha < \delta$. Examples of limit ordinals are ω and $\omega \cdot 2$.

Exercise 4.4.9. Show that $\alpha + 1$ is the smallest ordinal number $\beta > \alpha$. Show that every ordinal number is either 0, a successor ordinal, or a limit ordinal. Show that $\delta > 0$ is a limit ordinal if and only if $\delta = \sup\{\alpha \mid \alpha < \delta\}$. Show that $\delta > 0$ is a limit ordinal if and only if $\delta = \omega \cdot \alpha$ for some $\alpha > 0$.

Exercise 4.4.10. Show that the operations of ordinal arithmetic could have been defined by transfinite recursion as follows (letting δ denote a limit ordinal):

1. $\alpha + 0 = \alpha$, $\alpha + (\beta + 1) = (\alpha + \beta) + 1$, $\alpha + \delta = \sup\{\alpha + \beta \mid \beta < \delta\}$.
2. $\alpha \cdot 0 = 0$, $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$, $\alpha \cdot \delta = \sup\{\alpha \cdot \beta \mid \beta < \delta\}$.
3. $\alpha^0 = 1$, $\alpha^{\beta+1} = (\alpha^\beta) \cdot \alpha$, $\alpha^\delta = \sup\{\alpha^\beta \mid \beta < \delta\}$ (assuming $\alpha > 0$).

Exercise 4.4.11. For an ordinal number $\delta > 0$, show that the following are equivalent.

1. $\alpha + \delta = \delta$ for all $\alpha < \delta$.

2. $\alpha + \beta < \delta$ for all $\alpha, \beta < \delta$.

3. $\delta = \omega^\alpha$ for some $\alpha \leq \delta$.

An ordinal number with these properties is said to be *additively indecomposable*.

Exercise 4.4.12. Show that for any ordinal number α, there is one and only one way to write α in the form $\alpha = \alpha_1 + \cdots + \alpha_n$ where $\alpha_1 \geq \cdots \geq \alpha_n > 0$ are additively indecomposable, and $n \in \mathbb{N}$.

4.5 Cardinal Numbers, Continued

Lemma 4.5.1. Given a set X, there exists a choice function for X, i.e., a function

$$c : \mathcal{P}(X) \setminus \{\emptyset\} \to X$$

such that $c(Y) \in Y$ for all $Y \subseteq X$, $Y \neq \emptyset$.

Proof. Consider the indexed set of sets $\langle X_i \rangle_{i \in I}$, where $I = \mathcal{P}(X) \setminus \{\emptyset\}$ and $X_i = i$ for all $i \in I$. By the Axiom of Choice, $\prod_{i \in I} X_i$ is nonempty, i.e., there exists $\langle a_i \rangle_{i \in I}$ such that $a_i \in X_i$ for all $i \in I$. Putting $c(i) = a_i$ we obtain our choice function. □

Theorem 4.5.2 (Well-Ordering Theorem)**.** Given a set X, we can find a relation $R \subseteq X \times X$ such that (X, R) is a well-ordering.

Proof. We shall prove the theorem in the following equivalent formulation: For any set X, there exists an ordinal number α such that $X \approx \{\beta \mid \beta < \alpha\}$. (Neither α nor the one-to-one function from X onto $\{\beta \mid \beta < \alpha\}$ is asserted to be unique.)

Fix a choice function c for X. Fix an object a_0 such that $a_0 \notin X$. By transfinite recursion, define

$$F(\alpha) = \begin{cases} c(X \setminus \operatorname{rng}(F \restriction \{\beta \mid \beta < \alpha\})), & \text{if } X \setminus \operatorname{rng}(F \restriction \{\beta \mid \beta < \alpha\}) \neq \emptyset \\ a_0 & \text{otherwise.} \end{cases}$$

We claim that $F(\alpha) = a_0$ for some α. If not, we would have $F(\alpha) \in X$ for all α, and $F(\alpha) \neq F(\beta)$ for all $\alpha \neq \beta$. Form the set

$$Y = \operatorname{rng}(F) = \{a \in X \mid \exists \alpha (F(\alpha) = a)\}.$$

Then F^{-1} is a function with domain Y, and we have $\operatorname{rng}(F^{-1}) = \mathrm{Ord}$, hence Ord is a set. This contradiction proves the claim.

Let α be the smallest ordinal number such that $F(\alpha) = a_0$. Then $F \restriction \{\beta \mid \beta < \alpha\}$ is one-to-one, and $\operatorname{rng}(F \restriction \{\beta \mid \beta < \alpha\}) = X$. Thus $\{\beta \mid \beta < \alpha\} \approx X$. Our theorem is proved. □

Remark 4.5.3. The previous theorem shows that the Axiom of Choice implies the Well-Ordering Theorem. There is also a converse: the Well-Ordering Theorem implies the Axiom of Choice. To see this, suppose we have an indexed set of nonempty sets $\langle X_i \rangle_{i \in I}$. Put $A = \bigcup_{i \in I} X_i$. By the Well-Ordering Theorem, there exists $R \subseteq A \times A$ such that (A, R) is a well-ordering. Define $\langle a_i \rangle_{i \in I}$ by putting $a_i =$ the R-least element of X_i. Thus $\langle a_i \rangle_{i \in I} \in \prod_{i \in I} X_i$ and we have proved the Axiom of Choice from the Well-Ordering theorem.

Exercise 4.5.4. Let X be a set of sets. By a *chain within* X we mean a set $C \subseteq X$ such that for all $U, V \in C$ either $U \subseteq V$ or $V \subseteq U$. A chain within X is said to be *maximal* if it is not properly included in any other chain within X.

Use the Axiom of Choice plus transfinite recursion to prove that there exists a maximal chain within X.

Note: This is a version of Zorn's Lemma.

Definition 4.5.5. An *initial ordinal* is an ordinal number α such that, for all $\beta < \alpha$,

$$\{\gamma \mid \gamma < \alpha\} \not\approx \{\gamma \mid \gamma < \beta\}.$$

The finite ordinal numbers 0, 1, 2, ... are initial ordinals, as is the first infinite ordinal number ω. But it is easy to see that ordinal numbers such as $\omega + 1$, $\omega + 2$, ..., $\omega \cdot 2$, $\omega \cdot 2 + 1$, ... are not initial ordinals. Another simple fact worth noting is that every infinite initial ordinal is a limit ordinal.

Definition 4.5.6. For any set X, we define $|X|$ to be the smallest ordinal number α such that $X \approx \{\beta \mid \beta < \alpha\}$. (The existence of such an ordinal is a consequence of the Well-Ordering Theorem.) Clearly $|X|$ is an initial ordinal. In fact, $|X|$ is the unique initial ordinal such that $X \approx \{\beta \mid \beta < \alpha\}$.

Lemma 4.5.7. If $X \subseteq \{\beta \mid \beta < \alpha\}$, then $|X| \leq \alpha$.

Proof. Immediate from Lemma 4.3.15. □

Theorem 4.5.8. For all sets X and Y we have

$$X \approx Y \text{ if and only if } |X| = |Y|,$$

and

$$X \preccurlyeq Y \text{ if and only if } |X| \leq |Y|.$$

Proof. The first equivalence is obvious, as is the fact that $|X| \leq |Y|$ implies $X \preccurlyeq Y$. Suppose now that $X \preccurlyeq Y$. Then $X \approx Z$ for some $Z \subseteq \{\beta \mid \beta < |Y|\}$. By the previous lemma it follows that $|X| = |Z| \leq |Y|$. This completes the proof. □

Remark 4.5.9. By the previous theorem, we have $\text{card}(X) = \text{card}(Y)$ if and only if $|X| = |Y|$, and $\text{card}(X) < \text{card}(Y)$ if and only if $|X| < |Y|$. Thus we may identify cardinal numbers with initial ordinals. From now on we shall make this identification, writing $\text{card}(X) = |X|$. For instance, the finite cardinal numbers are now identified with the finite ordinal numbers, and the smallest infinite cardinal number is the same as the ordinal number ω.

Theorem 4.5.10.

1. If $X \preccurlyeq Y$ and $Y \preccurlyeq X$, then $X \approx Y$.
2. For all sets X and Y, either $X \preccurlyeq Y$ or $Y \preccurlyeq X$.

Proof. Both parts follow from the previous theorem plus the fact that $|X|$ and $|Y|$ are ordinal numbers, hence exactly one of $|X| < |Y|$, $|X| = |Y|$, $|Y| < |X|$ holds. □

4.6 Cardinal Arithmetic

We now present some basic results about the arithmetic of infinite cardinal numbers. Most of these results are easy consequences of the following lemma.

Lemma 4.6.1. For infinite cardinals κ, we have $\kappa \cdot \kappa = \kappa$.

Proof. If not, let κ be the smallest counterexample. Note that κ is an infinite initial ordinal, and $\lambda \cdot \lambda < \kappa$ for all $\lambda < \kappa$.

Put $A = \{\alpha \mid \alpha < \kappa\}$ and $R = \{(\alpha', \alpha) \mid \alpha' < \alpha < \kappa\}$. Thus (A, R) is a well-ordering of type κ. Note that $|A| = \kappa$ but every initial segment I of (A, R) has $|I| < \kappa$.

Put $B = A \times A$ and define $S \subseteq B \times B$ by

$$\begin{aligned}
&(\alpha', \beta')S(\alpha, \beta) \quad \text{if and only if} \\
&\max(\alpha', \beta') < \max(\alpha, \beta) \vee \\
&(\max(\alpha', \beta') = \max(\alpha, \beta) \wedge \alpha' < \alpha) \vee \\
&(\max(\alpha', \beta') = \max(\alpha, \beta) \wedge \alpha' = \alpha \wedge \beta' < \beta)\,.
\end{aligned}$$

It is straightforward to verify that (B, S) is a well-ordering.

If $J \subseteq B$ is any initial segment of (B, S), we have $J \subseteq I \times I$ where I is an appropriately chosen initial segment of (A, R). Thus every initial segment of (B, S) has cardinality $< \kappa$. Hence (A, R) cannot be isomorphic to an initial segment of (B, S). From comparability of well-orderings, it follows that (B, S) is isomorphic to (A, R). In particular $B \approx A$. In other words, $A \times A \approx A$, hence $\kappa \cdot \kappa = \kappa$. This completes the proof. □

Theorem 4.6.2. For infinite cardinals κ and λ, we have

$$\kappa + \lambda \;=\; \kappa \cdot \lambda \;=\; \max(\kappa, \lambda)\,.$$

Proof. Put $\mu = \max(\kappa, \lambda)$. Then by the previous lemma we have

$$\mu \;\leq\; \kappa + \lambda \;\leq\; \mu + \mu \;=\; 2 \cdot \mu \;\leq\; \mu \cdot \mu = \mu$$

and

$$\mu \;\leq\; \kappa \cdot \lambda \;\leq\; \mu \cdot \mu \;=\; \mu\,.$$

This proves the theorem. □

Theorem 4.6.3. For λ infinite and $2 \leq \kappa \leq 2^\lambda$, we have $\kappa^\lambda = 2^\lambda$.

Proof. $2^\lambda \leq \kappa^\lambda \leq (2^\lambda)^\lambda = 2^{\lambda \cdot \lambda} = 2^\lambda$. □

For any set X, let X^* be the set of finite sequences of elements of X, i.e.,

$$X^* = \{\langle a_i \rangle_{i<n} \mid n < \omega,\ a_i \in X \text{ for all } i < n\}.$$

Theorem 4.6.4. For any infinite set X, we have $|X^*| = |X|$.

Proof. Putting $\kappa = |X|$, we have $\kappa^2 = \kappa \cdot \kappa = \kappa$ and it is easy to prove by induction on n that $\kappa^n = \kappa$ for all $n \geq 1$, $n < \omega$. Hence we have

$$|X^*| \ = \ \sum_{n<\omega} \kappa^n \ = \ \omega \cdot \kappa \ = \ \kappa\,.$$

This proves the theorem. □

Definition 4.6.5. For any ordinal β we define $\beta^+ =$ the smallest initial ordinal $\kappa > \beta$. To each ordinal number α we associate an infinite initial ordinal ω_α as follows, by transfinite recursion:

1. $\omega_0 = \omega$,
2. $\omega_{\alpha+1} = \omega_\alpha^+$,
3. $\omega_\delta = \sup_{\alpha<\delta} \omega_\alpha$ for limit ordinals δ.

Remark 4.6.6. It is easy to see that $\langle \omega_\alpha \rangle_{\alpha \in \mathrm{Ord}}$ is a strictly increasing enumeration of all the infinite initial ordinals, i.e., the infinite cardinals. It follows that the class Card $= \{\kappa \mid \kappa$ is an infinite cardinal$\}$ is not a set.

Exercise 4.6.7. Prove that there exist arbitrarily large ordinals α such that $\alpha = \omega_\alpha$.

Remark 4.6.8. Although cardinals are now the same thing as initial ordinals, the notation $\aleph_\alpha = \omega_\alpha$ is sometimes used in order to maintain a notational distinction between cardinals and initial ordinals. $\aleph_\alpha$ is taken to be a cardinal, while ω_α is an initial ordinal. For example, even though $\aleph_0$ is the same thing as ω, $\aleph_0$ is thought of as the cardinality of the set of natural numbers, while ω is thought of as the order type of the natural numbers under $<$.

Theorem 4.6.9. Let $\mathbb{N}$, $\mathbb{Q}$, and $\mathbb{R}$ be the set of natural numbers, the rational numbers, and the real numbers respectively. The cardinalities of these sets are given by $|\mathbb{N}| = |\mathbb{Q}| = \aleph_0$, $|\mathbb{R}| = 2^{\aleph_0}$.

Proof. The fact that $|\mathbb{N}| = \aleph_0$ is obvious. Since $\mathbb{N} \subseteq \mathbb{Q}$ and each rational number $q \in \mathbb{Q}$ is of the form $q = \pm m/n$ for some $(m, n) \in \mathbb{N} \times \mathbb{N}$, we have

$$|\mathbb{N}| \ \leq \ |\mathbb{Q}| \ \leq \ 2 \cdot |\mathbb{N}| \cdot |\mathbb{N}| \ = \ |\mathbb{N}|$$

so $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$. For the real numbers, note first that $\mathcal{P}(\mathbb{N}) \preccurlyeq \mathbb{R}$ via the function which sends $X \subseteq \mathbb{N}$ to $\sum_{n \in X} 2/3^n$. Hence $2^{\aleph_0} \leq |\mathbb{R}|$. On the other hand, $\mathbb{R} \preccurlyeq \mathcal{P}(\mathbb{Q}) \approx \mathcal{P}(\mathbb{N})$ via the function which sends $x \in \mathbb{R}$ to $\{q \in \mathbb{Q} \mid q < x\}$. Thus $|\mathbb{R}| = 2^{\aleph_0}$. □

Exercise 4.6.10. Prove that $|\mathbb{R}^{\mathbb{N}}| = 2^{\aleph_0}$ and $|\mathbb{R}^{\mathbb{R}}| = 2^{2^{\aleph_0}}$.

The most important problem of infinite cardinal arithmetic is the *Continuum Problem*: What is the cardinality of $\mathbb{R}$? Equivalently, what is the ordinal number β such that $2^{\aleph_0} = \aleph_\beta$? By Cantor's Theorem we have $2^{\aleph_0} \geq \aleph_1$. The assertion that $2^{\aleph_0} = \aleph_1$ is known as the *Continuum Hypothesis*, or CH.

More generally, for any infinite cardinal κ, Cantor's Theorem tells us that $2^\kappa \geq \kappa^+$, and we can ask whether $2^\kappa = \kappa^+$. The assertion that $2^\kappa = \kappa^+$ for all infinite cardinals κ (equivalently, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for all ordinal numbers α) is known as the *Generalized Continuum Hypothesis*, or GCH.

Exercise 4.6.11. Prove that $2^{\aleph_0} \neq \aleph_\omega$. (Hint: Use König's Theorem.)

4.7 Some Classes of Cardinals

A cardinal is said to be *uncountable* if it is $> \aleph_0$. In this section we introduce some important classes of uncountable cardinals.

Definition 4.7.1. Let λ be an uncountable cardinal. We say that λ is a *successor cardinal* if $\lambda = \kappa^+$ for some $\kappa < \lambda$. We say that λ is a *limit cardinal* if $\kappa^+ < \lambda$ for all $\kappa < \lambda$. We say that λ is a *strong limit cardinal* if $2^\kappa < \lambda$ for all $\kappa < \lambda$.

Note that λ is a successor cardinal if and only if $\lambda = \aleph_{\alpha+1}$ for some successor ordinal $\alpha + 1$, and λ is a limit cardinal if and only if $\lambda = \aleph_\delta$ for some limit ordinal δ. The first few uncountable successor cardinals are $\aleph_1$, $\aleph_2$, ... The first uncountable limit cardinal is $\aleph_\omega$. Clearly every strong limit cardinal is a limit cardinal, and the GCH implies that every limit cardinal is a strong limit cardinal.

Lemma 4.7.2. Every uncountable cardinal is either a successor cardinal or a limit cardinal, and exactly one of these possibilities holds.

Proof. Obvious. □

Definition 4.7.3. An infinite cardinal λ is said to be *regular* if it is not the sum of fewer than λ cardinals each less than λ. In other words, for any indexed set of cardinals $\langle \kappa_i \rangle_{i \in I}$ with $|I| < \lambda$ and $\kappa_i < \lambda$ for all $i \in I$, we have $\sum_{i \in I} \kappa_i < \lambda$.

Trivially $\aleph_0$ is regular, since it is not the sum of a finite set of finite cardinals.

Theorem 4.7.4. Every uncountable successor cardinal is regular.

Proof. Let λ be an uncountable successor cardinal. Thus $\lambda = \kappa^+$ where κ is an infinite cardinal. Given an indexed set of cardinals $\langle \kappa_i \rangle_{i \in I}$, we see that $\kappa_i < \lambda$ implies $\kappa_i \leq \kappa$, also $|I| < \lambda$ implies $|I| \leq \kappa$, hence

$$\sum_{i \in I} \kappa_i \leq \sum_{i \in I} \kappa = |I| \cdot \kappa \leq \kappa \cdot \kappa = \kappa < \lambda.$$

This shows that λ is regular. □

In particular $\aleph_1$, $\aleph_2$, ... are regular. An infinite cardinal is said to be *singular* if it is not regular. The first singular cardinal is $\aleph_\omega$, since $\aleph_\omega = \sum_{n\in\mathbb{N}} \aleph_n$.

Exercise 4.7.5. Let α be an ordinal number which is $> \omega$. Show that α is a regular cardinal (i.e., a regular initial ordinal) if and only if, for every set of ordinal numbers X with $\sup X = \alpha$, we have $\text{type}(X) = \alpha$.

Definition 4.7.6. Let λ be an uncountable cardinal. The *cofinality of* λ, written $\text{cf}(\lambda)$, is the smallest cardinal κ such that $\lambda = \sum_{i\in I} \lambda_i$ for some indexed set of cardinals $\lambda_i < \lambda$, $i \in I$, with $|I| = \kappa$.

Exercise 4.7.7. Prove the following facts.

1. $\text{cf}(\lambda)$ is regular.
2. λ is regular if and only if $\text{cf}(\lambda) = \lambda$.
3. λ is singular if and only if $\text{cf}(\lambda) < \lambda$.
4. $\lambda^{\text{cf}(\lambda)} > \lambda$. (Hint: Use König's Theorem.)
5. For any infinite cardinal κ we have $\text{cf}(\mu^\kappa) > \kappa$ for all $\mu > 1$. In particular, $\text{cf}(2^\kappa) > \kappa$.

Exercise 4.7.8. Let κ be an infinite regular cardinal. Show that there exist arbitrarily large strong limit cardinals λ such that $\text{cf}(\lambda) = \kappa$. Moreover, for all such λ we have $\lambda^\mu = \lambda$ for all $\mu < \kappa$.

Exercise 4.7.9. Assuming the GCH, prove that for all infinite cardinals κ and λ we have

$$\lambda^\kappa = \begin{cases} \lambda & \text{if } \kappa < \text{cf}(\lambda), \\ \lambda^+ & \text{if } \text{cf}(\lambda) \le \kappa \le \lambda, \\ \kappa^+ & \text{if } \kappa \ge \lambda. \end{cases}$$

Definition 4.7.10. An *inaccessible cardinal* is an uncountable, regular, strong limit cardinal. A *weakly inaccessible cardinal* is an uncountable, regular, limit cardinal.

Remark 4.7.11. Clearly every inaccessible cardinal is weakly inaccessible, and the GCH implies that every weakly inaccessible cardinal is inaccessible. It can be shown that every weakly inaccessible cardinal is a fixed point of the $\aleph_\alpha$'s, i.e., such cardinals are of the form $\lambda = \aleph_\lambda$. Moreover, every strongly inaccessible cardinal has $\lambda^\kappa = \lambda$ for all $\kappa < \lambda$.

The existence of inaccessible and/or weakly inaccessible cardinals is not obvious. Indeed, we shall see later that the existence of such cardinals cannot be established using the accepted axioms of set theory.

4.8 Pure Well-Founded Sets

A set X is said to be *transitive* if, for every set Y such that $Y \in X$, we have $Y \subseteq X$.

Lemma 4.8.1. Given a set X, there is a smallest transitive set $\mathrm{TC}(X)$ including X. ($\mathrm{TC}(X)$ is called the *transitive closure* of X.)

Proof. Define $\mathrm{U}(X) = \bigcup\{Y \mid Y \in X, Y \text{ a set}\}$. By recursion on $n < \omega$ define

$$\begin{aligned} \mathrm{TC}_0(X) &= X \\ \mathrm{TC}_{n+1}(X) &= \mathrm{U}(\mathrm{TC}_n(X))\,. \end{aligned}$$

Then $\mathrm{TC}(X) = \bigcup_{n\in\mathbb{N}} \mathrm{TC}_n(X)$ is easily seen to be the smallest transitive set Y such that $Y \supseteq X$. □

For any set A, we write

$$\in|A \;=\; \{(b,a) \mid a,b \in A, a \text{ is a set}, b \in a\}\,.$$

Definition 4.8.2. A set X is said to be *well-founded* if the relational structure $(\mathrm{TC}(X), \in|\mathrm{TC}(X))$ is well-founded.

Applying Lemma 4.3.5 to the relational structure $(\mathrm{TC}(X), \in|\mathrm{TC}(X))$, we see that X is well-founded if and only if there is no infinite sequence of sets $\langle X_n\rangle_{n\in\mathbb{N}}$ with

$$X = X_0 \ni X_1 \ni \cdots \ni X_n \ni \cdots.$$

Definition 4.8.3. A set X is said to be *pure* if every element of $\mathrm{TC}(X)$ is a set. In other words, X is a pure set if not only X but also all the elements of X, elements of elements of X, ..., are sets.

By transfinite recursion we define transitive sets R_α, $\alpha \in \mathrm{Ord}$, as follows:

$$\begin{aligned} R_0 &= \emptyset \\ R_{\alpha+1} &= \mathcal{P}(R_\alpha) \\ R_\delta &= \textstyle\bigcup_{\alpha<\delta} R_\alpha \text{ for limit ordinals } \delta\,. \end{aligned}$$

By transfinite induction on $\alpha \in \mathrm{Ord}$, it is clear that $\beta < \alpha$ implies $R_\beta \in R_\alpha$, hence $\beta \leq \alpha$ implies $R_\beta \subseteq R_\alpha$.

Theorem 4.8.4. $X \in \bigcup_{\alpha\in\mathrm{Ord}} R_\alpha$ if and only if X is a pure, well-founded set.

Proof. It is straightforward to prove by transfinite induction on α that all elements of R_α are pure and well-founded. Conversely, suppose X is pure and well-founded. We claim that, for all $Y \in \mathrm{TC}(\{X\})$, there exists an ordinal number α such that $Y \in R_\alpha$. If not, let $Y \in \mathrm{TC}(\{X\})$ be $\in$-minimal such that no such α exists. For each $Z \in Y$, let $f(Z)$ be the least ordinal number β such that $Z \in R_\beta$. Put $\gamma = \sup_{Z\in Y} f(Z)$. Then $Y \subseteq R_\gamma$, hence $Y \in \mathcal{P}(R_\gamma) = R_{\gamma+1}$, a contradiction. This proves the claim. In particular, $X \in R_\alpha$ for some α. This proves the theorem. □

The class of all pure, well-founded sets is denoted V. Thus we have

$$V = \bigcup_{\alpha \in \mathrm{Ord}} R_\alpha \, .$$

If X is a pure, well-founded set, we define the *rank* of X to be the least ordinal number α such that $X \subseteq R_\alpha$. Then clearly

$$\operatorname{rank} X = \sup\{\operatorname{rank} Y + 1 \mid Y \in X\} \, .$$

Moreover, for all ordinals α we have

$$R_\alpha = \{X \mid X \text{ is a pure well-founded set of rank } < \alpha\} \, ,$$

and $\operatorname{rank} R_\alpha = \alpha$.

Exercise 4.8.5. Assuming the GCH, prove that $|R_{\omega+\alpha}| = \aleph_\alpha$ for all ordinals α.

4.9 Set-Theoretic Foundations

In the next chapter we shall begin the study of axiomatic set theory. In axiomatic studies of set theory, the set concept is usually restricted to pure, well-founded sets. This restriction tends to isolate set theory from the rest of mathematics. Nevertheless, the restriction is partially justified by the fact that many or most mathematical objects can be reconstructed or redefined as pure, well-founded sets.

For example, the natural numbers $0, 1, 2, \ldots$ are not ordinarily regarded as being sets, but within the universe of pure, well-founded sets, it is possible to define a structural replica of the natural numbers. Thus, from a certain perspective, natural numbers can be viewed as certain kinds of pure, well-founded sets.

A similar remark applies to each of following mathematical concepts: *natural number, real number, ordinal number, cardinal number, ordered pair, function.* For each concept in this list, it is possible to identify mathematical objects of the given type with certain pure, well-founded sets. The purpose of this section is to show exactly how these identifications can be made. We begin with ordered pairs and progress to functions, ordinal numbers, and real numbers.

Definition 4.9.1. For any two objects a and b, let us write

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

Thus (a, b) is a set. Note that if a and b are pure, well-founded sets, then so is (a, b).

Lemma 4.9.2. If $(a, b) = (a', b')$ then $a = a'$ and $b = b'$.

Proof. Putting $X = (a, b)$, we see that a is the unique element of $\bigcap_{Y \in X} Y$, and b is the unique element of $\bigcup_{Y \in X} Y \setminus \{a\}$ if the latter is nonempty, otherwise $b = a$. Thus a and b can be recovered from (a, b) by single-valued set-theoretic operations. The lemma follows. □

By the above lemma, we may view (a, b) as the *ordered pair* formed from a and b. From now on we shall make this identification, which is customary in pure set theory.

In an earlier section of these notes, we defined a function with domain X to be a rule associating to each $a \in X$ a unique b. In pure set theory, it is customary to replace this definition by the following, which we shall use from now on.

Definition 4.9.3. A *function* is a set of ordered pairs, f, which is single-valued, i.e.,

$$\forall a \, \forall b \, \forall c \, (((a, b) \in f \, \wedge \, (a, c) \in f) \, \Rightarrow \, b = c) \, .$$

The *domain* of f is $\mathrm{dom}(f) = \{a \mid \exists b \, ((a, b) \in f)\}$. If f is a function and $a \in \mathrm{dom}(f)$ we write $f(a) =$ the unique b such that $(a, b) \in f$.

The pure set-theoretic reconstruction of the ordinal numbers, due to von Neumann, is as follows:

Definition 4.9.4. A *von Neumann ordinal* is a transitive, pure, well-founded set A such that $(A, \in | A)$ is a well-ordering.

Note that if A is a von Neumann ordinal, then for each $b \in A$, the initial segment $B = \{a \mid a \in b\}$ is again a von Neumann ordinal.

Lemma 4.9.5. For each ordinal number α, there is a unique von Neumann ordinal A_α such that $\mathrm{type}(A_\alpha, \in | A_\alpha) = \alpha$. Moreover, the rank of A_α is α.

Proof. By transfinite recursion we define $A_\alpha = \{A_\beta \mid \beta < \alpha\}$ for all ordinals α. By transfinite induction on α, it is straightforward to verify that A_α is the unique von Neumann ordinal such that $\mathrm{type}(A_\alpha, \in | A_\alpha) = \alpha$, and that $\mathrm{rank}(A_\alpha) = \alpha$. □

Remark 4.9.6. It is customary in pure set theory to identify the ordinal number α with the von Neumann ordinal A_α. From now on we shall make this identification. Thus we have $0 = \emptyset = \{\}$, $1 = \{0\} = \{\{\}\}$, $2 = \{0, 1\} = \{\{\}, \{\{\}\}\}$, $\ldots$, $\omega = \{0, 1, 2, \ldots\} = \mathbb{N}$. Moreover, for all ordinals α we have $\alpha = \{\beta \mid \beta < \alpha\}$ and $\alpha + 1 = \alpha \cup \{\alpha\}$. Also, if X is any set of ordinals, then

$$\sup X = \bigcup X = \bigcup_{\alpha \in X} \alpha \, .$$

As for cardinal numbers, we have already seen how cardinal numbers may be identified with certain ordinal numbers, namely, the initial ordinals. Thus, we already know how to identify cardinal numbers with certain pure, well-founded sets.

Finally, we turn to the set-theoretic construction of the real number system. The construction emplys the usual factorization of a set by an equivalence relation, as per the following definitions and remark.

Definition 4.9.7. Let A be a set. An *equivalence relation* on A is a binary relation $R \subseteq A \times A$ with the following properties: aRb and bRc imply aRc; aRb implies bRa; and aRa for all $a \in A$.

Definition 4.9.8. Let R be an equivalence relation on A. For any $a \in A$ we write $[a]_R = \{b \in A \mid aRb\}$, the *equivalence class* of a with respect to R. We write $A/R = \{[a]_R \mid a \in A\}$.

Remark 4.9.9. Let R be an equivalence relation on A. Then aRb if and only if $[a]_R = [b]_R$. Moreover A/R is a partition of A, i.e., a collection of pairwise disjoint sets whose union is A.

Definition 4.9.10 (the real number system)**.** In order to define the real number system, we follow Dedekind and begin with the natural number system $(\mathbb{N}, +, \cdot, 0, 1, =, <)$.

The integers are defined by putting $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\equiv_{\mathbb{Z}}$, where $(m, n) \equiv_{\mathbb{Z}} (m', n')$ if and only if $m + n' = m' + n$. The ordered ring structure of $\mathbb{Z}$ is given by

$$\begin{aligned}
[(m,n)] +_{\mathbb{Z}} [(m',n')] &= [(m+m', n+n')] \\
[(m,n)] \cdot_{\mathbb{Z}} [(m',n')] &= [(mm'+nn', mn'+m'n)] \\
-_{\mathbb{Z}} [(m,n)] &= [(n,m)] \\
0_{\mathbb{Z}} &= [(0,0)] \\
1_{\mathbb{Z}} &= [(1,0)] \\
[(m,n)] = [(m',n')] &\Leftrightarrow m + n' = m' + n \\
[(m,n)] <_{\mathbb{Z}} [(m',n')] &\Leftrightarrow m + n' < m' + n
\end{aligned}$$

The rationals are defined by putting $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^+)/\equiv_{\mathbb{Q}}$, where $\mathbb{Z}^+ = \{b \in \mathbb{Z} \mid b > 0\}$, and $(a, b) \equiv_{\mathbb{Q}} (a', b')$ if and only if $a \cdot b' = a' \cdot b$. The ordered ring structure of $\mathbb{Q}$ is given by

$$\begin{aligned}
[(a,b)] +_{\mathbb{Q}} [(a',b')] &= [(ab' + a'b, b \cdot b')] \\
[(a,b)] \cdot_{\mathbb{Q}} [(a',b')] &= [(aa', bb')] \\
-_{\mathbb{Q}} [(a,b)] &= [(-a,b)] \\
0_{\mathbb{Q}} &= [(0,1)] \\
1_{\mathbb{Q}} &= [(1,1)] \\
[(a,b)] = [(a',b')] &\Leftrightarrow ab' = a'b \\
[(a,b)] <_{\mathbb{Q}} [(a',b')] &\Leftrightarrow ab' < a'b
\end{aligned}$$

Finally, the reals are defined by putting $\mathbb{R} = S/\equiv_{\mathbb{R}}$. Here S is defined to be the set of *Cauchy sequences* over $\mathbb{Q}$, i.e., sequences $\langle q_n \rangle_{n \in \mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ satisying

$$\forall \varepsilon > 0 \, \exists m \, \forall n \, (n > m \Rightarrow |q_m - q_n| < \varepsilon) \; .$$

And $\equiv_{\mathbb{R}}$ is the equivalence relation on S defined by putting $\langle q_n \rangle_n \equiv_{\mathbb{R}} \langle q'_n \rangle_n$ if and only if $\lim_n |q_n - q'_n| = 0$, i.e.,

$$\forall \varepsilon > 0 \, \exists m \, \forall n \, (n > m \Rightarrow |q_n - q'_n| < \varepsilon) \; .$$

The ordered ring structure of $\mathbb{R}$ is given by

$$\begin{aligned}
[\langle q \rangle_n] +_{\mathbb{R}} [\langle q'_n \rangle_n] &= [\langle q_n + q'_n \rangle_n] \\
[\langle q_n \rangle_n] \cdot_{\mathbb{R}} [\langle q'_n \rangle_n] &= [\langle q_n \cdot q'_n \rangle_n] \\
-_{\mathbb{R}} [\langle q_n \rangle_n] &= [\langle -q_n \rangle_n] \\
0_{\mathbb{R}} &= [\langle 0 \rangle_n] \\
1_{\mathbb{R}} &= [\langle 1 \rangle_n] \\
[\langle q_n \rangle_n] = [\langle q'_n \rangle_n] &\Leftrightarrow \forall \varepsilon > 0 \, \exists m \, \forall n \, (n > m \Rightarrow |q_n - q'_n| < \varepsilon) \\
[\langle q_n \rangle_n] <_{\mathbb{R}} [\langle q'_n \rangle_n] &\Leftrightarrow \exists \varepsilon > 0 \, \exists m \, \forall n \, (n > m \Rightarrow q_n + \varepsilon < q'_n)
\end{aligned}$$

Exercise 4.9.11. Show that the real number system is *complete*, i.e., every nonempty bounded subset of $\mathbb{R}$ has a least upper bound.

Remark 4.9.12. In this section we have shown how many or most mathematical objects may be redefined or reconstructed as pure, well-founded sets. In this sense, pure set theory may be said to encompass virtually all of mathematics, and one may speak of the *set-theoretic foundations* of mathematics. This is why set theory is viewed as being of fundamental or foundational importance.

Chapter 5

Axiomatic Set Theory

This chapter is an introduction to axiomatic set theory.

5.1 The Axioms of Set Theory

Definition 5.1.1. We define $\mathcal{L}_\in$, *the language of set theory*. The language contains variables $x, y, z, \ldots$. The *atomic formulas* of the language are $x = y$ and $x \in y$, where x and y are variables. Formulas are built up as usual from atomic formulas by means of propositional connectives $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$ and quantifiers $\forall$, $\exists$. The notion of *free variable* is defined as usual. A *sentence* is a formula with no free variables.

Remark 5.1.2. The standard or intended interpretation of $\mathcal{L}_\in$ is that the variables are to range over the class of pure, well-founded sets. Thus formulas and sentences are normally interpreted as making assertions about pure, well-founded sets. This standard interpretation or model of $\mathcal{L}_\in$ is sometimes known as *the real world*.

Example 5.1.3. An example of a sentence of $\mathcal{L}_\in$ is

$$\forall x \, \forall y \, (x = y \Leftrightarrow \forall u \, (u \in x \Leftrightarrow u \in y)) \, .$$

This sentence asserts the extensionality principle for pure, well-founded sets: two pure, well-founded sets are equal if and only if they contain the same pure, well-founded sets as elements.

Example 5.1.4. An example of a formula of $\mathcal{L}_\in$ is

$$\forall u \, (u \in z \Leftrightarrow (u = x \vee u = y)) \, .$$

This formula has free variables x, y, and z. It asserts that z is the unordered pair $\{x, y\}$, i.e., the set whose only elements are x and y.

As mentioned above, the standard interpretation of $\mathcal{L}_\in$ is in terms of the real world, i.e., the class of pure, well-founded sets. In later sections of this chapter, we shall consider interpretations or models of $\mathcal{L}_\in$ other than the real world. Such alternative interpretations play an essential role in axiomatic set theory.

We can expand the language $\mathcal{L}_\in$ indefinitely by introducing abbreviations. Some important abbreviations are given in the following definition.

Definition 5.1.5.

1. (unordered pair) $z = \{x, y\}$ is an abbreviation for
$$\forall u\,(u \in z \Leftrightarrow (u = x \vee u = y)).$$
2. (singleton) $z = \{x\}$ is an abbreviation for $z = \{x, x\}$.
3. (ordered pair) $z = (x, y)$ is an abbreviation for $z = \{\{x\}, \{x, y\}\}$, i.e.,
$$\exists u\,\exists v\,(u = \{x\} \wedge v = \{x, y\} \wedge z = \{u, v\}).$$
4. (subset) $x \subseteq y$ is an abbreviation for $\forall u\,(u \in x \Rightarrow u \in y)$.
5. (powerset) $z = \mathcal{P}(x)$ is an abbreviation for
$$\forall y\,(y \in z \Leftrightarrow y \subseteq x).$$
6. (union of a set of sets) $z = \bigcup x$ is an abbreviation for
$$\forall u\,(u \in z \Leftrightarrow \exists v\,(v \in x \wedge u \in v)).$$
7. (union of two sets) $z = x \cup y$ is an abbreviation for $z = \bigcup\{x, y\}$, i.e.,
$$\exists w\,(w = \{x, y\} \wedge z = \bigcup w).$$
8. (intersection of a set of sets) $z = \bigcap x$ is an abbreviation for
$$\forall u\,(u \in z \Leftrightarrow \forall v\,(v \in x \Rightarrow u \in v)).$$
9. (intersection of two sets) $z = x \cap y$ is an abbreviation for $z = \bigcap\{x, y\}$, i.e.,
$$\exists w\,(w = \{x, y\} \wedge z = \bigcap w).$$
10. (empty set) $x = \emptyset$ and $x = \{\}$ are abbreviations for $\forall u\,(u \notin x)$.

Using these abbreviations, we can write down sentences expressing some of the axioms of Zermelo-Fraenkel set theory:

Definition 5.1.6 (Some Axioms of Set Theory)**.**

1. Axiom of Extensionality: $\forall x \, \forall y \, (x = y \Leftrightarrow \forall u \, (u \in x \Leftrightarrow u \in y))$.
2. Empty Set Axiom: $\exists x \, (x = \emptyset)$.
3. Pairing Axiom: $\forall x \, \forall y \, \exists z \, (z = \{x, y\})$.
4. Union Axiom: $\forall x \, \exists z \, (z = \bigcup x)$.
5. Power Set Axiom: $\forall x \, \exists z \, (z = \mathcal{P}(x))$.
6. Axiom of Foundation: $\forall x \, (x \neq \emptyset \Rightarrow \exists u \, (u \in x \wedge u \cap x = \emptyset))$.

Most of the above axioms are self-explanatory. Only the Axiom of Foundation needs explanation. The Axiom of Foundation is an attempt to express the idea that all of the sets under consideration are well-founded. This is expressed by saying that, for all sets x, if x is nonempty then x contains an element u which is $\in$-minimal. Note that, for $u \in x$, $u \cap x = \emptyset$ means that u is $\in$-minimal among elements of x, i.e., there is no element v of x such that $v \in u$.

We now introduce some more abbreviations and axioms.

Definition 5.1.7.

1. (Cartesian product) $z = x \times y$ is an abbreviation of
$$\forall w \, (w \in z \Leftrightarrow \exists u \, \exists v \, (u \in x \wedge v \in y \wedge w = (u, v))).$$
2. (function) $\mathrm{Fcn}(f)$ is an abbreviation for a formula saying that f is a function, i.e.,
$$\forall w \, (w \in f \Rightarrow \exists x \, \exists y \, (w = (x, y))) \wedge \forall x \, \forall y \, \forall z \, (((x, y) \in f \wedge (x, z) \in f) \Rightarrow y = z) \, .$$
3. (value of a function) $y = f(x)$ is an abbreviation of
$$\mathrm{Fcn}(f) \wedge (x, y) \in f.$$
4. (domain of a function) $z = \mathrm{dom}(f)$ is an abbreviation of
$$\mathrm{Fcn}(f) \wedge \forall x \, (x \in z \Leftrightarrow \exists y \, (x, y) \in f).$$
5. (generalized Cartesian product) $z = \prod f$ is an abbreviation of
$$\mathrm{Fcn}(f) \wedge \forall g \, (g \in z \Leftrightarrow (\mathrm{dom}(g) = \mathrm{dom}(f) \wedge \forall x \, (x \in \mathrm{dom}(f) \Rightarrow g(x) \in f(x)))) \, .$$

Definition 5.1.8. The Axiom of Choice is the sentence
$$\forall f \, ((\mathrm{Fcn}(f) \wedge \forall x \, (x \in \mathrm{dom}(f) \Rightarrow f(x) \neq \emptyset)) \Rightarrow \prod f \neq \emptyset).$$

Definition 5.1.9. The Axiom of Infinity is the sentence

$$\exists z\,(\emptyset \in z \wedge \forall x\,(x \in z \Rightarrow x \cup \{x\} \in z)).$$

The purpose of the Axiom of Infinity is to assert the existence of at least one infinite set. This is accomplished by asserting the existence of a set that contains all of the sets $0 = \{\} = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, ...

We now introduce the two remaining axioms of Zermelo-Fraenkel set theory. Actually, these two so-called axioms are not individual axioms, but rather axiom schemes. An *axiom scheme* is an infinite set of axioms all of which have a common form.

Recall that, if F is a formula with free variables $x_1, \ldots, x_n$, then the *universal closure* of F is the sentence $\forall x_1 \cdots \forall x_n\, F$.

Definition 5.1.10.

1. The Comprehension Scheme is an infinite set of axioms, consisting the universal closures of all formulas of the form
$$\exists z\,\forall u\,(u \in z \Leftrightarrow (u \in x \wedge F(u)))\,,$$
where $F(u)$ is any formula in which z does not occur freely.

2. For any formula $F(u)$, we write $z = \{u \in x \mid F(u)\}$ as an abbreviation for
$$\forall u\,(u \in z \Leftrightarrow (u \in x \wedge F(u)))\,.$$

The Comprehension Scheme is our attempt to express the principle that, given a set x and a property P that particular elements of x may or may not have, there necessarily exists a set $z \subseteq x$ consisting of all elements of x which have the given property P. Since our language $\mathcal{L}_\in$ does not enable us to discuss or quantify over arbitrary properties, we restrict attention to properties that are definable, i.e., expressible by means of a formula $F(u)$. The syntactical requirement that the variable z does not occur freely in $F(u)$ is imposed in order to avoid obvious contradictions such as $z = \{u \in x \mid u \notin z\}$, the idea being that the set z should be in some sense logically subordinate to the property P.

The Comprehension Scheme is extremely useful and important. For example, given a function f, the Comprehension Scheme together with the Union, Pairing, and Power Set Axioms logically imply the existence of a set z which is the domain of f,
$$z = \mathrm{dom} f = \{x \in \bigcup\bigcup f \mid \exists y\,((x, y) \in f)\},$$
and of the generalized Cartesian product
$$\prod f = \{g \in \mathcal{PPP}(\bigcup\bigcup f \cup \bigcup\bigcup\bigcup f) \mid \mathrm{dom} g = z \wedge \forall x\,(x \in z \Rightarrow g(x) \in f(x))\}.$$

Definition 5.1.11.

1. We write $\exists!\, x$ to mean "there exists exactly one x such that". In other words, for any formula $F(x)$ in which x occurs as a free variable, $\exists!\, x\, F(x)$ is an abbreviation of
$$\exists y\,\forall x\,(F(x) \Leftrightarrow x = y)\,.$$

2. The Replacement Scheme is an infinite set of axioms, consisting of the universal closures of all formulas of the form

$$\forall u\,(u \in x \Rightarrow \exists\,!\,v\,F(u,v)) \Rightarrow \exists y\,\forall v\,(v \in y \Leftrightarrow \exists u\,(u \in x \wedge F(u,v)))\,,$$

where $F(u,v)$ is any formula in which y does not occur freely.

The Replacement Scheme is our attempt to express the principle that, given a set x and a rule associating to each element u of x a unique object v, there exists a set y consisting of all the objects v which are associated to elements of x. Since our language $\mathcal{L}_\in$ does not enable us to discuss or quantify over arbitrary rules, we restrict attention to rules that are *definable*, i.e., expressible by means of a formula $F(u,v)$. The syntactical requirement that the variable y does not occur freely in $F(u,v)$ is imposed in order to avoid obvious contradictions.

We have now introduced all of the axioms of Zermelo/Fraenkel set theory. We have, finally:

Definition 5.1.12 (Zermelo/Fraenkel Set Theory)**.** The axioms of Zermelo/Fraenkel set theory are as follows: the Axiom of Extensionality, the Empty Set Axiom, the Pairing Axiom, the Union Axiom, the Power Set Axiom, the Axiom of Foundation, the Axiom of Infinity, the Comprehension Scheme, and the Replacement Scheme. We use ZF as an abbreviation for "Zermelo/Fraenkel set theory".

Definition 5.1.13 (ZFC)**.** The axioms of ZFC consist of the axioms of ZF plus the Axiom of Choice.

The Zermelo/Fraenkel axioms together with the Axiom of Choice constitute the commonly accepted, rigorous, set-theoretic foundation of mathematics. A mathematical theorem is regarded as proved if and only if it is clear how to deduce it as a theorem of ZFC, i.e., a logical consequence[1] of the ZFC axioms. It can be shown that all of the theorems of 19th and 20th century rigorous mathematics are logical consequences of the ZFC axioms. In particular, essentially all of the results of Chapter 4 can be stated and proved as theorems of ZFC.

5.2 Models of Set Theory

As mentioned above, the intended interpretation of $\mathcal{L}_\in$ is the so-called *real world*, i.e., the class of pure, well-founded sets. However, the general notion of pure, well-founded set is rather vague. In order to study and delimit this vagueness, axiomatic set theorists frequently consider alternative interpretations of $\mathcal{L}_\in$.

One important class of interpretations of $\mathcal{L}_\in$ is given in terms of relational structures. Recall that a *relational structure* is an ordered pair (A,E) where A is a set and $E \subseteq A \times A$. Given a relational structure (A,E) and a sentence F of $\mathcal{L}_\in$, it makes sense to ask whether F is *true in* (A,E), i.e., true when the variables are interpreted as ranging over A and $x \in y$ is interpreted as xEy, i.e., $(x,y) \in E$.

[1]The notions of *theorem* and *logical consequence* that we are using here will be explained in the next section.

Examples 5.2.1. The Axiom of Extensionality is true in a particular relational structure (A, E) if and only if (A, E) is *extensional*, i.e., for all a, $b \in A$, $a \neq b$ implies $\{c \mid cEa\} \neq \{c \mid cEb\}$. Note that some relational structures are extensional and some are not. An example of an extensional relational structure is any linear ordering. An example of a nonextensional relational structure is (A, E) whenever $|A| \geq 2$ and $E = \emptyset$.

Thus a relational structure is extensional if and only if it is a model of (i.e., *satisfies*) the Axiom of Extensionality. The general point here is that any collection of sentences of $\mathcal{L}_\in$ defines a property of relational structures, namely the property of satisfying the given sentences. We formalize this in the following definition.

Definition 5.2.2. Let S be any set of sentences of $\mathcal{L}_\in$. A *model of* S is a relational structure (A, E) such that all of the sentences of S are true in (A, E). We say that S is *consistent* if there exists a model of S. If F is another sentence of $\mathcal{L}_\in$, we say that F *is a logical consequence of* S, written $S \vdash F$, if F is true in every model of S.

Note that if S is inconsistent then all sentences are logical consequences of S, so the notion of logical consequence is uninteresting in this case. If however S is consistent, then it is meaningful to ask which sentences are logical consequences of S, i.e., what conclusions follow when the sentences of S are assumed as axioms. This is the kind of question which axiomatic set theory seeks to answer. Naturally the focus is on sets of sentences which make assertions that could reasonably be true in the intended model, i.e., the real world, i.e., the class of all pure, well-founded sets.

As an easy example of the notion of logical consequence, note that the sentence $\forall x\,(x \notin x)$ is a logical consequence of the Axiom of Foundation plus the Pairing Axiom. This is so because $x \in x$ would imply that $\{x\}$ has no $\in$-minimal element.

Specializing Definition 5.2.2 to $S = \text{ZF}$ and $S = \text{ZFC}$, we have:

Definition 5.2.3. A *model of* ZFC is a relational structure (A, E) such that (A, E) satisfies all of the Zermelo/Fraenkel axioms plus the Axiom of Choice. A *theorem of* ZFC is any sentence which is a logical consequence of the ZFC axioms. The notions *model of* ZF and *theorem of* ZF are defined similarly.

Axiomatic set theory is essentially the study of models of ZF and of ZFC, with an eye to discovering which set-theoretic propositions follow or do not follow from these axiom systems. For instance, one of the important results[2] of axiomatic set theory is that there exists a model of ZF which is not a model of ZFC. In other words, the Axiom of Choice is not a logical consequence of the ZF axioms. Another key result is that both the Continuum Hypothesis and its negation are consistent with ZFC. In other words, CH is *independent* of ZFC. Thus the ZFC axioms, although powerful and flexible, do not suffice to answer basic set-theoretic questions such as the Continuum Problem.

[2]This result will not be proved here.

We end this section by presenting some general definitions and results concerning relational structures.

Definition 5.2.4. Let (A, E) be a relational structure. A k-place predicate $P \subseteq A^k$ is said to be *definable over* (A, E) if there exists a formula $F(x_1, \ldots, x_k, y_1, \ldots, y_m)$ of $\mathcal{L}_\in$ and parameters $b_1, \ldots, b_m \in A$ such that

$$P \;=\; \{\langle a_1, \ldots, a_k\rangle \in A^k \mid (A, E) \text{ satisfies } F(a_1, \ldots, a_k, b_1, \ldots, b_m)\}\,. \qquad (5.1)$$

More generally, given $B \subseteq A$, we say that $P \subseteq A^k$ is *definable over* (A, E) *allowing parameters from* B if there exists a formula

$$F(x_1, \ldots, x_k, y_1, \ldots, y_m)$$

of $\mathcal{L}_\in$ and parameters $b_1, \ldots, b_m \in B$ such that (5.1) holds.

Definition 5.2.5. Let (A, E) be a relational structure. Then $\mathrm{Def}((A, E))$ is the set of all subsets of A that are definable over (A, E). Note that $\mathrm{Def}((A, E)) \subseteq \mathcal{P}(A)$.

Lemma 5.2.6. Let (A, E) be a relational structure.

1. If A is finite, then $\mathrm{Def}((A, E)) = \mathcal{P}(A)$ and $|\mathrm{Def}((A, E)| = 2^{|A|}$.
2. If A is infinite, then $|\mathrm{Def}((A, E))| = |A|$.

Proof. For finite A the result is obvious. Suppose now that A is infinite. By Gödel numbering, the set of all formulas of $\mathcal{L}_\in$ is countable. Since any element of $\mathrm{Def}((A, E))$ is determined by a formula and a finite sequence of parameters from A, we have

$$|\mathrm{Def}((A, E))| \;\leq\; \aleph_0 \cdot |A^*| \;=\; |A|\,.$$

On the other hand $\{\{a\} \mid a \in A\} \subseteq \mathrm{Def}((A, E))$, hence $|A| \leq |\mathrm{Def}((A, E))|$. This completes the proof. □

Definition 5.2.7. Let (A, E) and (A', E') be relational structures. We say that (A', E') *is a substructure of* (A, E), abbreviated $(A', E') \subseteq (A, E)$, if $A' \subseteq A$ and $E' = E \cap (A' \times A')$. We say that (A', E') *is an elementary substructure of* (A, E), abbreviated $(A', E') \subseteq_{\mathrm{elem}} (A, E)$, if $(A', E') \subseteq (A, E)$ and, for all formulas $F(x_1, \ldots, x_n)$ and $a_1, \ldots, a_n \in A'$, (A, E) satisfies $F(a_1, \ldots, a_n)$ if and only if (A', E') satisfies $F(a_1, \ldots, a_n)$.

Lemma 5.2.8. Given $(A', E') \subseteq (A, E)$, we have $(A', E') \subseteq_{\mathrm{elem}} (A, E)$ if and only if every nonempty subset of A which is definable over (A, E) allowing parameters from A' has a nonempty intersection with A'.

Proof. Straightforward. □

Recall that a relational structure (A, E) is said to be *countable* if the underlying set A is countable.

Theorem 5.2.9 (Löwenheim/Skolem Theorem)**.** For any relational structure (A, E), there exists a countable elementary substructure $(A', E') \subseteq_{\text{elem}} (A, E)$.

Proof. Let $c : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ be a choice function for A. We define recursively a sequence of sets $A_n \subseteq A$, $n \in \mathbb{N}$, by $A_0 = \emptyset$, $A_{n+1} = \{c(X) \mid \emptyset \neq X \subseteq A \wedge X$ is definable over (A, E) allowing parameters from $A_n\}$. Note that $A_n \subseteq A_{n+1}$ for all n. By induction on n it is straightforward to show that A_n is countable for all n. Hence $A' = \bigcup\{A_n \mid n \in \mathbb{N}\}$ is countable. Moreover $c(X) \in A'$ for all $X \neq \emptyset$ definable over (A, E) allowing parameters from A'. Hence by Lemma 5.2.8 we have $(A', E') \subseteq_{\text{elem}} (A, E)$, where $E' = E \cap (A' \times A')$. This completes the proof. □

Corollary 5.2.10 (Skolem Paradox)**.** If ZFC is consistent, then there exists a countable model of ZFC.

Proof. Assume that ZFC is consistent. Then there exists a model (A, E) of ZFC. By Theorem 5.2.9 (A, E) has a countable elementary submodel, (A', E'). Then (A', E') is a countable model of ZFC. □

The Skolem Paradox is called a paradox for the following reason: the existence of a countable model of ZFC would seem to contradict the fact that the existence of uncountable sets is a theorem of ZFC. Actually, there is no contradiction here, because a set that is uncountable within a particular model (A, E) may be countable in the real world. In other words, the notion of countability is relative to the model under consideration (as are many other set-theoretic notions).

A straightforward generalization of Theorem 5.2.9 is:

Theorem 5.2.11 (Generalized Löwenheim-Skolem Theorem)**.** Let κ be an infinite cardinal. Let (A, E) be a relational structure such that $|A| \geq \kappa$, and let $X \subseteq A$ be a subset of A such that $|X| \leq \kappa$. Then there exists an elementary substructure (A', E') of (A, E) such that $X \subseteq A'$ and $|A'| = \kappa$.

Proof. Straightforward. □

Exercise 5.2.12. Prove Theorem 5.2.11.

5.3 Transitive Models and Inaccessible Cardinals

In this section we study an important class of models. Recall that a set T is *transitive* if and only if every element of T is a subset of T.

Definition 5.3.1. Let S be a set of sentences of $\mathcal{L}_\in$. A *transitive model of* S is any transitive, pure, well-founded set T such that the relational structure $(T, \in|T)$ satisfies all the sentences of S. In this context it is customary to identify the transitive set T with the relational structure $(T, \in|T)$.

Note that every transitive model is well-founded and extensional. The following theorem provides a converse and thereby characterizes transitive models up to isomorphism among arbitrary models.

Theorem 5.3.2. Let (A, E) be a relational structure which is well-founded and extensional. Then there exists a transitive, pure, well-founded set T such that the relational structures (A, E) and $(T, \in|T)$ are isomorphic. Moreover the transitive set T and the isomorphism $f : (A, E) \cong (T, \in|T)$ are unique.

Proof. Fix an object $a_0 \notin A$. By transfinite recursion on the rank of an arbitrary pure, well-founded set x, define $F(x)$ as follows: $F(x) =$ the unique $a \in A$ such that $\mathrm{rng}(F\restriction x) = \{b \mid bEa\}$ if such an a exists; $F(x) = a_0$ otherwise. Note that $F(x) = F(y) \in A$ implies $x = y$. Hence $T = \mathrm{rng}(F^{-1}\restriction A)$ is a set. It is easy to verify that T is a transitive, pure, well-founded set and that $F\restriction T$ is an isomorphism of $(T, \in|T)$ onto (A, E). Hence $f = F^{-1}\restriction A$ is an isomorphism of (A, E) onto $(T, \in|T)$. It is straightforward to verify that T and f are unique. □

Corollary 5.3.3. If (A, E) is a relational structure, then the following assertions are equivalent:

1. (A, E) is isomorphic to some transitive model $(T, \in|T)$;
2. (A, E) is well-founded and extensional.

The rest of this section is devoted to the study of transitive models, i.e., relational structures of the form $(A, \in|A)$ where T is a transitive, pure, well-founded set. The following definition concerning transitive models is of general interest.

Definition 5.3.4. Let T be any transitive, pure, well-founded set. A k-place predicate $P \subseteq T^k$ is said to be *definable over* T if and only if it is definable over $(T, \in|T)$ (allowing parameters from T). We write

$$\mathrm{Def}(T) \;=\; \mathrm{Def}((T, \in|T)) \;=\; \{X \subseteq T \mid X \text{ is definable over } T\}\,.$$

Of particular interest are transitive models of ZFC. The following lemma consists of some simple remarks characterizing which transitive models satisfy which axioms of ZFC.

Lemma 5.3.5. Let T be a transitive, pure, well-founded set.

1. T always satisfies the Axiom of Extensionality.
2. T always satisfies the Axiom of Foundation.
3. T satisfies the Pairing Axiom if and only if T is closed under pairing, i.e.,

$$\forall a\, \forall b\, ((a \in T \wedge b \in T) \Rightarrow \{a, b\} \in T).$$

4. T satisfies the Union Axiom if and only if T is closed under union, i.e.,

$$\forall a\,(a \in T \Rightarrow \bigcup a \in T).$$

5. T satisfies the Empty Set Axiom if and only if $\emptyset \in T$.

6. T satisfies the Axiom of Infinity if and only if $\exists a\,(a \in T \wedge \omega \subseteq a)$.

7. T satisfies the Power Set Axiom if and only if

$$\forall a\,(a \in T \Rightarrow \mathcal{P}(a) \cap T \in T).$$

8. T satisfies the Axiom of Choice if and only if, for every indexed family of nonempty sets $\langle a_i \rangle_{i \in I} \in T$, we have $T \cap \prod_{i \in I} a_i \neq \emptyset$.

9. T satisfies the Comprehension Scheme if and only if, for all $X \in \mathrm{Def}(T)$, we have

$$\forall a\,(a \in T \Rightarrow a \cap X \in T).$$

10. T satisfies the Replacement Scheme if and only if for all functions $F : T \to T$ such that $F \in \mathrm{Def}(T)$, we have

$$\forall a\,(a \in T \Rightarrow \mathrm{rng}(F \restriction a) \in T).$$

Proof. Straightforward. □

We shall now show that inaccessible cardinals give rise to transitive models of ZFC. Recall that an *inaccessible cardinal* is a regular, uncountable, strong limit cardinal. Recall also that we have identified cardinals with initial von Neumann ordinals (cf. Sections 4.4.5 and 4.4.8).

Lemma 5.3.6. Let δ be a limit ordinal $> \omega$. Then R_δ is a transitive model of all of the ZFC axioms except possibly the Replacement Scheme.

Proof. We apply Lemma 5.3.5. The Axioms of Extensionality and Foundation hold in R_δ because R_δ is a transitive, pure, well-founded set. The Empty Set, Power Set, Pairing, and Union Axioms and the Axiom of Choice and the Comprehension Scheme hold in R_δ because δ is a limit ordinal. The Axiom of Infinity holds in R_δ because $\omega \in R_\delta$, since $\omega < \delta$. □

Lemma 5.3.7. An infinite cardinal λ is regular if and only if, for all $X \subseteq \lambda$, $|X| < \lambda$ implies $\sup X < \lambda$.

Proof. Straightforward. □

Lemma 5.3.8. If λ is an inaccessible cardinal, then

1. $\forall x\,((x \subseteq R_\lambda \wedge |x| < \lambda) \Rightarrow x \in R_\lambda)$.

2. $\forall x\,(x \in R_\lambda \Rightarrow |x| < \lambda)$.

3. $|R_\lambda| = \lambda$.

Proof. 1. Define $\rho : x \to \lambda$ by $\rho(u) = \text{rank}(u)$. Then $|\text{rng}\rho| \leq |x| < \lambda$. Since λ is regular, it follows by the previous lemma that $\sup(\text{rng}\rho) < \lambda$, say $\text{rng}\rho \subseteq \alpha < \lambda$. Hence $x \subseteq R_\alpha$, hence $x \in R_{\alpha+1} \subseteq R_\lambda$ since λ is a limit ordinal.

2. By transfinite induction on $\alpha < \lambda$ we prove $|R_\alpha| < \lambda$. We have $R_0 = \emptyset$. If $|R_\alpha| = \kappa < \lambda$, then $|R_{\alpha+1}| = |\mathcal{P}(R_\alpha)| = 2^\kappa < \lambda$ since λ is a strong limit cardinal. For limit ordinals $\delta < \lambda$, we have inductively $|R_\delta| = |\bigcup_{\alpha<\delta} R_\alpha| = \sup_{\alpha<\delta} |R_\alpha| < \lambda$, since $|R_\alpha| < \lambda$ and λ is regular.

3. $|R_\lambda| = \sup_{\alpha<\lambda} |R_\alpha| = \lambda$. □

Theorem 5.3.9. Let λ be an inaccessible cardinal. Then R_λ is a transitive model of ZFC.

Proof. Clearly λ is a limit ordinal $> \omega$, hence by Lemma 5.3.6 we see that R_λ satisfies all of the ZFC axioms except possibly the Replacement Scheme.

Let $F : R_\lambda \to R_\lambda$ and $a \in R_\lambda$ be given. Then $\text{rng}(F\restriction a) \subseteq R_\lambda$ and $|\text{rng}(F\restriction a)| \leq |a| < \lambda$, hence by the previous lemma $\text{rng}(F\restriction a) \in R_\lambda$. Specializing this to the case when F is definable over R_λ, we see by Lemma 5.3.5 that the Replacement Scheme holds in R_λ. This completes the proof. □

Corollary 5.3.10. If there exists an inaccessible cardinal, then ZFC is consistent.

Proof. Immediate from the theorem. □

Exercise 5.3.11. A *hereditarily finite set* is a finite set x such that all elements of x, elements of elements of x, ..., are finite sets. Show that R_ω is the set of all hereditarily finite, pure, well-founded sets. Show that R_ω is a model of all of the axioms of ZFC except the Axiom of Infinity.

Exercise 5.3.12. Define $E \subseteq \mathbb{N}$ by putting mEn if and only if 2^m occurs in the binary expansion of n, i.e., $m = n_i$ for some i where $n = 2^{n_1} + \cdots + 2^{n_k}$.

1. Show that $(\mathbb{N}, E) \cong (R_\omega, \in|R_\omega)$.
2. Conclude that $P \subseteq \omega^k$ is definable over R_ω if and only if P is arithmetical.

Theorem 5.3.13. If there exists an inaccessible cardinal, then the existence of an inaccessible cardinal is not a theorem of ZFC.

Proof. Assume that there exists an inaccessible cardinal. Let λ be the smallest inaccessible cardinal. By the previous theorem, R_λ is a model of ZFC. We claim that R_λ also satisfies "inaccessible cardinals do not exist". To see this, suppose that R_λ satisfies "there exists at least one inaccessible cardinal". Let $\kappa \in R_\lambda$ be such that R_λ satisfies "κ is an inaccessible cardinal". Then it is easy to see that κ is also an inaccessible cardinal in the real world. But clearly $\kappa < \lambda$. This contradicts the choice of λ. Thus R_λ is a model of ZFC + "inaccessible cardinals do not exist". □

The previous theorem shows that, if we assume only the axioms of ZFC, then we cannot hope to prove the existence of inaccessible cardinals.

Exercise 5.3.14. Show that, if two or more inaccessible cardinals exist, then the existence of two or more inaccessible cardinals is not a theorem of ZFC + "there exists at least one inaccessible cardinal".

Theorem 5.3.15. If there exists an inaccessible cardinal, then there exists a countable, transitive model of ZFC.

Proof. Let λ be an inaccessible cardinal. Then $(R_\lambda, \in | R_\lambda)$ is a model of ZFC. By the Löwenheim-Skolem Theorem, there exists a countable set $A \subseteq R_\lambda$ such that $(A, \in | A)$ is an elementary submodel of $(R_\lambda, \in | R_\lambda)$. Thus $(A, \in | A)$ is a countable, well-founded, extensional model of ZFC. By Theorem 5.3.2, $(A, \in | A)$ is isomorphic to a transitive model $(T, \in | T)$. Thus $(T, \in | T)$ is a countable, transitive model of ZFC. □

Exercise 5.3.16. Let λ be an inaccessible cardinal. Prove that there exists a limit ordinal $\delta < \lambda$ such that $(R_\delta, \in | R_\delta)$ is an elementary submodel of $(R_\lambda, \in | R_\lambda)$.

5.4 Constructible Sets

Recall that, if T is any transitive, pure, well-founded set, $\mathrm{Def}(T)$ is the set of all subsets of T that are definable over T (i.e., over $(T, \in | T)$) allowing parameters from T.

Definition 5.4.1. By transfinite recursion we define L_α, $\alpha \in \mathrm{Ord}$, as follows:

$$\begin{aligned} L_0 &= \emptyset \\ L_{\alpha+1} &= \mathrm{Def}(L_\alpha) \\ L_\delta &= \textstyle\bigcup_{\alpha<\delta} L_\alpha \qquad \text{for limit ordinals } \delta\,. \end{aligned}$$

A set X is said to be *constructible* if $X \in L_\alpha$ for some ordinal α. The class of all constructible sets is denoted L.

Lemma 5.4.2. For all ordinals α, L_α is a transitive, pure, well-founded set, and $L_\alpha \subseteq R_\alpha$.

Proof. For any transitive, pure, well-founded set T, we have $T \subseteq \mathrm{Def}(T) \subseteq \mathcal{P}(T)$ and hence $\mathrm{Def}(T)$ is again a transitive, pure, well-founded set. With these observations, the lemma follows easily by transfinite induction on α. □

Lemma 5.4.3. For all ordinals α, we have $\alpha = L_\alpha \cap \mathrm{Ord}$.

Proof. If T is any transitive, pure, well-founded set, then for any $a \in T$ we have that a is an ordinal (i.e., a von Neumann ordinal) if and only if T satisfies "a is transitive and $(a, \in | a)$ is a linear ordering". Thus $T \cap \mathrm{Ord} \in \mathrm{Def}(T)$. With this observation, the lemma follows easily by transfinite induction on (von Neumann) ordinals α. □

We are going to show that the constructible sets form a model of ZFC.

Some of the axioms of ZFC are straightforwardly verified in L using Lemma 5.3.5. For instance, the Union Axiom holds in L because $x \in L_\alpha$ implies $\bigcup x \in L_\alpha$. The Pairing Axiom holds in L because $x, y \in L_\alpha$ implies $\{x, y\} \in L_{\alpha+1}$. The Empty Set Axiom holds in L because $\emptyset \in L_1$. The Axiom of Infinity holds in L because $\omega \in L_{\omega+1}$. The Axioms of Extensionality and Foundation hold in L because L is transitive and consists of pure, well-founded sets.

To show that the Power Set Axiom holds in L, let X be any constructible set. For each $Y \in \mathcal{P}(X) \cap L$ put $\rho(Y) =$ the least β such that $Y \in L_\beta$. Put $\alpha = \sup\{\rho(Y) \mid Y \in \mathcal{P}(X) \cap L\}$. Thus $\mathcal{P}(X) \cap L \subseteq L_\alpha$. Hence $\mathcal{P}(X) \cap L$ is definable over L_α; namely, it is the set of all $Y \in L_\alpha$ such that L_α satisfies $Y \subseteq X$. Hence $\mathcal{P}(X) \cap L \in \mathrm{Def}(L_\alpha) = L_{\alpha+1}$. We have now shown that for all $X \in L$, $\mathcal{P}(X) \cap L \in L$. From this it follows by Lemma 5.3.5 that the Power Set Axiom holds in L.

To show that Comprehension and Replacement hold in L, we shall need the following lemmas.

Lemma 5.4.4. Let $f_1, \ldots, f_k$ be functions from Ord to Ord. Then there exist arbitrarily large ordinals α such that α is closed under $f_1, \ldots, f_k$, i.e., $f_i(\beta) < \alpha$ for all $\beta < \alpha$, $1 \leq i \leq k$.

Proof. Given an ordinal γ, define an increasing sequence of ordinals α_n, $n \in \mathbb{N}$ inductively by $\alpha_0 = \gamma$, $\alpha_{n+1} = \max(\alpha_n + 1, \sup\{f_i(\beta) \mid \beta < \alpha_n, 1 \leq i \leq k\})$. Putting $\alpha = \sup\{\alpha_n \mid n \in \mathbb{N}\}$ we see that $\alpha > \gamma$ and α is closed under $f_1, \ldots, f_k$. □

Lemma 5.4.5 (reflection)**.** Let $F(x_1, \ldots, x_n)$ be a formula of $\mathcal{L}_\in$ with free variables $x_1, \ldots, x_n$. Then there exist arbitrarily large ordinals α such that, for all $a_1, \ldots, a_n \in L_\alpha$, L satisfies $F(a_1, \ldots, a_n)$ if and only if L_α satisfies $F(a_1, \ldots, a_n)$.

Proof. Replacing $\forall$ by $\neg\exists\neg$ as necessary, we may safely assume that F contains no occurrences of $\forall$. Now let $\exists y\, G_i$, $i = 1, \ldots, k$ be a list of the subformulas of F of the form $\exists y\, G$. Write $G_i \equiv G_i(y, x_{i1}, \ldots, x_{in_i})$ where $x_{i1}, \ldots, x_{in_i}$ are the free variables of $\exists y\, G_i$. For $a_1, \ldots, a_{n_i} \in L$, put $g_i(a_1, \ldots, a_{n_i}) =$ the least ordinal β such that $a_1, \ldots, a_{n_i} \in L_\beta$ and such that, if L satisfies $\exists y\, G_i(y, a_1, \ldots, a_{n_i})$, then L satisfies $G_i(b, a_1, \ldots, a_{n_i})$ for some $b \in L_\beta$. Define $f_i : \mathrm{Ord} \to \mathrm{Ord}$ by $f_i(\beta) = \sup\{g_i(a_1, \ldots, a_{n_i}) \mid a_1, \ldots, a_{n_i} \in L_\beta\}$. By the previous lemma, there exist arbitrarily large ordinals α such that that α is closed under $f_1, \ldots, f_k$. It is straightforward to verify that such an α has the desired property. □

Remark 5.4.6. The proof of the previous lemma used only the following properties of the constructible hierarchy: $\alpha \leq \beta$ implies $L_\alpha \subseteq L_\beta$; and $L_\delta = \bigcup_{\alpha<\delta} L_\alpha$ for limit ordinals δ. Since the R_α hierarchy also has these properties, the same lemma holds for the R_α hierarchy as well. This has the following interesting consequence: If $F_1, \ldots, F_k$ is a finite set of sentences that are true in the real world, then there exist arbitrarily large ordinals α such that $F_1, \ldots, F_k$ are true in R_α.

Lemma 5.4.7. L satisfies the Comprehension and Replacement Schemes.

Proof. To show that the Replacement Scheme holds in L, let $f : L \to L$ be a function which is definable over L. We must prove that, for all $a \in L$, $\mathrm{rng}(f\restriction a) = \{f(u) \mid u \in a\}$ also belongs to L. Note first that, since f is definable over L, we have parameters $c_1, \ldots, c_n \in L$ and a formula $F(u, v, z_1, \ldots, z_n)$ with free variables $u, v, z_1, \ldots, z_n$ such that, for all $u \in L$, $f(u) =$ the unique $v \in L$ such that L satisfies $F(u, v, c_1, \ldots, c_n)$. Now given $a \in L$, put $b = \mathrm{rng}(f\restriction a)$. We must show that $b \in L$. Let β be an ordinal so large that $a, c_1, \ldots, c_n \in L_\beta$ and $b \subseteq L_\beta$. By Reflection, let α be such that $\alpha > \beta$ and, for all $u, v \in L_\alpha$, L satisfies $F(u, v, c_1, \ldots, c_n)$ if and only if L_α satisfies $F(u, v, c_1, \ldots, c_n)$. We claim that b is definable over L_α. This is clear since

$$\begin{aligned} b &= \{v \in L \mid L \text{ satisfies } \exists u\,(u \in a \wedge F(u, v, c_1, \ldots, c_n))\} \\ &= \{v \in L_\alpha \mid L_\alpha \text{ satisfies } \exists u\,(u \in a \wedge F(u, v, c_1, \ldots, c_n))\}\,. \end{aligned}$$

Thus $b \in \mathrm{Def}(L_\alpha) = L_{\alpha+1}$, whence $b \in L$. This shows that the Replacement Scheme holds in L. The proof that the Comprehension Scheme holds in L is similar. □

We introduce some more abbreviations:

Definition 5.4.8.

1. $\mathrm{Const}(x)$ is an abbreviation for a formula asserting that a given pure, well-founded set x is constructible. In more detail, $\mathrm{Const}(x)$ asserts the existence of a transfinite sequence of sets $\langle L_\beta \rangle_{\beta \leq \alpha}$ such that $L_\beta = \bigcup\{\mathrm{Def}(L_\gamma) \mid \gamma < \beta\}$ for all $\beta \leq \alpha$, and $x \in L_\alpha$.

2. Recall that V is the class of all pure, well-founded sets, and L is the class of all constructible sets. We use $V = L$ to abbreviate $\forall x\, \mathrm{Const}(x)$. Thus $V = L$ is a sentence asserting that all pure, well-founded sets are constructible.

Theorem 5.4.9. The class L of constructible sets satisfies the ZF axioms plus $V = L$.

Proof. The above lemmas show that L satisfies the ZF axioms. It is tedious but straightforward to show that L satisfies $V = L$. □

Lemma 5.4.10. For all ordinals $\alpha \geq \omega$, we have $|L_\alpha| = |\alpha|$.

Proof. By Lemma 5.2.6 we have $|L_\omega| = \aleph_0$ and, for $\alpha \geq \omega$, $|L_{\alpha+1}| = |\mathrm{Def}(L_\alpha)| = |L_\alpha|$. From this the lemma easily follows by induction on $\alpha \geq \omega$. □

Theorem 5.4.11. The class L of constructible sets satisfies the Axiom of Choice.

Proof. Lemma 5.4.10 implies that each L_α is well-orderable. Refining the proof of Lemma 5.4.10, we can explicitly define by transfinite recursion a function $F : \mathrm{Ord} \to V$ such that, for all ordinals α, $F(\alpha)$ is a well-ordering of L_α. Since the definition of F is explicit, its validity does not depend on the Axiom of Choice. Hence by Theorem 5.4.9 the definition of F can be carried out within L. In particular L satisfies that each L_α is well-orderable. Hence by Remark 4.5.3 L satisfies the Axiom of Choice. This argument actually shows that the Axiom of Choice follows from ZF plus $V = L$. □

Our remaining goal with respect to constructible sets is to show that L satisfies the GCH.

Lemma 5.4.12. There is a sentence S of $\mathcal{L}_\in$ with the following property. For all transitive sets A, A satisfies S if and only if $A = L_\alpha$ for some limit ordinal α.

Proof. The construction of the sentence S is straightforward but tedious. Roughly speaking, S is identical with the sentence $V = L$ of Definition 5.4.8. For details of the construction of S, see Boolos and Putnam, "Degrees of unsolvability of constructible sets of integers," *Journal of Symbolic Logic*, Volume 33, 1968, pages 497–513. □

Lemma 5.4.13. If a is any constructible subset of ω, then $a \in L_\alpha$ for some countable ordinal α. More generally, if $a \in \mathcal{P}(\kappa) \cap L$ where κ is an infinite cardinal, then $a \in L_\alpha$ for some ordinal α such that $|L_\alpha| = \kappa$.

Proof. Let κ be an infinite cardinal. Suppose that $a \subseteq \kappa$ and a is constructible. Let $\delta > \kappa$ be a limit ordinal such that $a \in L_\delta$. By the Generalized Löwenheim/-Skolem Theorem (Theorem 5.2.11), we can find a set $A \subseteq L_\delta$ such that $\kappa \cup \{a\} \subseteq A$, $|A| = \kappa$, and $(A, \in|A)$ is an elementary submodel of $(L_\delta, \in|L_\delta)$. By Theorem 5.3.2 and Lemma 5.4.12, we have $(A, \in|A) \cong (L_\alpha, \in|L_\alpha)$ for some limit ordinal α. Since $\kappa \cup \{a\}$ is a transitive subset of A, it follows by another application of Theorem 5.3.2 that $\kappa \cup \{a\} \subseteq L_\alpha$. In particular $a \in L_\alpha$. Clearly $|L_\alpha| = \kappa$, and this completes the proof. □

Lemma 5.4.14. For any infinite cardinal κ, we have $|\mathcal{P}(\kappa) \cap L| \leq \kappa^+$.

Proof. From the previous lemma we have $\mathcal{P}(\kappa) \cap L \subseteq L_{\kappa^+}$. The desired conclusion is immediate, since $|L_{\kappa^+}| = |\kappa^+|$. □

Theorem 5.4.15. The class L of constructible sets satisfies the Generalized Continuum Hypothesis.

Proof. Since L satisfies the axioms of set theory, the proof of the previous lemma can be carried out within L. Thus for all infinite cardinals κ of L, we have within L that $|\mathcal{P}(\kappa)| = \kappa^+$, hence $2^\kappa = \kappa^+$. This proves the theorem. □

Theorem 5.4.16.

1. If ZF has a transitive model, then so does ZFC + GCH.

2. If ZF is consistent, then so is ZFC + GCH.

Proof. Let A be a transitive model of ZF. Within A we can carry out the definition of L to obtain a transitive submodel B (sometimes called an "inner model") consisting of the constructible sets of A. (It can be shown that $B = L_\alpha$ where α is the least ordinal that is not an element of A.) The proofs of theorems 5.4.9, 5.4.11, and 5.4.15 then show that B is a model of ZF plus $V = L$ plus the Axiom of Choice plus the GCH. This proves the first part. The proof of the second part is similar, starting with a model (A, E) that is not necessarily transitive. □

Remark 5.4.17. The previous theorem, due to Gödel 1939, is one of the most significant achievements of axiomatic set theory. The second part is sometimes described as a relative consistency result: ZFC + GCH is consistent relative to ZF.

5.5 Forcing

Let M be a countable transitive model of ZFC. Let $P = (P, \leq)$ be a partially ordered set belonging to M. We say that $p, q \in P$ are *compatible* if there exists $r \in P$ such that $r \leq p$ and $r \leq q$. If $p, q \in P$ are incompatible, we write $p \perp q$.

Definition 5.5.1. A *filter* on P is a set $G \subseteq P$ such that

1. $p, q \in G$ implies $\exists r \in G\,(r \leq p, q)$;

2. $p \in G$, $p \leq q$ imply $q \in G$.

Definition 5.5.2. $D \subseteq P$ is *dense open* if

1. $\forall p \in P\, \exists q \leq p\, (q \in D)$;

2. $\forall p \in D\, \forall q \leq p\, (q \in D)$.

Definition 5.5.3. A filter $G \subseteq P$ is said to be *M-generic* if $G \cap D \neq \emptyset$ for all dense open $D \subseteq P$ such that $D \in M$.

Lemma 5.5.4. Given $p \in P$ we can find an M-generic filter $G \subseteq P$ such that $p \in G$.

Proof. Let $\{D_n \mid n \in \mathbb{N}\}$ be an enumeration of $\{D \in M \mid D \text{ dense open in } P\}$. Put $p_0 = p$ and, given p_n, let $p_{n+1} \leq p_n$ be such that $p_{n+1} \in D_n$. It is easy to verify that $G = \{q \in P \mid \exists n\, (p_n \leq q)\}$ is an M-generic filter. □

Definition 5.5.5. Let G be an M-generic filter. We put

$$M[G] = \{a_G \mid a \in M\},$$

where

$$a_G = \{b_G \mid (p, b) \in a \text{ for some } p \in G\}.$$

Remark 5.5.6. Think of each $a \in M$ as a "name" for $a_G \in M[G]$. We shall show that $M[G]$ is a countable transitive model of ZFC containing M.

Lemma 5.5.7. $M[G]$ is a countable transitive set. We have $M[G] \supseteq M \cup \{G\}$, and $\mathrm{Ord} \cap M[G] = \mathrm{Ord} \cap M$.

Proof. It is obvious from the definition that $M[G]$ is a countable transitive set. For all $a \in M$ we have $a = (\dot{a})_G$, where $\dot{a} = P \times \{\dot{b} \mid b \in a\}$. We also have $G = (\dot{G})_G$, where $\dot{G} = \{(p, \dot{p}) \mid p \in P\}$. Thus $M \cup \{G\} \subseteq M[G]$, and from this it follows that $\mathrm{Ord} \cap M \subseteq \mathrm{Ord} \cap M[G]$. On the other hand, for each $a \in M$ we clearly have $\mathrm{rank}(a) \geq \mathrm{rank}(a_G)$, hence $\mathrm{Ord} \cap M \supseteq \mathrm{Ord} \cap M[G]$. □

A major result is:

Theorem 5.5.8. $M[G]$ is a countable transitive model of ZFC.

Remark 5.5.9. The proof of Theorem 5.5.8 is long and employs a new method known as forcing. However, some parts of the proof are easy and do not require forcing.

For example, given $a, b \in M$, put $c = P \times \{a, b\}$, then $c_G = \{a_G, b_G\}$. This shows that $M[G]$ satisfies the Pairing Axiom. Also, $M[G]$ satisfies the Axiom of Infinity because $\omega = (\dot{\omega})_G \in M[G]$. Furthermore, $M[G]$ satisfies Extensionality and Foundation automatically, because $M[G]$ is a transitive set.

So far we have not used the assumption that G is an M-generic filter.

In order to prove the rest of Theorem 5.5.8, we now introduce the method of forcing.

Definition 5.5.10. The *forcing language* consists of binary relation symbols $\in$ and $=$ plus constant symbols a for each $a \in M$. Sentences of the forcing language are of the form $F(a_1, \ldots, a_n)$, where $F(x_1, \ldots, x_n)$ is a formula of $\mathcal{L}_\in$ with free variables $x_1, \ldots, x_n$, and $a_1, \ldots, a_n \in M$. We have $M[G] \models F(a_1, \ldots, a_n)$ if and only if $F(a_1, \ldots, a_n)$ is true in $M[G]$, where quantifiers are interpreted as ranging over $M[G]$, and $a_1, \ldots, a_n$ are interpreted as $(a_1)_G, \ldots, (a_n)_G$ respectively.

Definition 5.5.11 (forcing)**.** Let $p \in P$ and let F be a sentence of the forcing language. We say that $p \Vdash F$ (read p *forces* F) if and only if $M[G] \models F$ for all M-generic filters G such that $p \in G$.

Lemma 5.5.12 (the extension lemma)**.** If $p \Vdash F$ and $q \leq p$, then $q \Vdash F$.

Proof. This is obvious, because $q \in G$, $q \leq p$ imply $p \in G$. □

Lemma 5.5.13 (definability of forcing)**.** For each formula $F(x_1, \ldots, x_n)$ there is a formula $F^*(p, x_1, \ldots, x_n)$ such that, for all $p \in P$ and $a_1, \ldots, a_n \in M$,

$$p \Vdash F(a_1, \ldots, a_n) \text{ if and only if } M \models F^*(p, a_1, \ldots, a_n).$$

Lemma 5.5.14 (forcing equals truth)**.** $M[G] \models F$ if and only if $\exists p \in G\,(p \Vdash F)$.

Proof. We shall prove Lemmas 5.5.13 and 5.5.14 by simultaneous induction on the number of connectives and quantifiers in F. We assume that F contains only $\wedge$, $\neg$, and $\forall$ (not $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\exists$).

For the base step, we need to find formulas $\in^*(p,x,y)$ and $=^*(p,x,y)$ of $\mathcal{L}_\in$ defining the relations $p \Vdash a \in b$ and $p \Vdash a = b$, respectively, over M. The formulas $\in^*$ and $=^*$ are defined by a rather complicated simultaneous transfinite recursion within M. The properties

$$p \Vdash a \in b \text{ if and only if } M \models \in^*(p,a,b)$$

and

$$p \Vdash a = b \text{ if and only if } M \models =^*(p,a,b)$$

are proved by transfinite induction on $\mathrm{rank}(a)$ and $\mathrm{rank}(b)$. We omit the details.

For the inductive step, note that

$$p \Vdash F_1 \wedge F_2 \text{ if and only if } p \Vdash F_1 \text{ and } p \Vdash F_2,$$

and

$$p \Vdash \forall x\, F(x) \text{ if and only if } p \Vdash F(a) \text{ for all } a \in M.$$

Thus we may define $(F_1 \wedge F_2)^* = F_1^* \wedge F_2^*$ and $(\forall x\, F(x))^* = \forall x\, F^*(x)$. This takes care of $\wedge$ and $\forall$. For $\neg$, we claim that

$$p \Vdash \neg F \text{ if and only if } \neg\,\exists q \le p\,(q \Vdash F).$$

To see this, assume the right hand side. Let G be generic with $p \in G$. To show $M[G] \models \neg F$. Otherwise, $M[G] \models F$ so let $q \in G$ be such that $q \Vdash F$. Let $r \in G$ be such that $r \le p$ and $r \le q$. Then $r \le p$ and $r \Vdash F$, contradicting our assumption. For the converse, assume the left hand side. Suppose $q \le p$, $q \Vdash F$. Let G be generic such that $q \in G$. Then $M[G] \models F$. Also $p \in G$ since $q \le p$. Therefore p does not force $\neg F$, contradicting our assumption.

Thus, for definability of forcing, we may take

$$(\neg F)^*(p, a_1, \ldots, a_n) \equiv \neg\,(\exists q \le p)\, F^*(q, a_1, \ldots, a_n).$$

For focing equals truth, suppose $M[G] \models \neg F$. To show $(\exists p \in G)\, p \Vdash \neg F$. Put $D = \{p \mid p \Vdash F \text{ or } p \Vdash \neg F\}$. Clearly D is dense open. By definability of forcing, $D \in M$. Let $p \in D \cap G$. If $p \Vdash F$, then $M[G] \models F$, a contradiction. Hence $p \Vdash \neg F$. □

We now proceed to the proof of Theorem 5.5.8.

Lemma 5.5.15. $M[G] \models$ the Comprehension Scheme.

Proof. Given $a, a_1, \ldots, a_n \in M$, to find $c \in M$ such that

$$M[G] \models \forall u\,(u \in c \Leftrightarrow (u \in a \wedge F(u, a_1, \ldots, a_n))).$$

Put

$$c = \{(p, b) \mid b \in \bigcup\bigcup a \text{ and } p \Vdash b \in a \wedge F(b, a_1, \ldots, a_n)\}.$$

Then $c \in M$, by Definability of Forcing in M. Then, by the Forcing Equals Truth Lemma, we have

$$c_G = \{b_G \mid b \in \bigcup\bigcup a \text{ and } M[G] \models F(b, a_1, \ldots, a_n)\}.$$

□

Lemma 5.5.16. $M[G] \models$ the Power Set Axiom.

Proof. Given $a \in M$, put $c = P \times \mathcal{P}(P \times \bigcup\bigcup a) \cap M$. We claim that

$$c_G \supseteq \mathcal{P}(a_G) \cap M[G].$$

To see this, given $e_G \in M[G]$, let $d = \{(p, b) \in P \times \bigcup\bigcup a \mid p \Vdash b \in e \cap a\}$. By definability of forcing, $d \in M$, hence $d_G \in c_G$. Moreover $d_G = e_G \cap a_G$. This proves our claim. The Power Set Axiom follows by Comprehension in $M[G]$, since $\mathcal{P}(a_G) \cap M[G] = \{d_G \in c_G \mid M[G] \models d \subseteq a\}$. □

Lemma 5.5.17. $M[G] \models$ the Union Axiom.

Proof. This is similar to the Power Set Axiom. Given $a \in M$ put

$$c = P \times \bigcup\bigcup\bigcup\bigcup a.$$

Then $c_G \supseteq \bigcup a_G$, and the Union Axiom follows by Comprehension in $M[G]$. □

Lemma 5.5.18. $M[G] \models$ the Replacement Scheme.

Proof. It suffices to prove that $M[G] \models$ the Bounding Scheme:

$$\forall w_1 \cdots w_n\, [\, \forall u\, \exists !\, v\, F(u, v, w_1, \ldots, w_n) \Rightarrow \forall x\, \exists y\, \forall u \in x\, \exists v \in y\, F(u, v, w_1, \ldots, w_n)\,].$$

This is because Bounding plus Comprehension implies Replacement.

Given $a, a_1, \ldots, a_n \in M$, let $c \in M$ be such that, for all $(p, b) \in P \times \bigcup\bigcup a$, if there exists $d \in M$ such that $p \Vdash F(b, d, a_1, \ldots, a_n)$, then c contains such a d. We then have

$$M[G] \models \forall u\, \exists !\, v\, F(u, v, w_1, \ldots, w_n) \Rightarrow \forall u \in a\, \exists v \in c'\, F(u, v, a_1, \ldots, a_n),$$

where $c' \in M$, namely $c' = P \times c$. Thus $M[G] \models$ Bounding. □

Lemma 5.5.19. $M[G] \models$ the Axiom of Choice.

Proof. Given $a_G \in M[G]$, let $f \in M$ map an ordinal α onto $\bigcup\bigcup a$. Since $M \subseteq M[G]$, we have $f = (\dot{f})_G \in M[G]$. Composing f with the function $b \mapsto b_G$, we obtain in $M[G]$ a mapping of $\alpha = (\dot{\alpha})_G$ onto $\{b_G \mid b \in \bigcup\bigcup a\} \supseteq a_G$. Thus a_G is well orderable in $M[G]$. □

The proof of Theorem 5.5.8 is now complete.

As a first application, we prove the independence of $V = L$.

Theorem 5.5.20. There exists a countable transitive model of ZFC plus $V \neq L$.

Proof. Let M be a countable transitive model of ZFC. Let P be the set of finite partial functions from ω into $2 = \{0, 1\}$. Partially order P by putting $p \leq q$ if and only if p extends q. Then $P \in M$. Let G be an M-generic filter on P. By Theorem 5.5.8 we have $M[G] \models \text{ZFC}$.

Note that $p, q \in P$ are compatible if and only if $p \cup q \in P$. Thus $g = \bigcup G$ is a partial function from ω into 2. We claim that $\text{dom}(g) = \omega$. To see this, given $n \in \omega$, put $D_n = \{p \in P \mid n \in \text{dom}(g)\}$. Clearly D_n is dense open, and $D_n \in M$. Letting $p \in G \cap D_n$, we see that $n \in \text{dom}(p)$, hence $n \in \text{dom}(g)$.

Thus $g : \omega \to 2$ and $g \in M[G]$. We claim that $g \notin M$. If $g \in M$, then clearly $G = \{p \in P \mid p \subseteq g\} \in M$, so let $D = P \setminus G = \{p \in P \mid p \notin G\}$. Then $D \in M$, and clearly D is dense open. But $G \cap D = \emptyset$, a contradiction.

We claim that $M[G] \models V \neq L$. In fact,

$$M[G] \models \dot{g} \notin L \wedge \dot{g} : \omega \to 2$$

where $(\dot{g})_G = g$. □

5.6 Independence of CH

As in the previous section, let M be a countable transitive model of ZFC, let P be a partially ordered set belonging to M, and let G be an M-generic filter on P. We begin with a discussion of cardinal collapsing and cardinal preservation in $M[G]$.

Remark 5.6.1. Clearly every cardinal of $M[G]$ is a cardinal of M. However, the converse does not always hold. Cardinals of M can be *collapsed* in $M[G]$.

Example 5.6.2. Let κ be an uncountable cardinal of M. Let P be the set of finite partial functions from ω into κ, ordered by $p \leq q$ if and only if p extends q. Let G be an M-generic filter on P. Put $g = \bigcup G$. As in the proof of Theorem 5.5.20, we see that $g : \omega \to \kappa$.

We claim that $\text{rng}(g) = \kappa$. To see this, give $\alpha < \kappa$, put $D_\alpha = \{p \in P \mid \alpha \in \text{rng}(p)\}$. Clearly $D_\alpha \in M$. Because ω is infinite, D_α is dense open. Letting $p \in G \cap D_\alpha$, we see that $\alpha \in \text{rng}(p)$, hence $\alpha \in \text{rng}(g)$.

Thus $g \in M[G]$ maps ω onto κ. It follows that $M[G] \models$ "$\dot{\kappa}$ is a countable ordinal". In particular κ is not a cardinal of $M[G]$.

On the other hand, cardinals of M are often *preserved*, i.e., remain cardinals in $M[G]$.

Lemma 5.6.3. Suppose $M \models$ "κ is a cardinal $> |P|$". Then $M[G] \models$ "κ is a cardinal". In other words, all cardinals $> |P|$ in M are preserved in $M[G]$.

Proof. Suppose not, say $f_G : \lambda \to \kappa$, $\lambda < \kappa$, $\text{rng}(f_G) = \kappa$, $f_G \in M[G]$. Then in M we have

$$\forall \alpha < \kappa \ \exists \beta < \lambda \ \exists p \in P \ (p \Vdash f \mid \dot{\lambda} \to \dot{\kappa} \text{ and } p \Vdash f(\dot{\beta}) = \dot{\alpha}).$$

By the Pigeonhole Principle, we can find $p \in P$, $\beta < \lambda$, $\alpha_1 < \alpha_2 < \kappa$ such that $p \Vdash f : \dot{\lambda} \to \dot{\kappa}$ and $p \Vdash f(\dot{\beta}) = \dot{\alpha_1}$ and $f(\dot{\beta}) = \dot{\alpha_2}$. This is a contradiction. □

Definition 5.6.4. An *antichain* in P is a set $A \subseteq P$ such that the elements of A are pairwise incompatible. P is said to have the *countable chain condition* (c.c.c.) if every antichain of P is countable.

Lemma 5.6.5. Suppose $M \models P$ is c.c.c. Then all cardinals of M are preserved in $M[G]$.

Proof. Suppose not, say $\kappa > \lambda$, $M \models$ "κ is a cardinal", $M[G] \models$ "f maps $\dot{\lambda}$ onto $\dot{\kappa}$". Fix $p \in P$ such that $p \Vdash$ "f maps $\dot{\lambda}$ onto $\dot{\kappa}$". Reasoning within M, for $\alpha < \kappa$ and $\beta < \lambda$ say that α *is a possible value of* $f(\beta)$ if $\exists q \leq p\, (q \Vdash f(\dot{\beta}) = \dot{\alpha})$. Let $X_\beta = \{\alpha \mid \alpha \text{ is a possible value of } f(\beta)\}$. Note that $\kappa = \bigcup_{\beta<\lambda} X_\beta$. Therefore, some X_β is uncountable. Fix such a β. For each $\alpha \in X_\beta$ let $q_\alpha \leq p$ be such that $q_\alpha \Vdash f(\dot{\beta}) = \dot{\alpha}$. Note that $\alpha_1, \alpha_2 \in X_\beta$, $\alpha_1 \neq \alpha_2$ implies $q_{\alpha_1} \perp q_{\alpha_2}$. Thus $A_\beta = \{q_\alpha \mid \alpha \in X_\beta\}$ is an uncountable antichain in P. This contradicts the assumption that P is c.c.c. □

We now proceed to the independence of the Continuum Hypothesis.

Definition 5.6.6. A Δ-*system* is an indexed family of sets $\langle X_i \rangle_{i \in I}$ such that, for some fixed set D, $X_i \cap X_j = D$ for all $i, j \in I$, $i \neq j$.

Lemma 5.6.7 (the Δ-system lemma)**.** Any uncountable family of finite sets contains an uncountable subfamily which is a Δ-system.

Proof. Let $\langle X_i \rangle_{i \in I}$ be an uncountable family of finite sets. We may safely assume that $|I| = \aleph_1$ and that $\bigcup_{i \in I} X_i \subseteq \omega_1$. Passing to an uncountable subfamily, we may assume that $\exists n\, \forall i \in I\, |X_i| = n$. For each $i \in I$, let $X_i(1) < \cdots < X_i(n)$ be the elements of X_i.

Case 1: For each $k = 1, \ldots, n$, $\{X_i(k) : i \in I\}$ is countable. In this case, $\bigcup_{i \in I} X_i$ is countable. Hence, by passing to an uncountable subfamily, we may assume $X_i = X_j$ for all $i, j \in I$. In particular, we have an uncountable Δ-system.

Case 2: Otherwise. Let k be as small as possible such that $\{X_i(k) \mid i \in I\}$ is uncountable. Then, for each $l < k$, $\{X_i(l) \mid i \in I\}$ is countable. By passing to an uncountable subfamily, we may assume $X_i(l) = X_j(l)$ for all $l < k$ and all $i, j \in I$. Thus we have a fixed finite set $D = \{X_i(l) \mid 1 \leq l < k\}$ for all $i \in I$. Since $\{X_i(k) \mid i \in I\}$ is uncountable, we may use transfinite recursion to define a function $f : \omega_1 \to I$ such that, for each $\alpha < \omega_1$, $X_{f(\alpha)}(k) > \sup_{\beta<\alpha} X_{f(\beta)}(n)$. Then $\langle X_{f(\alpha)} \rangle_{\alpha<\omega_1}$ is an uncountable Δ-system contained in $\langle X_i \rangle_{i \in I}$. □

Lemma 5.6.8. Let X be any set. Let P be the set of finite partial functions from X into $\{0, 1\}$, ordered by putting $p \leq q$ if and only if $p \supseteq q$. Then P is c.c.c.

Proof. Suppose not. Let $\langle p_i \rangle_{i \in I}$ be an uncountable antichain in P. By the Δ-system lemma, we may pass to a subfamily such that $\langle \mathrm{dom}(p_i) \rangle_{i \in I}$ is a Δ-system. Say $\mathrm{dom}(p_i) \cap \mathrm{dom}(p_j) = D$ for all $i, j \in I$, $i \neq j$. There are only finitely

many functions from D into $\{0,1\}$, so by passing to an uncountable subfamily we may assume that $p_i \restriction D = p_j \restriction D$ for all $i, j \in I$. Then for all $i, j \in I$ we have that $p_i \cup p_j$ is a function, hence p_i and p_j are compatible, a contradiction. □

Theorem 5.6.9. Let M be a countable transitive model of ZFC. Let κ be an uncountable cardinal of M. Then there exists a countable transitive model M' of ZFC extending M such that (1) M' satisfies $2^{\aleph_0} \geq \kappa$, and (2) M' has the same ordinals and cardinals as M.

Proof. Let P be the set of finite partial functions from $\kappa \times \omega$ into $\{0,1\}$. Let G be an M-generic filter on P. By Lemma 5.5.7 and Theorem 5.5.8, $M[G]$ is a countable transitive model of ZFC which includes M and has the same ordinals as M. By Lemma 5.6.8 P is c.c.c. By Lemma 5.6.5 $M[G]$ has the same cardinals as M.

Put $g = \bigcup G$. As in the proof of Theorem 5.5.20 we see that $g \in M[G]$ and $g : \kappa \times \omega \to \{0,1\}$. For $\alpha < \kappa$ define $g_\alpha : \omega \to \{0,1\}$ by $g_\alpha(n) = g((\alpha, n))$. We claim that $g_\alpha \neq g_\beta$ for all $\alpha < \beta < \kappa$. To see this, let $D_{\alpha\beta}$ be the set of $p \in P$ such that $p((\alpha, n)) \neq p((\beta, n))$ for some $n \in \omega$ such that $(\alpha, n), (\beta, n) \in \mathrm{dom}(p)$. Clearly $D_{\alpha\beta} \in M$ and is dense open. Hence $G \cap D_{\alpha\beta} \neq \emptyset$. Hence $g_\alpha \neq g_\beta$.

It is now clear that $M[G] \models 2^{\aleph_0} \geq \dot{\kappa}$. Thus we may take $M' = M[G]$. □

Chapter 6

Topics in Set Theory

6.1 Stationary Sets

Definition 6.1.1. Let S be a set of ordinals. We say that S is *unbounded in* a limit ordinal δ if $\sup(S \cap \delta) = \delta$. We say that S is *closed in* κ if $S \subseteq \kappa$ and, for all limit ordinals $\delta < \kappa$, if S is unbounded in δ then $\delta \in S$. A *closed unbounded set in* κ (sometimes called a *club* of κ) is any subset of κ which is closed in κ and unbounded in κ.

Lemma 6.1.2. Let κ be a regular uncountable cardinal.

1. If C_i, $i \in I$, is a collection of closed unbounded sets in κ, and if $|I| < \kappa$, then $\bigcap_{i \in I} C_i$ is again a closed unbounded set in κ.
2. If C_α, $\alpha < \kappa$ is a collection of closed unbounded sets in κ indexed by the ordinals less than κ, then the diagonal intersection

$$\triangle_{\alpha<\kappa} C_\alpha \;=\; \{\beta < \kappa \mid \beta \in C_\alpha \text{ for all } \alpha < \beta\}$$

   is again a closed unbounded set in κ.

Proof. Straightforward. □

Definition 6.1.3. Let κ be a regular uncountable cardinal. A set $S \subseteq \kappa$ is said to be *stationary* in κ if $S \cap C \neq \emptyset$ for every closed unbounded set C in κ.

Lemma 6.1.4. Let κ be a regular uncountable cardinal, and let $S \subseteq \kappa$ be stationary in κ. Suppose $S = \bigcup_{i \in I} S_i$ where $|I| < \kappa$. Then S_i is stationary for some $i \in I$.

Proof. Suppose the conclusion fails. Then for each $i \in I$ let C_i be a closed unbounded set such that $S_i \cap C_i = \emptyset$. By Lemma 6.1.2.1, $C = \bigcap_{i \in I} C_i$ is a closed unbounded set. Since S is stationary, $S \cap C$ is nonempty, say $\alpha \in S \cap C$. Then for each $i \in I$ we have $\alpha \notin S_i$, a contradiction. □

Theorem 6.1.5 (Fodor's Theorem)**.** Let κ be a regular uncountable cardinal, and let $S \subseteq \kappa$ be stationary in κ. Suppose $f : S \to \kappa$ is such that $f(\alpha) < \alpha$ for all $\alpha \in S$. Then f is constant on a stationary set. In other words, there exist a stationary $S_0 \subseteq S$ and a $\beta_0 < \kappa$ such that $f(\alpha) = \beta_0$ for all $\alpha \in S_0$.

Proof. Similar to the proof of the previous lemma, using 6.1.2.2 instead of 6.1.2.1. The details are left as an exercise for the reader. □

Theorem 6.1.6. For any regular uncountable cardinal κ, there exists a stationary set $S \subseteq \kappa$ such that $\kappa \setminus S$ is also stationary.

Proof. ... □

We state without proof the following theorem of Solovay.

Theorem 6.1.7. Let κ be a regular uncountable cardinal. Any stationary set $S \subseteq \kappa$ can be decomposed into κ pairwise disjoint stationary sets.

6.2 Large Cardinals

Definition 6.2.1 (hyperinaccessible cardinals)**.** For each $n < \omega$ we define a class of cardinals called the *n-hyperinaccessible* cardinals. We define κ to be 0-hyperinaccessible if it is inaccessible. We define κ to be n+1-hyperinaccessible if it is inaccessible and

$$\{\lambda < \kappa \mid \lambda \text{ is } n\text{-hyperinaccessible}\}$$

is unbounded in κ.

Definition 6.2.2 (Mahlo cardinals)**.** For each $n < \omega$ we define a class of cardinals called the *n-Mahlo* cardinals. We define κ to be 0-Mahlo if it is inaccessible. We define κ to be n+1-Mahlo if it is inaccessible and $\{\lambda < \kappa \mid \lambda \text{ is } n\text{-Mahlo}\}$ is stationary in κ.

Exercise 6.2.3. Show that n+1-hyperinaccessible implies n-hyperinaccessible. Show that n+1-Mahlo implies n-Mahlo. Show that 1-Mahlo implies n-hyperinaccessible for all $n < \omega$.

Lemma 6.2.4. Let δ be a limit ordinal. Suppose $\kappa < \delta$ and $n < \omega$. Then κ is n-hyperinaccessible if and only if R_δ satisfies "κ is n-hyperinaccessible." Also, κ is n-Mahlo if and only if R_δ satisfies "κ is n-Mahlo."

Proof. Straightforward. □

Theorem 6.2.5.

1. The existence of an n+1-hyperinaccessible cardinal is not provable in ZFC + "for all α there exists $\kappa > \alpha$ such that κ is n-hyperinaccessible" (assuming this theory is consistent).

2. The existence of an n+1-Mahlo cardinal is not provable in ZFC + "for all α there exists $\kappa > \alpha$ such that κ is n-Mahlo" (assuming this theory is consistent).

Proof. Straightforward using the previous lemma. □

Lemma 6.2.6.

1. If κ is a cardinal, then L satisfies "κ is a cardinal."
2. If κ is a regular cardinal, then L satisfies "κ is a regular cardinal."
3. If κ is n-hyperinaccessible, then L satisfies "κ is n-hyperinaccessible."
4. If κ is n-Mahlo, then L satisfies "κ is n-Mahlo."

Proof. Straightforward. □

Theorem 6.2.7.

1. If ZFC + "there exists an n-hyperinaccessible cardinal" is consistent, then so is ZFC + $V = L$ + "there exists an n-hyperinaccessible cardinal."
2. If ZFC + "there exists an n-Mahlo cardinal" is consistent, then so is ZFC + $V = L$ + "there exists an n-Mahlo cardinal."

Proof. Straightforward using the previous lemma. □

6.3 Ultrafilters and Ultraproducts

Definition 6.3.1. Let I be a nonempty set. A *filter* on I is a set $\mathcal{F} \subseteq \mathcal{P}(I)$ such that

1. $\emptyset \notin \mathcal{F}$ and $I \in \mathcal{F}$;
2. if $X_1, \ldots, X_n \in \mathcal{F}$ then $X_1 \cap \ldots \cap X_n \in \mathcal{F}$;
3. if $X \in \mathcal{F}$ and $X \subseteq Y \in \mathcal{P}(I)$ then $Y \in \mathcal{F}$.

Examples 6.3.2.

1. $\mathcal{F} = \{I\}$.
2. $\mathcal{F} = \{X \subseteq I \mid X \supseteq X_0\}$, where $\emptyset \neq X_0 \subseteq I$. Such an $\mathcal{F}$ is called a *principal filter*.
3. $\mathcal{F} = \{X \subseteq I \mid X$ is cofinite, i.e., $I \setminus X$ is finite$\}$ (assuming I is infinite).
4. $\mathcal{F} = \{X \subseteq I \mid |I \setminus X| < \kappa\}$, where κ is any infinite cardinal $\leq |I|$.
5. $I = \mathbb{R}^n$, $\mathcal{F} = \{X \subseteq \mathbb{R}^n \mid \mathbb{R}^n \setminus X$ has Lebesgue measure $0\}$. Here we could replace $\mathbb{R}^n$ by any measure space.

6. $I = \mathbb{R}^n$, $\mathcal{F} = \{X \subseteq \mathbb{R}^n \mid \mathbb{R}^n \setminus X \text{ is meager}\}$. Here we could replace $\mathbb{R}^n$ by any complete metric space.

7. Let $I = \kappa$ where κ is a regular uncountable cardinal. Then

$$\mathcal{F} = \{X \subseteq \kappa \mid X \supseteq C \text{ for some closed unbounded set } C \subseteq \kappa\}$$

is a filter, known as the *closed unbounded filter* on κ.

8. Let A be an uncountable set. Put

$$I = \mathcal{P}_c(A) = \{Y \subseteq A \mid Y \text{ is countable}\}.$$

Recall that $A^{<\omega}$ is the set of finite sequences of elements of A. Given $f : A^{<\omega} \to A$, put

$$C_f = \{Y \in \mathcal{P}_c(A) \mid Y \text{ is closed under } f, \text{ i.e., } f[Y^{<\omega}] \subseteq Y\}.$$

Then

$$\mathcal{F}_c(A) = \{X \subseteq \mathcal{P}_c(A) \mid X \supseteq C_f \text{ for some } f\}$$

is a filter known as the *closed unbounded filter* on $\mathcal{P}_c(A)$.

Definition 6.3.3. Let κ be an infinite cardinal. A filter $\mathcal{F}$ is said to be κ-*additive* if $\bigcap_{i\in I} X_i \in \mathcal{F}$ whenever $X_i \in \mathcal{F}$ for all $i \in I$, $|I| < \kappa$.

Examples 6.3.4.

1. Every filter is *finitely additive*, i.e., $\aleph_0$-additive.

2. The Lebesgue and Baire filters on $\mathbb{R}^n$ are *countably additive*, i.e., $\aleph_1$-additive.

3. For any infinite cardinal $\kappa \leq |I|$, the filter $\{X \subseteq I \mid |I - X| < \kappa\}$ is κ-additive.

4. For any regular uncountable cardinal κ, the closed unbounded filter on κ is κ-additive.

5. For any uncountable set A, the closed unbounded filter on $\mathcal{P}_c(A)$ is countably additive.

Definition 6.3.5. An *ultrafilter* on I is a filter $\mathcal{U}$ on I such that for all $X \subseteq I$ either $X \in \mathcal{U}$ or $I \setminus X \in \mathcal{U}$.

Remark 6.3.6. The filters in 6.3.2.3–8 are not ultrafilters. Indeed, it is difficult to find explicit examples of nonprincipal ultrafilters. However, as we shall now show, nonprincipal ultrafilters can be constructed by means of transfinite recursion plus the Axiom of Choice.

Theorem 6.3.7. Any filter $\mathcal{F}$ on I can be extended to an ultrafilter $\mathcal{U}$ on I.

Proof. Say that $\mathcal{G} \subseteq \mathcal{P}(I)$ has the *finite intersection property* (f.i.p.) if $Y_1 \cap \ldots \cap Y_m \neq \emptyset$ for all $Y_1, \ldots, Y_m \in \mathcal{G}$.

By the well-ordering theorem, let $\kappa = |\mathcal{P}(I)|$, say

$$\mathcal{P}(I) = \{X_\alpha \mid \alpha < \kappa\}.$$

We shall use transfinite recursion to define a sequence of sets $\mathcal{F}_\alpha \subseteq \mathcal{P}(I)$, $\alpha \leq \kappa$, each of which has the f.i.p.

Stage 0. Put $\mathcal{F}_0 = \mathcal{F}$. Note that $\mathcal{F}$ has the f.i.p. since it is a filter.

Stage $\alpha + 1$. Assume inductively that $\mathcal{F}_\alpha$ has the f.i.p. We claim that at least one of $\mathcal{F}_\alpha \cup \{X_\alpha\}$, $\mathcal{F}_\alpha \cup \{I \setminus X_\alpha\}$ has the f.i.p. Otherwise we would have $X_\alpha \cap Y_1 \cap \ldots \cap Y_m = \emptyset$, $Y_1, \ldots, Y_m \in \mathcal{F}_\alpha$, $(I \setminus X_\alpha) \cap Z_1 \cap \ldots \cap Z_m = \emptyset$, $Z_1, \ldots, Z_n \in \mathcal{F}_\alpha$. Then $Y_1 \cap \ldots \cap Y_m \cap Z_1 \cap \ldots \cap Z_n = \emptyset$ so $\mathcal{F}_\alpha$ does not have the f.i.p., a contradiction. We therefore set

$$\mathcal{F}_{\alpha+1} = \begin{cases} \mathcal{F}_\alpha \cup \{X_\alpha\} & \text{if this has the f.i.p.,} \\ \mathcal{F}_\alpha \cup \{I \setminus X_\alpha\} & \text{otherwise.} \end{cases}$$

Then clearly $\mathcal{F}_{\alpha+1}$ has the f.i.p.

Stage δ, where δ is a limit ordinal. Put $\mathcal{F}_\delta = \bigcup_{\alpha<\delta} \mathcal{F}_\alpha$. Clearly this has the f.i.p.

Finally put $\mathcal{U} = \mathcal{F}_\kappa = \bigcup_{\alpha<\kappa} \mathcal{F}_\alpha$. Clearly $\mathcal{U}$ has the f.i.p. and for every $X \in \mathcal{P}(I)$ either $X \in \mathcal{U}$ or $I \setminus X \in \mathcal{U}$. It follows easily that $\mathcal{U}$ is an ultrafilter. This completes the proof. □

Lemma 6.3.8. Any principal ultrafilter $\mathcal{U}$ on I is of the form

$$\mathcal{U} = \{X \subseteq I \mid i_0 \in X\}$$

for some fixed $i_0 \in I$.

Proof. Let $\mathcal{U}$ be a principal ultrafilter on I. By definition we have

$$\mathcal{U} = \{X \subseteq I \mid X \supseteq X_0\}$$

where $\emptyset \neq X_0 \subseteq I$. If $|X_0| \geq 2$, let $Y \subseteq I$ be such that $Y \cap X_0 \neq \emptyset$ and $(I \setminus Y) \cap X_0 \neq \emptyset$. Then $Y, I \setminus Y \notin \mathcal{U}$, a contradiction. Thus $|X_0| = 1$, i.e., $X_0 = \{i_0\}$ for some $i_0 \in I$. This proves the lemma. □

Theorem 6.3.9. For every infinite set I there exists a nonprincipal ultrafilter $\mathcal{U}$ on I.

Proof. Consider the filter $\mathcal{F} = \{X \subseteq I \mid I \setminus X \text{ is finite}\}$. By Theorem 6.3.7, let $\mathcal{U}$ be an ultrafilter on I such that $\mathcal{F} \subseteq \mathcal{U}$. For all $i_0 \in I$ we have $I \setminus \{i_0\} \in \mathcal{F} \subseteq \mathcal{U}$, hence $\{i_0\} \notin \mathcal{U}$. Thus $\mathcal{U}$ is nonprincipal. □

Definition 6.3.10. A *structure* is a relational structure, i.e., an ordered pair (A, E) where A is a nonempty set and $E \subseteq A \times A$.

Definition 6.3.11 (ultraproduct)**.** Suppose we are given an indexed family of structures $\langle (A_i, E_i)\rangle_{i\in I}$ and an ultrafilter $\mathcal{U}$ on the index set I. We are going to define a structure

$$(A, E) \;=\; \prod_{\mathcal{U}} \langle (A_i, E_i)\rangle_{i\in I}$$

known as an *ultraproduct*. Recall that

$$\prod_{i\in I} A_i \;=\; \left\{ f \;\middle|\; f : I \to \bigcup_{i\in I} A_i, f(i) \in A_i \text{ for all } i \in I \right\} .$$

For $f, g \in \prod_{i\in I} A_i$ define

$$\begin{array}{lll} f \approx g & \Leftrightarrow_{\text{def}} & f \approx_{\mathcal{U}} g \\ & \Leftrightarrow_{\text{def}} & \{i \in I \mid f(i) = g(i)\} \in \mathcal{U} . \end{array}$$

This is an equivalence relation. We define

$$[f] \;=_{\text{def}}\; [f]_{\mathcal{U}} \;=_{\text{def}}\; \left\{ g \in \prod_{i\in I} A_i \;\middle|\; f \approx_{\mathcal{U}} g \right\}$$

and

$$A \;=\; \prod_{\mathcal{U}} \langle A_i\rangle_{i\in I} \;=\; \prod_{i\in I} A_i \Big/ \mathcal{U} \;=\; \left\{ [f]_{\mathcal{U}} \;\middle|\; f \in \prod_{i\in I} A_i \right\} .$$

Finally, for $f, g \in \prod_{i\in I} A_i$, we define

$$([f], [g]) \in E \;\Leftrightarrow_{\text{def}}\; \{i \in I \mid (f(i), g(i)) \in E_i\} \in \mathcal{U} .$$

Note that this last definition is independent of representatives, i.e., $f \approx f'$, $g \approx g'$, $([f], [g]) \in E$ imply $([f'], [g']) \in E$. Thus $E \subseteq A \times A$ is well-defined, and so (A, E) is a structure.

Theorem 6.3.12 (Łoś's Theorem)**.** Let $(A, E) = \prod_{\mathcal{U}} \langle (A_i, E_i)\rangle_{i\in I}$ be an ultraproduct. Let $\psi(x_1, \ldots, x_k)$ be a formula with free variables among $x_1, \ldots, x_k$. Then for all $[f_1], \ldots, [f_k] \in A$ we have

$$\models_{(A,E)} \psi([f_1], \ldots, [f_k]) \;\Leftrightarrow\; \{i \in I \mid \models_{(A_i,E_i)} \psi(f_1(i), \ldots, f_k(i))\} \in \mathcal{U} .$$

6.4 Measurable Cardinals

6.5 Ramsey's Theorem

Index