An Introduction to Reverse Mathematics

A thesis submitted
by

John Cobb

to
The Departments of Mathematics and Philosophy
in partial fulfillment of the requirements
for the degree of
Bachelor of Arts with Honors
Harvard College
Cambridge, Massachusetts

March 30, 2009

Acknowledgements

There are many people who have helped to make this thesis a reality. First and foremost, I want to thank Dr. Warren Goldfarb whose mentorship has proved invaluable. His guidance throughout the entire process allowed me to meet and surpass my expectations and turned the daunting task of producing a thesis into a pleasant and intellectually invigorating experience.

I also want to thank those scholars whose work provided the basis for this thesis. I thank Harvey Friedman for his work in establishing reverse mathematics, an area which is both fascinating and of inherent value. I also want to thank Rodney Downey and Reed Solomon for their work on the reverse mathematics of Hahn's embedding theorem, the subject of the third chapter of this thesis. Additionally, I want to express my gratitude to Stephen Simpson both for his work on Hilbert's basis theorem and for writing an excellent introductory text on reverse mathematics.

I want to thank my friends and family for all of their support. My parents and my brother Daniel have been there for me all of my life, and I owe them my deepest thanks. Finally, I want to thank my best friend and confidante, Laura. Without you I would not be the person I am today.

Introduction

Reverse mathematics is a relatively new program in the foundations of mathematics. Its basic goal is to assess the relative logical strengths of theorems from ordinary non-set theoretic mathematics. To this end, one tries to find the minimal natural axiom system $\mathfrak{A}$ that is capable of proving a theorem T. In order to verify that $\mathfrak{A}$ is in some sense the weakest axiom system that would allow a proof of T it would be nice to be able to show that $\mathfrak{A}$ in fact follows from T, for this would demonstrate that the axioms of $\mathfrak{A}$ are necessary for T to hold. However, no theorem T from ordinary mathematics is strong enough to prove any reasonable axiomatization of mathematics. Therefore, one must supplement T with a weak axiom system $\mathfrak{B}$ known as the *base system.* If one is able to find axiom systems $\mathfrak{A}$ and $\mathfrak{B}$ and a theorem T such that $\mathfrak{A}$ is capable of proving T and such that $\mathfrak{B} + T$ is capable of proving $\mathfrak{A}$ in turn, then one says that T and $\mathfrak{A}$ are *equivalent over* $\mathfrak{B}$. A proof that $\mathfrak{A}$ follows from $\mathfrak{B}$ and T is called a *reversal of* T. The goal of reverse mathematics is to find axiom systems to which the theorems of ordinary mathematics are equivalent.

It turns out that many of the theorems of ordinary mathematics are either provable in the weak base system RCA_0, which essentially corresponds to computable or recursive mathematics, or are equivalent over RCA_0 to one of four subsystems of second order arithmetic WKL_0, ACA_0, ATR_0 and $\Pi^1_1 - \mathrm{CA}_0$. These subsystems differ primarily in their *set comprehension axioms*, which lay out what sets must exist. Additionally, all of these systems may be arranged linearly in terms of logical strength, with RCA_0 the weakest system and $\Pi^1_1 - \mathrm{CA}_0$ the strongest. It is somewhat surprising that so many of the theorems of ordinary mathematics can be shown equivalent to so few axiom systems, and it is even more surprising that these systems can be ordered linearly by their logical strength. This is one of the key insights provided by reverse mathematics. In Chapter I, we will explore the reverse mathematics of some completeness and compactness properties of the real line with respect to three of these basic axiom systems as an illustration of the standard practice of reverse mathematics.

There are also additional benefits of studying reverse mathematics. In general, it is harder to find a reversal of a given theorem than a proof of that theorem in the equivalent axiom system. For this reason, reversals tend to grant some deeper insight into the theorems than is afforded by their statements and proofs alone. For example, in Chapter II we will study the reverse mathematics of Hilbert's basis theorem. We will show that while Hilbert's proof of this theorem could never have been constructive, the theorem can be proven constructively if one assumes a basic fact from the theory of ordinals, namely that ω^ω is well-ordered. Moreover, we will show that the well-ordering of ω^ω is equivalent to Hilbert's basis theorem over constructive mathematics.

As another example of the extra insight that reverse mathematics can provide, we will see in Chapter III that a reversal of T can sometimes be reinterpreted as showing that T

is not an *effective theorem*, that is the structures that it proves to exist are not always computable. In particular, we will show constructively that Hahn's embedding theorem for ordered abelian groups is not an effective theorem.

Chapter I - Elementary Reverse Mathematics

In this chapter we will study the reverse mathematics of completeness and compactness properties of the real numbers in RCA_0, ACA_0 and WKL_0. We will also briefly discuss results from reverse mathematics in other areas and in ATR_0 and $\Pi^1_1 - \mathrm{CA}_0$. All of the results from this chapter may be found in [1]. Before discussing these results, however, we must briefly turn our attention to second order arithmetic, the arena in which the action of reverse mathematics occurs.

Second Order Arithmetic

Most of the reverse mathematics to date has been carried out using subsystems of *second order arithmetic*, often denoted Z_2. The language of second order arithmetic consists of the logical symbols $\wedge$,$\vee$,$\neg$,(,), quantifiers $\forall$ and $\exists$, relations $=$,$<$,$\in$, binary operators $+$ and $*$, a constant symbol 0, a unary operator S representing the successor function on the natural numbers, and a two-tiered system of variables x,y,z,... that range over natural numbers and X,Y,Z,... that range over sets of natural numbers.

Sets of sets of natural numbers are not part of second order arithmetic, hence it cannot handle *essentially* uncountable mathematics. While this is a significant limitation, large parts of mathematics can be dealt with using only countable structures. For example, the study of continuous functions on complete separable metric spaces is not essentially uncountable. Using second order arithmetic also has technical advantages because basic existence axioms are not as strong as they might be in essentially uncountable mathematics.

The axioms of second order arithmetic are the usual logical axioms and arithmetic axioms of Peano arithmetic in addition to two axiom schemata. The first, is the *comprehension axiom schema*, which essentially dictates which sets are known to exist. In full second order arithmetic this schema is given by

$$\exists X \forall n (n \in X \leftrightarrow \phi(n))$$

where ϕ is any well-formed formula in which X is not a free variable. ϕ may have other free variables, in which case the universalization of the sentence above is understood to hold, or it may have parameters.

The second axiom schema is the *schema of induction*

$$(\phi(0) \land \forall n(\phi(n) \to \phi(Sn))) \to \forall n \phi(n)$$

where ϕ is a well-formed formula, which may or may not have other free variables. In full second order arithmetic, this axiom schema is actually redundant. It may be replaced by the *second order induction axiom*

$$\forall X((0 \in X \land \forall n(n \in X \to Sn \in X)) \to \forall n(n \in X)).$$

This sentence in addition to the comprehension schema immediately imply the induction schema.

All subsystems of second order arithmetic we will consider here include the basic logical and arithmetic axioms. The comprehension and induction axiom schemata, however, are limited in these subsystems. In order to delineate these limitations, we must first classify the formulae of second order arithmetic.

We say that a formula is an *arithmetical formula* if it has no universal or existential quantifiers that range over set variables. In other words, the only quantifiers in an arithmetical formula are number quantifiers. Arithmetical formulae may be further subdivided into the classes Σ_0^0, Σ_1^0, Π_1^0 and Δ_1^0. A formula is said to be Σ_0^0 if it is equivalent to a formula with only number quantifiers that are bounded above and no other quantifiers.[1] We say that a formula is Σ_1^0 if it is equivalent to a formula of the form $\exists n \phi(n)$ where $\phi(n)$ is Σ_0^0. Similarly, a formula is Π_1^0 if it is equivalent to a formula of the form $\forall n \phi(n)$ where $\phi(n)$ is Σ_0^0. A formula is Δ_1^0 just in case it is both Σ_1^0 and Π_1^0. It should be noted that Δ_1^0 formulae define recursive sets and that Σ_1^0 formulae define recursively enumerable sets. The complement of a Σ_1^0 formula is Π_1^0 and vice-versa.

Having made these preliminary definitions, we may now turn our attention to our first subsystem of second order arithmetic, RCA_0.

The Base System: RCA_0

RCA_0, or *recursive comprehension axiom with limited induction*, is the base system used in most of reverse mathematics, and it will be the base systems for all of the results we discuss here. It is a subsystem of second order arithmetic that is meant to correspond more or less with computable and constructive mathematics. In RCA_0, the full comprehension schema is replaced by comprehension only for Δ_1^0 sets. That is we have

$$\exists X \forall n(n \in X \leftrightarrow \phi(n))$$

[1] By equivalent here we mean that the same sets of natural numbers satisfy the two formulae. We will treat this equivalence informally here for the sake of readability. For more details, see [2]. By a number quantifier that is bounded above we mean expressions such as $\forall j(j < n \to \phi(j))$ or $\exists i \leq p(\theta(i))$

only for formulae ϕ that are Δ^0_1. Similarly, the induction schema is limited to Σ^0_1 formulae. In other words, RCA_0 is second order mathematics restricted to recursive sets and where induction is restricted to recursively enumerable sets. Not surprisingly, the recursive sets form a minimal model of RCA_0 (See [1] Corollary II.1.8).

Finite sets, ordered tuples, and finite sequences may be encoded as natural numbers using elementary number theory in RCA_0. Similarly, infinite sequences and the Cartesian products of sets may be encoded as sets, and a function $f : X \to Y$ may be encoded as subsets of $X \times Y$ in the standard manner. Additionally, the set of integers, $\mathbb{Z}$, and the set of rational numbers, $\mathbb{Q}$, and the arithmetic operations on these sets can be encoded and shown to fulfill the usual ring and field axioms respectively. We will employ the ordinary notation of mathematics, and for the most part ignore these issues of encoding as atomic terms for these encodings are all Σ^0_0. For details, see [1]. The encoding of $\mathbb{R}$ is more subtle in second order arithmetic and will be discussed below.

Primitive Recursion

In this section we will show some basic results about RCA_0. Namely, we will show that all primitive recursive functions are provably total functions in RCA_0 and will derive two important consequences from this fact.

Theorem I.1. If $f : \mathbb{N}^k \to \mathbb{N}$ is a primitive recursive function, then its existence may be proven in RCA_0. Additionally, the characteristic function of a set X is also exists in RCA_0. That is, the following functions may be shown to exist in RCA_0:

(i) The constant functions

(ii) The composition of two functions

(iii) For any two functions $f : \mathbb{N}^k \to \mathbb{N}$ and $g : \mathbb{N}^{k+2} \to \mathbb{N}$, a function $h : \mathbb{N}^{k+1} \to \mathbb{N}$ defined by

$$h(0, n_1, \dots, n_k) = f(n_1, \dots, n_k)$$
$$h(m + 1, n_1, \dots, n_k) = g(h(m, n_1, \dots, n_k), m, n_1, \dots, n_k)$$

(iv) For any function $f : \mathbb{N}^{k+1} \to \mathbb{N}$ such that for all $(n_1, \dots, n_k) \in \mathbb{N}^k$ there exists some $m \in \mathbb{N}$ such that $f(m, n_1, \dots, n_k) = 1$, a function $g : \mathbb{N}^k \to \mathbb{N}$ defined by

$$g(n_1, \dots, n_k) = \text{least } m \text{ such that } f(m, n_1, \dots, n_k) = 1$$

and

(v) For any set X, the *characteristic function of* X, $\chi_X : \mathbb{N} \to \mathbb{N}$ defined such that $\chi_X(n) = 1$ if $n \in X$ and $\chi_X(n) = 0$ if $n \notin X$.

Proof.

(i) If $c \in \mathbb{N}$ is a constant, then the function $f = \{(i,j) \,|\, j = c\}$ exists by Σ^0_0 comprehension.

(ii) Let $f : X \to Y$ and $g : Y \to Z$ be functions. Then their composition $h : X \to Z$ is given by

$$h = \{(i,j) \,|\, \exists k \in Y((i,k) \in f \wedge (k,j) \in g)\} = \{(i,j) \,|\, i \in X \wedge \forall k((i,k) \in f \to (k,j) \in g)\},$$

which exists by Δ^0_1 comprehension. This is a well-defined function provided that f and g are well-defined functions.

(iii) Let $\theta(s, m, (n_1, \ldots, n_k))$ be the Σ^0_0 formula that says that s is a sequence of the initial m values of $h(n_1, \ldots, n_k)$. That is, $\theta(s, m, (n_1, \ldots, n_k))$ says that s encodes a sequence of length $m+1$ such that $s_0 = f(n_1, \ldots, n_k)$, and for all $i < m$, $s_{i+1} = g(s_i, m, n_1, \ldots, n_k)$.

We may define

$$\begin{aligned} h &= \{((m, n_1, \ldots, n_k), j) \,|\, \exists s(\theta(s, m, (n_1, \ldots, n_k)) \wedge s(m) = j)\} \\ &= \{((m, n_1, \ldots, n_k), j) \,|\, \forall s(\theta(s, m, (n_1, \ldots, n_k)) \to s(m) = j)\}, \end{aligned}$$

which exists by Δ^0_1 comprehension. To prove that this is a well-defined function, we must show in RCA_0 that there exists an essentially unique s for all m and $(n_1, \ldots, n_k)$ such that $\theta(s, m, (n_1, \ldots, n_k))$.

Fix $(n_1, \ldots, n_k)$. The formula

$$\phi(m) = \exists s\, \theta(s, m, (n_1, \ldots, n_k))$$

is Σ^1_0, and

$$\phi(0) \wedge \forall m(\phi(m) \to \phi(Sm))$$

is by hypothesis a theorem of RCA_0. Therefore, by Σ^0_1 induction, $\forall m\, \phi(m)$ is a theorem of RCA_0. Moreover, we can prove that s is unique for fixed m, i.e.

$$(\theta(s, m, (n_1, \ldots, n_k)) \wedge \theta(s', m, (n_1, \ldots, n_k))) \to \forall i < m+1(s_i = s'_i).$$

(iv) Define

$$g = \{((n_1, \ldots, n_k), m) \,|\, ((m, n_1, \ldots, n_k), 1) \in f \wedge \neg \exists m' < m(((m', n_1, \ldots, n_k), 1) \in f)\},$$

which exists by Σ^0_0 comprehension. This is a well-defined function by hypothesis.

(v) Define

$$\chi_X = \{(i,j) \,|\, (i \in X \wedge j = 1) \vee (i \notin X \wedge j = 0)\},$$

which exists by Σ^0_0 comprehension.□

Corollary I.2. For any infinite set X, one can prove in RCA_0 that there exists a function $\pi_X : \mathbb{N} \to X$ that enumerates all of the elements of X in order.

Proof. We will show that π_X is primitive recursive relative to χ_X, which exists by (v) above. First, define $\nu_X : \mathbb{N} \to \mathbb{N}$ by $\nu_X(n) =$ least m such that $n > m$ and $\chi_X(m) = 1$, which exists by (iv) above. Now we can define π_X by (iii) above.

$$\pi_X(0) = \nu_X(0)$$

$$\pi_X(m+1) = \nu_X(\pi_X(m)).□$$

Corollary I.3. Let $\phi(n)$ be a Σ^0_1 formula in which f does not occur freely. One can prove in RCA_0 that either only finitely many n satisfy $\phi(n)$, or there exists a one-to-one function $f : \mathbb{N} \to \mathbb{N}$ whose range is precisely those n that satisfy $\phi(n)$.

Proof. By the normal form theorem, there exists a Σ^0_0 formula $\theta(j,n)$ such that $\phi(n)$ is logically equivalent to $\exists j\, \theta(j,n)$. Define $X = \{(j,n) \,|\, \theta(j,n) \wedge \neg\exists j' < j(\theta(j',n))\}$. Either only finitely many n satisfy $\phi(n)$, or X is infinite. If X is infinite, then by Corollary I.2, π_X exists, and we may set $f(n) = p_2(\pi_X(n))$ where p_2 is the projection function $p_2 = \{(m,k) \,|\, m$ encodes $(i,j) \wedge k = j$, which exists by Σ^0_0 comprehension.□

Arithmetical Comprehension: ACA_0

ACA_0, or *arithmetical comprehension with limited induction*, is a formal system defined similarly to RCA_0 although it is in fact quite a bit stronger. Just as in RCA_0 it has all the logical and arithmetic axioms of standard Peano arithmetic. Unlike RCA_0, however, ACA_0 has a comprehension schema covering all arithmetical formulae. Recall that a formula is arithmetical just in case it has no quantifiers ranging over the universe of sets. Induction in ACA_0 is accomplished using a single axiom - the second order axiom of induction - as discussed above. This allows induction to be carried out on all arithmetical formulae.

The following lemma provides some weaker conditions for concluding that arithmetical comprehension holds. These are very useful in proving reversals involving ACA_0.

Lemma I.4. Arithmetical comprehension is equivalent over RCA_0 to the following:

(i) Σ^0_1 comprehension, i.e. $\exists X \forall n(n \in X \leftrightarrow \phi(n))$ for any Σ^0_1 formula ϕ in which X is not free.

(ii) For all one-to-one functions $f : \mathbb{N} \to \mathbb{N}$, the range of f exists, i.e.

$$\exists X \forall n (n \in X \leftrightarrow \exists m (f(m) = n)).$$

Proof. That arithmetical comprehension implies (i) is clear. That (i) implies (ii) follows from the fact that $\exists m(f(m) = n)$ is Σ^0_1. That (ii) implies (i) follows from Corollary I.3. All that remains to be shown is that (i) implies arithmetical comprehension.

Assume (i) holds. Every arithmetical formula is equivalent to some formula that consists of alternating universal and existential number quantifiers followed by a Σ^0_0 formula.[2] Therefore, we may take our formula to be in this form and further stipulate that the string of quantifiers begins with an existential quantifier by using dummy variables if necessary. Because the negation of a universal quantifier is an existential quantifier and vice-versa, and because the complement of a set necessarily exists, it is immaterial whether the formula begins with a universal quantifier or an existential quantifier. We proceed by induction on m, the number of alternations between types of quantifiers that appear. The $m = 0$ case follows from (i). Assume that comprehension holds in the case $m = k$, and let $\phi(n)$ have $k + 1$ alternations beginning with an existential quantifier. We may write $\phi(n)$ as $\exists j\, \theta(j, n)$ where $\theta(j, n)$ has k alternations beginning with a universal quantifier. Let

$$X = \{(j, n) \mid \neg\theta(j, n)\}.$$

The negation in $\neg\theta(j, n)$ may be propagated along the alternating quantifiers until it is absorbed by the Σ^0_0 portion of $\theta(j, n)$. This results in a formula that conforms to the $m = k$ case, and thus X exists by the inductive hypothesis. Let

$$Y = \{n \mid \exists j((j, n) \notin X)\},$$

which exists by Σ^0_1 comprehension. We have

$$\forall n(\phi(n) \leftrightarrow \exists j\, \theta(j, n) \leftrightarrow \neg\forall j(\neg\theta(j, n)) \leftrightarrow \neg\forall j((j, n) \in X) \leftrightarrow \exists j((j, n) \notin X) \leftrightarrow n \in Y).$$

Thus, Y is the set defined by $\phi(n)$, so we have comprehension with $k+1$ quantifier alternations.□

Weak König's Lemma: WKL_0

WKL_0, or RCA_0 *with weak König's lemma*, is an axiom system with logical strength between RCA_0 and ACA_0. It consists of the axioms of RCA_0 plus an additional lemma concerning infinite binary trees called weak König's lemma.

Definitions. Recall that in second order arithmetic finite sequences may be encoded as natural numbers. Let $2^{<\mathbb{N}}$ denote the set of *binary sequences*, or finite sequences consisting

[2] For a constructive proof of this statement that is readily formalized into RCA_0, see [2].

only of 0's and 1's. This set exists in RCA_0 by Σ^0_0 comprehension. If $s = (s_0, \ldots, s_n) \in 2^{<\mathbb{N}}$ is a sequence, let $\ell(s) = n + 1$ be the *length of* s. This function is primitive recursive and hence exists in RCA_0 by Theorem I.1. If $s = (s_0, \ldots, s_n)$ and $t = (t_0, \ldots, t_m)$ are two binary sequences, then define the *concatenation of* s *and* t to be $s \diamond t = (s_0, \ldots, s_n, t_0, \ldots, t_m)$. A binary sequence s is said to be an *initial part* of a binary sequence t, denoted $s \subseteq t$, just in case there exists a (possibly null) sequence u such that $s \diamond u = t$.

A *binary tree*, $T \subset 2^{<\mathbb{N}}$ is a set of binary sequences such that if $s \in T$ and $t \subseteq s$, then necessarily $t \in T$. A *path through* T is a function $f : \mathbb{N} \to \{0, 1\}$ such that $(f(0), \ldots, f(n)) \in T$ for all $n \in \mathbb{N}$. *Weak König's lemma* states that for any infinite binary tree T, there exists a path through T.[3]

Real Numbers in RCA_0

We will now define and develop some of the basic properties of the real numbers $\mathbb{R}$ within second order arithmetic. We will then show that RCA_0 is strong enough to prove that $\mathbb{R}$ satisfies a certain completeness property called nested interval completeness. In the chapters that follow, we will study the reverse mathematics of real numbers in ACA_0 and WKL_0, culminating with the following theorem:

Main Theorem I. The following are theorems of RCA_0:

(A) The real numbers are nested interval complete.

(B) ACA_0 is equivalent to the following statements:
(ii) The real numbers are complete.
(iii) $[0, 1]$ is sequentially compact.

(C) WKL_0 is equivalent to the compactness of $[0, 1]$.

Definitions. A set $\mathbf{x}$ is a *real number* in second order arithmetic if it is an infinite sequence of rational numbers $x = \{x_k \in \mathbb{Q}\}_{k \in \mathbb{N}}$ such that $|x_k - x_{k+i}| \leq 2^{-k}$ for all $k, i \in \mathbb{N}$. Notice that the set of real numbers $\mathbb{R}$ does not exist in second order arithmetic as it is uncountable. We will however, use the term $\mathbf{x} \in \mathbb{R}$ as a stand-in for the full expression that $\mathbf{x}$ is a real number. $\mathbf{x} \in \mathbb{R}$ is *not* a Σ^0_0 formula, but is instead a Π^0_1 formula because of the universal quantification over i and k in the definition.

Two real numbers $\mathbf{x}$ and $\mathbf{y}$ are *equal* if, for all $k \in \mathbb{R}$, $|x_k - y_k| \leq 2^{-k+1}$. Again we will denote equality as $\mathbf{x} = \mathbf{y}$, but this is not ordinary equality and is Π^0_1 rather than Σ^0_0. Addi-

[3] The full form of König's lemma is the same statement concerning finitely branching trees with arbitrary natural numbers for nodes. König's lemma is in fact equivalent to ACA_0 over RCA_0. See [1] for details.

tion, multiplication and comparison can be defined similarly and atomic formulae involving these are also Π^0_1. Because, for example, $\mathbf{x} < \mathbf{y}$ is equivalent to $\neg(\mathbf{x} \geq \mathbf{y})$, atomic formulae involving comparison are actually Δ^0_1.

Sequences of real numbers may also be encoded as sets, and we say that a sequence of real numbers $\{\mathbf{x_n} \in \mathbb{R}\}_{n \in \mathbb{N}}$ *converges* to a real number $\mathbf{x}$, denoted $\mathbf{x_n} \to \mathbf{x}$, just in case $\forall \epsilon > 0 \, \exists i \, \forall j (|\mathbf{x} - \mathbf{x_{i+j}}| < \epsilon)$.

We may imbed the rationals in the reals by identifying a rational number q with the real number $\mathbf{q} = \{q_k = q\}_{k \in \mathbb{N}}$, and say that a real number $\mathbf{x}$ is *rational* if $\mathbf{x} = \mathbf{q}$ for some $q \in \mathbb{Q}$. It can be shown in RCA_0 that $\mathbb{R}$ satisfies all the usual axioms of an ordered field.

While we cannot prove that the reals are complete[4], we can prove a slightly weaker completeness property.

Theorem I.5. In RCA_0 one can prove that the real numbers are nested interval complete, i.e. if $\{\mathbf{a_n} \in \mathbb{R}\}_{n \in \mathbb{N}}$ and $\{\mathbf{b_n} \in \mathbb{R}\}_{n \in \mathbb{N}}$ are sequences of real numbers such that $\mathbf{a_n} \leq \mathbf{a_{n+1}} \leq \mathbf{b_{n+1}} \leq \mathbf{b_n}$ for all $n \in \mathbb{N}$, and such that $\mathbf{b_n} - \mathbf{a_n} \to 0$, then there exists a real number $\mathbf{x}$ such that $\mathbf{a_n} \leq \mathbf{x} \leq \mathbf{b_n}$ for all n.

Proof. Let $\mathbf{a_n} = \{a_{n,k} \in \mathbb{Q}\}_{k \in \mathbb{N}}$ and $\mathbf{b_n} = \{b_{n,k} \in \mathbb{Q}\}_{k \in \mathbb{N}}$ for all $n \in \mathbb{N}$. Define

$$X_k = \{m \,|\, (m \geq k+2) \wedge (b_{m,m} - a_{m,m} \leq 2^{-k+2})\},$$

which exists by Δ^0_1 comprehension. Because $\mathbf{b_n} - \mathbf{a_n} \to 0$, X_k is non-empty for each $k \in \mathbb{N}$. By Theorem I.1 (iv) and (v), there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that

$$f(k) = \text{least } m \text{ such that } m \in X_k.$$

Define $\mathbf{x} = \{x_k = a_{f(k),f(k)}\}_{k \in \mathbb{N}}$. By definition, $\mathbf{x}$ is a real number and $\mathbf{a_n} \leq \mathbf{x} \leq \mathbf{b_n}$ for all n.$\Box$

Real Numbers in ACA_0

Theorem I.6. ACA_0 is strong enough to prove that $\mathbb{R}$ is complete and that $[0,1]$ is sequentially compact.

Proof. We will first prove the sequential compactness of $[0,1]$. Let $\{\mathbf{x_n} \in [0,1]\}_{n \in \mathbb{N}}$ be a sequence of real numbers in $[0,1]$. We must show that there exists a subsequence that converges to a real number $\mathbf{x}$ in $[0,1]$. Let

$$\phi(k,i) = \forall N \exists n > N((i < 2^k) \wedge (i * 2^{-k} \leq \mathbf{x_n} \leq (i+1) * 2^{-k})).$$

[4] In fact, as Main Theorem I asserts, the completeness of the reals is equivalent to ACA_0, which is strictly stronger than RCA_0.

$\phi(k,i)$ says that infinitely many $\mathbf{x_n}$ lie in the interval $[i * 2^{-k}, (i+1) * 2^{-k}] \subset [0,1]$. Because $0 \leq \mathbf{x_n} \leq 1$ for all n, infinitely many $\mathbf{x_n}$ must lie in at least one of these intervals. Thus $\phi(k,i)$ for at least one i for each k. Now let

$$f = \{(k,i) \mid \phi(k,i) \wedge \neg\exists j((j > i) \wedge \phi(k,j))\},$$

which exists by arithmetical comprehension. f is a well defined function because $(k,i) \in f$ exists and is unique for each k by definition.

Let $\mathbf{x} = \{x_k = f(k) * 2^{-k}\}_{k \in \mathbb{N}}$. $\mathbf{x}$ is a real number because each rational number x_k with $k > N$ will lie in $[f(N) * 2^{-N}, (f(N)+1) * 2^{-N}]$. $0 \leq x_k \leq 1$ for all k, so $\mathbf{x} \in [0,1]$. Now define another function

$$g(k+1) = \text{least } n \text{ such that } (n > g(k)) \wedge (|\mathbf{x} - \mathbf{x_n}| \leq 2^{-k}),$$

which exists by Theorem I.1 and because infinitely many $\mathbf{x_n}$ lie within 2^{-k} of $\mathbf{x}$ for all k by definition. The subsequence $\{\mathbf{x_{g(k)}}\}_{k \in \mathbb{N}}$ converges to $\mathbf{x}$. Thus, $[0,1]$ is sequentially compact.

Now we shall show that $\mathbb{R}$ is complete. In other words, we must show that any *Cauchy sequence*, i.e. a sequence of reals $\{\mathbf{x_n} \in \mathbb{R}\}_{n \in \mathbb{N}}$ such that $\forall \epsilon > 0\, \exists m\, \forall n(m < n \rightarrow |x_m - x_n| < \epsilon)$, converges to a real number $\mathbf{x}$. Now it is clear from the definition that every Cauchy sequence is bounded, so by linearly rescaling we may take the sequence to lie entirely in $[0,1]$. The last result implies that a subsequence of this scaled sequence converges. However, if a subsequence of a Cauchy sequence converges, then the entire sequence converges to the same number. Thus, after reversing the scaling process, we have found an $\mathbf{x} \in \mathbb{R}$ such that $\{\mathbf{x_n}\} \rightarrow \mathbf{x}$.□

Theorem I.7. ACA_0 is equivalent to the completeness of $\mathbb{R}$ and the sequential compactness of $[0,1]$ over RCA_0.

Proof. We have already shown that these two theorems may be proven in ACA_0. Therefore, we need only find reversals. That is, we must prove that given RCA_0 and either of these two theorems, we can show that arithmetical comprehension holds. As we saw in the proof of the previous theorem, the sequential compactness of $[0,1]$ implies the completeness of $\mathbb{R}$. Therefore, it is sufficient to find a reversal for the completeness of $\mathbb{R}$.

Working in RCA_0, assume that $\mathbb{R}$ is complete. Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be an arbitrary function. Let

$$\mathbf{x_n} = \sum_{i=0}^{n} 2^{-f(i)}.$$

$\{\mathbf{x_n}\}$ is a bounded, increasing sequence of real numbers, so it is Cauchy. By the completeness of $\mathbb{R}$, $\{\mathbf{x_n}\} \rightarrow \mathbf{x}$ for some $\mathbf{x} \in \mathbb{R}$. Having this number $\mathbf{x}$ in hand allows us to effectively bound our search for a number $i \in \mathbb{N}$ such that $f(i) = k$. That is, we know that for all k,

$$\exists i(f(i) = k) \leftrightarrow \forall n(|\mathbf{x_n} - \mathbf{x}| < 2^{-k} \rightarrow \exists i \leq n(f(i) = k)).$$

However, this equivalent reformulation of k being in the range of f is Π^0_1, while the original formulation is Σ^0_1. Therefore, we may define

$$X = \{k \,|\, \exists i(f(i) = k)\},$$

which exists by Δ^0_1 comprehension. We have constructed a set that is equal to the range of an arbitrary function f. By Lemma I.4, this implies arithmetical comprehension.□

Real Numbers in WKL$_0$

Following Main Theorem I, we wish to show that WKL$_0$ is equivalent to the compactness of $[0,1]$ over RCA$_0$. To say that $[0,1]$ is *compact* is to say that given a *countable covering of* $[0,1]$, i.e. sequences of real numbers $\{\mathbf{a_n} \in \mathbb{R}\}_{n\in\mathbb{N}}$ and $\{\mathbf{b_n} \in \mathbb{R}\}_{n\in\mathbb{N}}$ such that for any $\mathbf{x} \in [0,1]$ there exists $i \in \mathbb{N}$ such that $\mathbf{a_i} \leq \mathbf{x} \leq \mathbf{b_i}$, there is a *finite subcovering of* $[0,1]$, i.e. there exists N such that for any $\mathbf{x} \in [0,1]$ there exists $i < N$ such that $\mathbf{a_i} \leq \mathbf{x} \leq \mathbf{b_i}$. We will first prove that $[0,1]$ is compact working in WKL$_0$, and then we will find a reversal.

Theorem I.8. WKL$_0$ is strong enough to prove the compactness of $[0,1]$.

Proof. First we will reduce to the special case where $\mathbf{a_n} = a_n \in \mathbb{Q}$ and $\mathbf{b_n} = b_n \in \mathbb{Q}$. Let

$$\phi(q,r) = q \in \mathbb{Q} \wedge r \in \mathbb{Q} \wedge \exists i(\mathbf{a_i} < q < r < \mathbf{b_i}).$$

$\phi(q,r)$ is Σ^0_1, so by Corollary I.3, there exists a function $f : \mathbb{N} \to \mathbb{Q} \times \mathbb{Q}$ such that

$$\forall q \forall r(\phi(q,r) \leftrightarrow \exists n((q,r) = f(n))).$$

Without loss of generality, we may take $(a_n, b_n) = f(n)$.

We proceed by finding, for each $n \in \mathbb{N}$, a partition of $[0,1]$ into 2^n pieces indexed by the set of binary sequences $s \in 2^{<\mathbb{N}}$ of length $\ell(s) = n$. Let

$$c_s = \sum_{i=0}^{\ell(s)-1} \frac{s_i}{2^{i+1}}$$

and

$$d_s = c_s + \frac{1}{2^{\ell(s)}}.$$

$c_{(0,\ldots,0)} = 0$ and $d_{(1,\ldots,1)} = \sum_{i=0}^{n-1} 2^{-i+1} + 2^{-\ell n} = 1$, where n is the number of 1's, so $[c_s, d_s]$ do in fact partition $[0,1]$ for each n. Note that if $s \subseteq t$, then $[c_t, d_t] \subseteq [c_s, d_s]$. We will now define a tree T based on these partitions and the countable covering of $[0,1]$ by rational intervals. Let

$$T = \{s \in 2^{<\mathbb{N}} \,|\, \neg\exists i \leq \ell(s)(a_i < c_s < d_s < b_i)\},$$

which exists by Σ^0_0 comprehension.

We claim that there is no path through T. Assume otherwise that there is a path $f : \mathbb{N} \to \{0,1\}$ through T. We will associate f with a real number in $[0,1]$ by using its binary representation. That is, define

$$\mathbf{x_f} = \{\sum_{i=0}^{n} \frac{f(i)}{2^{i+1}} \in \mathbb{Q}\}_{n \in \mathbb{N}}.$$

We have $\mathbf{x_f} \in [0,1]$ and $\mathbf{x_f}$ is the unique number such that $\mathbf{x_f} \in [c_{(f(0),\ldots,f(n))}, d_{(f(0),\ldots,f(n))}]$ for all $n \in \mathbb{N}$ by Σ^0_1 induction. Because $\{(a_n, b_n)\}$ cover $[0,1]$, there exists i such that $a_i < \mathbf{x_f} < b_i$. Because $\mathbf{x_f}$ is the only number that lies in $[c_{(f(0),\ldots,f(n))}, d_{(f(0),\ldots,f(n))}]$ for all n, and because $s \subseteq t$ implies $[c_t, d_t] \subseteq [c_s, d_s]$, we may find $N \geq i$ such that
$a_i < c_{(f(0),\ldots,f(N))} < d_{(f(0),\ldots,f(N))} < b_i$. This, however, implies that $(f(0), \ldots, f(N)) \notin T$, by the definition of T, which contradicts the fact that f is a path.

We have shown that there is no path through T. By weak König's lemma, this implies that T is finite. Let N be larger than the length of any binary sequence in T. We thus have, by the definition of T, that

$$\forall s \in 2^{<\mathbb{N}}(\ell(s) = N \to \exists i \leq N(a_i < c_s < d_s < b_i)).$$

However, $\{[c_s, d_s]\}_{\ell(s)=N}$ cover $[0,1]$, therefore $\{(a_0, b_0), \ldots, (a_N, b_N)\}$ is a finite subcover of $[0,1]$.□

Definitions. In what follows we will call a real number $\mathbf{x} \in [0,1]$ a *Cantor point* if there exists a path $f : \mathbb{N} \to \{0,1\}$ through $2^{<\mathbb{N}}$ such that

$$\mathbf{x} = \{\sum_{i=0}^{n} \frac{2f(i)}{3^{i+1}} \in \mathbb{Q}\}_{n \in \mathbb{N}}.$$

If no such path exists, then we will say that $\mathbf{x} \in [0,1]$ is a *non-Cantor point*.

Additionally, for any binary tree $T \subset 2^{<\mathbb{N}}$, define the set of *leaves of* T to be

$$L_T = \{s \in T \mid s \diamond (0) \notin T \wedge s \diamond (1) \notin T\},$$

which exists for any given T by Σ^0_0 comprehension.

Lemma I.9. Over RCA_0 for a given tree T, if L_T is finite, then either T is finite or it has a path.

Proof. Assume that T is infinite, but that L_T is finite. We shall show that T has a path. Consider the set of binary sequences

$$X = \{s \in T \mid \exists t \in L_T(s \subseteq t)\},$$

which exists by Σ^0_0 comprehension because L_T is finite. For any given $t \in L_T$, there can only be finitely many subsequences of t. Because the finite union of finite sets is finite, this implies that X is finite. Because T is infinite, there must exist a binary sequence $s^0 \in T$ such that $s^0 \notin X$. By definition of X, there exists $s^1 \in T$ such that s^1 is either $s^0 \diamond (0)$ or $s^0 \diamond (1)$, and $s^1 \notin X$. By Σ^0_0 induction there exists s^n for all n such that $s^n \in T$ and s^{n+1} is either $s^n \diamond (0)$ or $s^n \diamond (1)$. Let $f : \mathbb{N} \to \{0, 1\}$ to be either $f(n) = s^0_n$ if $n < \ell(s^0)$ or $f(n) = s_n^{n-\ell(s^0)+1}$ otherwise. By the above, f is a path through T.□

Theorem I.10. WKL$_0$ is equivalent to the compactness of $[0, 1]$ over RCA$_0$.

Proof. By Theorem I.8, it is sufficient to find a reversal for the compactness of $[0, 1]$. Working in RCA$_0$, assume that $[0, 1]$ is complete. Let T be a binary tree such that there are no paths through T. Our goal is to show that T must be finite. By Lemma I.9, it is sufficient to show that L_T is finite.

Define the following sequences of real numbers in $[0, 1]$ indexed by binary sequences $s \in 2^{<\mathbb{N}}$:

$$\begin{aligned}
\mathbf{a_s} &= \sum_{i=0}^{\ell(s)-1} \frac{2s_i}{3^{i+1}} \\
\mathbf{b_s} &= \mathbf{a_s} + 3^{-\ell(s)} \\
\mathbf{c_s} &= \mathbf{a_s} - 3^{-\ell(s)-1} \\
\mathbf{d_s} &= \mathbf{b_s} + 3^{-\ell(s)-1}
\end{aligned}$$

For any non-Cantor point $\mathbf{x}$ there exists $s \in 2^{<\mathbb{N}}$ such that $\mathbf{x} \in (\mathbf{b_{s\diamond(1)}}, \mathbf{a_{s\diamond(0)}})$ while no Cantor points will lie in any of these intervals. This may be verified by formalizing in RCA$_0$ any standard presentation of the Cantor set (see, for example, [3]). Thus, the intervals $X = \{(\mathbf{b_{s\diamond(1)}}, \mathbf{a_{s\diamond(0)}})\}_{s\in 2^{<\mathbb{N}}}$ cover precisely the non-Cantor points of $[0, 1]$.

We claim that the set $Y = \{(\mathbf{c_s}, \mathbf{d_s})\}_{s\in L_T}$ consists of pairwise disjoint intervals that cover at least the Cantor points of $[0, 1]$. From the definition of $\mathbf{c_s}$ and $\mathbf{d_s}$, any two intervals $(\mathbf{c_s}, \mathbf{d_s})$ and $(\mathbf{c_t}, \mathbf{d_t})$ are disjoint unless $s \subseteq t$ or $t \subseteq s$. However, no two leaves of a tree may overlap in this way, so we have that the intervals given above are pairwise disjoint.

To see that the intervals in Y cover at least the Cantor points of $[0, 1]$, we will assume otherwise and show that this implies the existence of a path for T. Let $\mathbf{x} = \{\sum_{i=0}^{n} \frac{2f(i)}{3^{i+1}}\}_{n\in\mathbb{N}}$ be a Cantor point that does not lie in any interval $(\mathbf{c_s}, \mathbf{d_s})$ for $s \in L_T$. Then, f is a path through T because $\mathbf{x} \in (\mathbf{c}_{(f(0),\ldots,f(n))}, \mathbf{d}_{(f(0),\ldots,f(n))})$ for all $n \in \mathbb{N}$ by Δ^0_1 induction, so $(f(0), \ldots, f(n)) \in T$ for all n.

Hence, we have shown that the intervals $X \cup Y$ together form a countable cover of $[0, 1]$. By compactness, there should be a finite subcover. However, each of the intervals in Y is needed because they are pairwise disjoint and each interval contains at least one Cantor point $\mathbf{a_s} \in (\mathbf{c_s}, \mathbf{d_s})$. Thus Y must be a finite set. This implies that L_T is finite, which in turn implies that T is finite, completing the proof.□

Proof of Main Theorem I. The theorem follows directly from Theorems I.5, I.7, and I.10.□.

Further Results

In this section we will list several other standard reverse mathematical results and briefly discuss the remaining standard subsystems of second order arithmetic used in reverse mathematics, ATR_0 and $\Pi^1_1 - \text{CA}_0$. Proofs of all of these theorems may be found in [1].

Theorem I.11. The following theorems can be proven in RCA_0:

(i) The real line satisfies the intermediate value property.

(ii) The Baire category theorem.

(iii) A version of the Tietze extension theorem for complete separable metric spaces.

(iv) A strong version of the soundness theorem in mathematical logic.

(v) The algebraic closure for any countable field exists.

(vi) The Banach/Steinhaus theorem.

Theorem I.12. The following are equivalent to WKL_0 over RCA_0:

(i) The Heine/Borel theorem for compact metric spaces.

(ii) Several properties of continuous functions on compact metric spaces including uniform continuity, the maximum principle, Riemann integrability, and Weierstrass approximation.

(iii) The completeness and compactness theorems of mathematical logic.

(iv) The uniqueness of the algebraic closure for countable fields.

(v) The Brouwer and Schauder fixed point theorems.

(vi) The Peano existence theorem for solutions of ordinary differential equations.

(vii) The separable Hahn/Banach theorem.

Theorem I.13. The following are equivalent to ACA_0 over RCA_0:

(i) Every countable vector space over $\mathbb{Q}$ has a basis.

(ii) Every countable commutative ring has a maximal ideal.

(iii) The divisible closure of an arbitrary countable Abelian group is unique.

(iv) König's lemma for subtrees of $\mathbb{N}^{<\mathbb{N}}$

(v) Ramsey's theorem for colorings of $[\mathbb{N}]^3$.

ATR_0, or *arithmetical transfinite recursion with limited induction*, is a subsystem of second order arithmetic that is logically stronger than ACA_0 and the other systems we discussed in this chapter. The system may be described informally as taking ACA_0 and allowing for the transfinite iteration of the Turing jump operator along any countable well-ordering.

Theorem I.14. The following are equivalent to ATR_0 over RCA_0:

(i) Lusin's separation theorem.

(ii) The Borel domain theorem.

(iii) The perfect set theorem.

(iv) The existence of Ulm resolutions.

(v) The comparability of countable well-orderings.

(vi) The open and clopen Ramsey theorems.

$\Pi^1_1 - \mathrm{CA}_0$, or Π^1_1 *comprehension with limited induction*, is the strongest subsystem of second order arithmetic considered in standard reverse mathematics. It is defined similarly to RCA_0 and ACA_0 except recursive and arithmetical comprehension are replaced with Π^1_1 *comprehension*, i.e. the comprehension schema applies to formulae of the form $\forall X(\phi(X))$ where X is a set variable and $\phi(X)$ is arithmetical.

Theorem I.15. The following are equivalent to $\Pi^1_1 - \mathrm{CA}_0$ over RCA_0:

(i) The Cantor/Bendixson theorem for closed sets.

(ii) Kondo's theorem on coanalytic uniformization.

(iii) Silver's theorem on Borel equivalence relations.

(iv) Every countable Abelian group is a direct sum of a divisible group and a reduced group.

(v) The Δ^0_2 Ramsey theorem.

As can be seen from this list of results, reverse mathematics provides a wealth of information about the equivalencies and relative logical strengths of many of the theorems of mathematics. It is surprising that all of these theorems can be seen as equivalent up to constructive mathematics to basic axioms that describe what counts as a set. Furthermore, it is quite intriguing that all of these theorems can be arranged in a linear ordering of logical strength starting from RCA_0 and working up to $\Pi^1_1 - \mathrm{CA}_0$.

Finally, it may be interesting to note that each of the five standard subsystems of second order arithmetic that arise in the study of reverse mathematics can be seen as corresponding to different philosophical approaches to the foundations of mathematics. RCA_0 can be associated with the constructivism of Bishop, WKL_0 with the finitistic reductionism of Hilbert, ACA_0 with the predicativism of Weyl and Feferman, ATR_0 with the predicative reductionism of Friedman and Simpson, and $\Pi^1_1 - \mathrm{CA}_0$ with the impredicativity of Feferman and others. These connections are explored in more detail in [1].

Reverse mathematics, thus, gives deep insight into the nature of many theorems of ordinary mathematics, into the relations and equivalencies between these theorems, into the axioms that we may choose to consider and the nature of the set, and into several of the philosophical approaches to the foundations of mathematics. In the following two chapters we will explore some interesting theorems of reverse mathematics that go beyond the standard results and that serve to further illustrate these themes.

Chapter II - The Reverse Mathematics of Hilbert's Basis Theorem

In this chapter we will prove a unique theorem of reverse mathematics. Namely, we will show that Hilbert's basis theorem is equivalent to the well-ordering of ω^ω over RCA_0. This chapter is based on the proof by Simpson in [4], although the presentation and structure have been significantly altered.

Definitions. A *countable ring* A is a tuple $(|A|, +_A, *_A, 0_A, 1_A)$ where $|A|$ is a set of natural numbers - the set of codes for elements of A - $+_A$ and $*_A$ are functions from $|A| \times |A|$ to $|A|$, and 0_A and 1_A are distinct distinguished elements of $|A|$ such that these objects obey the usual axioms for a commutative ring with unit. Standard ring notation will be freely used in place of the explicit notation using $|\cdot|$ and the subscript A.

The *polynomial ring in m variables* associated with a countable ring A, which is denoted $A[x_1, \ldots, x_m]$, is a countable ring whose elements are (codes for) finite sums of the form $\sum a_{i_1,\ldots,i_m} x_1^{i_1} \cdots x_m^{i_m}$. Addition, multiplication and the additive and multiplicative identities are defined as usual for polynomials.

A *monomial* is an element of $A[x_1, \ldots, x_m]$ that consists of only one term and does not include the coefficient of this term i.e. an expression of the form $x_1^{i_1} \cdots x_m^{i_m}$. The *monomial ordering* is a total-ordering on the monomials given by first ordering by total degree (the sum $i_1 + \cdots + i_m$) and then ordering lexicographically. For any polynomial $P \in A[x_1, \ldots, x_m]$, the monomial that appears in P and which is greatest under this ordering is called the *leading monomial* of P. A monomial $M = x_1^{i_1} \cdots x_m^{i_m}$ is said to *divide* another monomial $N = x_1^{j_1} \cdots x_m^{j_m}$ if $i_k \leq j_k$ for all k from 1 to m.

A countable ring A is said to be *Hilbertian* if it possesses the following property: For every sequence of elements $\{a_k \in A\}_{k \in \mathbb{N}}$ there exists a natural number N such that for all k there exist $f_0, \ldots, f_N \in A$ such that $a_k = f_0 * a_0 + \cdots + f_N * a_N$. In other words, a countable ring is Hilbertian iff all sequences of its elements are finitely generated.[5]

The version of *Hilbert's basis theorem* considered in this chapter is a theorem which states that for all countable rings A and natural numbers $m > 0$, $A[x_1, \ldots, x_m]$ is Hilbertian.

The set of *ordinals up to ω^ω*, denoted O, is the set of (codes for) finite sequences of natural numbers along with a special code $|\omega^\omega|$, which can be arbitrary as long as it is distinct from the other elements of O. The code $|\alpha| = (\alpha_0, \ldots, \alpha_n)$ is intended to represent the ordinal $\alpha = \alpha_n * \omega^n + \alpha_{n-1} * \omega^{n-1} + \cdots + \alpha_0$ with $|\omega^\omega|$ of course representing ω^ω. The ordinals in O have the usual lexicographical ordering with ω^ω as the largest element.

[5] In RCA_0 it is possible to show that a countable ring is Hilbertian just in case all Σ^0_1 *ideals* are finitely generated where a Σ^0_1 ideal is a sequence $\{a_k \in A\}_{k \in \mathbb{N}}$ such that (1) $a_k \neq 0$ for all k (2) for all i and j there exists k such that $a_k = a_i + a_j$ and (3) for all i and all $a \in A$ there exists k such that $a_k = a * a_i$. In ACA_0 one can show that Σ^0_1 ideals are the same as ideals as usually construed, i.e. subsets of A that are closed under addition and multiplication by arbitrary elements of A. See [4].

The *natural sum* and *natural product* of ordinals are *commutative* binary operations on ordinals, defined by first ordering the summands or factors from largest to smallest and then taking the sum or product as it is usually defined for ordinals. For example, the natural sum of $\alpha = \alpha_m * \omega^m + \alpha_{m-1} * \omega^{m-1} + \cdots + \alpha_0$ and $\beta = \beta_m * \omega^m + \beta_{m-1} * \omega^{m-1} + \cdots + \beta_0$ where $m > n$ is simply

$$\alpha + \beta = \beta_m * \omega^m + \beta_{m-1} * \omega^{m-1} + \cdots + \beta_{n+1} * \omega^{n+1} + (\alpha_n + \beta_n) * \omega^n + \cdots + \alpha_0 + \beta_0.$$

To say that an ordinal $\eta \in O$ is *well-ordered* is to say that there does not exist a sequence $\{\eta_k \in O\}_{k \in \mathbb{N}}$ such that $\eta_0 = \eta$ and $\eta_{k+1} < \eta_k$ for all k.

Main Theorem II. Hilbert's basis theorem and the well-ordering of ω^ω are equivalent over RCA$_0$.

Remarks. As we saw above for the purposes of this chapter Hilbert's basis theorem just says that for all $m \in \mathbb{N}$ and for all countable rings A, $A[x_1, \ldots, x_m]$ is Hilbertian. Furthermore, it is clear that the well-ordering of ω^ω is equivalent to the well-ordering of ω^m for all $m \in \mathbb{N}$. Therefore, it is sufficient to prove that for any given $m \in \mathbb{N}$, the following are equivalent over RCA$_0$:

(1) For any countable ring A, $A[x_1, \ldots, x_m]$ is Hilbertian.
(2) ω^m is well-ordered.

We shall begin by proving that (1) implies (2).

Theorem II.1. Over RCA$_0$ for fixed m, if $A[x_1, \ldots, x_m]$ is Hilbertian for some A, then ω^m is well-ordered.

Proof. Let $\{\eta_k \in O\}_{k \in \mathbb{N}}$ be a sequence of ordinals beginning with ω^m and with $\eta_k = \eta_{k,m} * \omega^{m-1} + \eta_{k,m-1} * \omega^{m-2} + \cdots + \eta_{k,1} < \omega^m$ for $k > 0$. Disregarding the first element in the sequence, create a sequence of monomials in $A[x_1, \ldots, x_m]$ by setting $M_k = x_1^{\eta_{k,1}} \cdots x_m^{\eta_{k,m}}$. Because $A[x_1, \ldots, x_m]$ is Hilbertian, there exists N such that $M_{N+1} = g_1 * M_1 + \cdots + g_N * M_N$ with $g_1, \ldots, g_N \in A[x_1, \ldots, x_m]$.

We claim that M_{N+1} divides M_i for some $i \leq N$. Assume otherwise. Because M_{N+1} does not divide M_1, and because the sum $g_1 * M_1 + \cdots + g_N * M_N$ must add up to a monomial, the term $g_1 * M_1$ must be exactly canceled by the other terms. This reasoning holds for all $i \leq N$, which implies that $M_{N+1} = 0$. However, M_{N+1} is non-zero by construction. Therefore, there exists $i \leq N$ such that M_{N+1} divides M_i.

This in turn implies that $\eta_{N+1,j} \leq \eta_{i,j}$ for all j from 1 to m. However, this means that $\eta_{N+1} \leq \eta_i$. Therefore, $\{\eta_k\}$ cannot be a strictly decreasing sequence. Because $\{\eta_k\}$ was arbitrary, ω^m must be well-ordered.□

We will now show that (2) implies (1) over RCA$_0$. In order to accomplish this, we will proceed in three steps. First, we will reduce the Hilbertianness of $A[x_1, \ldots, x_m]$ to a similar condition on sequences of monomials. Second, we will demonstrate an equivalent characterization of this condition on sequences of monomials. Finally, we will show how any counter-example to this reduction of the Hilbertianness of $A[x_1, \ldots, x_m]$ can be used to construct a counter-example to the well-orderedness of ω^m.

Theorem II.2. Over RCA$_0$ for a given polynomial ring $A[x_1, \ldots, x_m]$, if $A[x_1, \ldots, x_m]$ satisfies

$(*)$ For every sequence of monomials $\{M_k \in A[x_1, \ldots, x_m]\}_{k\in\mathbb{N}}$ there exists N such that for all k there exists $i \leq N$ such that M_i divides M_k,

then $A[x_1, \ldots, x_m]$ is Hilbertian.

Remarks. From the cancellation argument in the proof of Theorem II.1, we can see that condition $(*)$ is equivalent to the sequence $\{M_k\}$ being finitely generated. This theorem shows, then, that if all sequences of monomials are finitely generated, then all sequences of polynomials must be finitely generated as well.

Proof. Let $\{P_k \in A[x_1, \ldots, x_m]\}_{k\in\mathbb{N}}$ be a sequence of polynomials. Note that the formula "$H = F_0 * P_0 + \cdots + F_n * P_n$" is Σ^0_0 because the equality here is just numerical equality between codes in $|A[x_1, \ldots, x_m]|$, and $*_{A[x_1,\ldots,x_m]}$ and $+_{A[x_1,\ldots,x_m]}$ act as parameters. Therefore, the formula $\phi(H) \equiv$ "There exist $n \in \mathbb{N}$ and $F_0, \ldots, F_n \in A[x_1, \ldots, x_m]$ such that $H = F_0 * P_0 + \cdots + F_n * P_n$" is a Σ^0_1 formula. Thus by Corollary I.3, we can conclude in RCA$_0$ that there exists a sequence $\{H_k \in A[x_1, \ldots, x_m]\}_{k\in\mathbb{N}}$ that enumerates precisely the polynomials in $A[x_1, \ldots, x_m]$ that are finite linear combinations of the P_k. Note that if $\{H_k\}$ is finitely generated, then $\{P_k\}$ must also be finitely generated because $\{P_k\} \subset \{H_k\}$ and every H_k is a finite linear combination of the P_k.

Define $\{M_k \in A[x_1, \ldots, x_m]\}_{k\in\mathbb{N}}$ to be a sequence of monomials such that M_k is the leading monomial of H_k. By the supposition of $(*)$, there exists N such that for all k there exists $i \leq N$ such that M_i divides M_k.

We claim that $H_0, \ldots, H_N$ generate $\{H_k\}$, which we will prove by induction on the monomial ordering of the leading monomials, M_k. Given a fixed k, we know that there exists $i \leq N$ such that M_i divides M_k i.e. $M_k = M_i * N_k$ where N_k is another monomial. Necessarily for any $a \in A$, $H_k - aN_k * H_i$ is equal to H_l for some $l \in \mathbb{N}$. For some choice of a, a_k, the leading monomial of H_j is canceled by $a_k N_k * H_i$ hence H_l has a lesser leading monomial i.e. M_l comes before M_k in the monomial ordering. By the inductive hypothesis

$H_l = F_0 * H_0 + \cdots + F_N * H_N$ for some $F_0, \ldots, F_N \in A[x_1, \ldots, x_m]$. Thus,

$$H_k = F_0 * H_0 + \cdots + (F_i + a_k N_k) * H_i + \cdots + F_N * H_N.$$

By induction $\{H_k\}$ is finitely generated. Hence, $\{P_k\}$ is finitely generated, so $A[x_1, \ldots, x_m]$ is Hilbertian.□

Theorem II.3. For a given polynomial ring $A[x_1, \ldots, x_m]$, condition $(*)$ is equivalent over RCA_0 to

$(*')$ For every sequence of monomials $\{M_k \in A[x_1, \ldots, x_m]\}_{k \in \mathbb{N}}$ there exist i and k such that $i < k$ and M_i divides M_k.

Proof. That $(*)$ implies $(*')$ is clear by taking $k = N + 1$.

Assume $A[x_1, \ldots, x_m]$ satisfies condition $(*')$. Fix a sequence of monomials $\{M_k\}$. Let X be the set of natural numbers k such that there does not exist $i < k$ such that M_i divides M_k. This set exists by Σ^0_0 comprehension because the existential quantifier is a bounded quantifier.

We claim that for all natural numbers k there exists an $i \in X$ such that M_i divides M_k. Assume for the purpose of contradiction that there exists a $k \in \mathbb{N}$ such that whenever M_i divides M_k, then i is not an element of X. We proceed by finding an infinite regress of monomials M_{i_j} that divide M_k. Let $i_0 = k$. By the inductive hypothesis we assume that M_{i_j} divides M_k. i_j is therefore not an element of X. By definition this means we can find $i_{j+1} < i_j$ such that $M_{i_{j+1}}$ divides M_k. This creates an infinite regress of the natural numbers i_j, so for all $k \in \mathbb{N}$ there exists $i \in X$ such that M_i divides M_k.

Next, we claim that X is finite. Suppose otherwise. By Corollary I.2, there exists a monotonic function $\pi_X : \mathbb{N} \to X$ that enumerates the elements of X. Consider the infinite subsequence $\{M_{\pi_X(k)}\}$. By $(*')$ there must exist $i < k$ such that $M_{\pi_X(i)}$ divides $M_{\pi_X(k)}$. However, having $\pi_X(i) < \pi_X(k)$ and $M_{\pi_X(i)}$ divides $M_{\pi_X(k)}$ contradicts the definition of X. Therefore, X must be finite.

By the second claim, X is finite, so it has an upper bound N. By the first claim, for all k there exists $i \leq N$ such that M_i divides M_k. This holds for arbitrary $\{M_k\}$, so therefore $A[x_1, \ldots, x_m]$ satisfies condition $(*)$.□

Definitions. In order to complete the proof of the main theorem, we require some definitions concerning the space $\mathbb{N}^m$ of all m-tuples of natural numbers. With u and v ordinals less than or equal to ω define the *interval* $[u, v)$ to be the set of natural numbers n such that $u \leq n < v$. An *m-box*, denoted $[\mathbf{u}, \mathbf{v}) = \prod_{i=1}^{m} [u_i, v_i) \subset \mathbb{N}^m$, is the Cartesian product of these intervals. Further define the *volume* of a countable union of m-boxes indexed by a set I to be

$$\Big|\bigcup_{[\mathbf{u},\mathbf{v})\in I}[\mathbf{u},\mathbf{v})\Big| = \sum_{[\mathbf{u},\mathbf{v})\in I}\prod_{i=1}^{m}(v_i - u_i)$$

where natural sums and natural products are used on the right.

Theorem II.4. The existence of a polynomial ring $A[x_1,\ldots,x_m]$ that does not satisfy condition $(*')$ implies over RCA_0 that ω^m is not well-ordered.

Proof. Let $\{M_k \in A[x_1,\ldots,x_m]\}_{k\in\mathbb{N}}$ be a sequence of monomials that does not satisfy the condition in $(*')$. In other words, $k < l$ implies that M_k does not divide M_l. We will use $\{M_k\}$ to construct a sequence of ordinals $\{\eta_k \in O\}_{k\in\mathbb{N}}$ such that $\eta_0 = \omega^m$ and $\eta_{k+1} < \eta_k$ for all k. The existence of such a sequence demonstrates that ω^m is not well-ordered by definition.

Roughly speaking, in order to construct this sequence of ordinals we will inductively create a partition of the space $\mathbb{N}^m$. Note that the collection of exponents of a monomial in $A[x_1,\ldots,x_m]$ can be identified with a point in $\mathbb{N}^m$. Because $k < l$ implies that M_k does not divide M_l, the exponents of each M_k specify some m-box in $\mathbb{N}^m$ in which none of the remaining exponents can lie. At each step, we will throw away this piece of the partition and define η_k to be the volume of what remains.

Let I_0, the initial partition of $\mathbb{N}^m$, be the trivial partition $\{\prod_i[0,\omega)\}$. Let

$$\eta_0 = |\prod_i[0,\omega)| = \omega^m.$$

Let $(j_{k,1},\ldots,j_{k,m}) \in \mathbb{N}^m$ be given by $M_k = x_1^{j_{k,1}}\cdots x_m^{j_{k,m}}$.

At each step take the m-box $[\mathbf{u}_k,\mathbf{v}_k) \in I_{k-1}$ such that $(j_{k,1},\ldots,j_{k,m}) \in [\mathbf{u}_k,\mathbf{v}_k)$ and split it into 2^m m-boxes made up of each combination of $[u_{k,i}, j_{k,i})$ and $[j_{k,i}, v_{k,i})$. Let I_k be the union of $I_{k-1} - \{[\mathbf{u}_k,\mathbf{v}_k)\}$ and these m-boxes except for the m-box given by $[j_{k,1}, v_{k,1}) \times \cdots \times [j_{k,m}, v_{k,m})$. Because for all $l > k$ we cannot have M_k divides M_l by hypothesis, the exponents for M_l can never lie in this removed piece. Therefore, the subsets in I_k partition a portion of $\mathbb{N}^m$ that contains the exponents for each remaining M_l. Finally, define

$$\eta_k = \Big|\bigcup_{[\mathbf{u},\mathbf{v})\in I_k}[\mathbf{u},\mathbf{v})\Big|.$$

It remains to be shown that $\eta_{k+1} < \eta_k$ for all k. To prove this, it is sufficient to show that the combined volume of the m-boxes that replace $[\mathbf{u}_k,\mathbf{v}_k)$ is strictly less than $|[\mathbf{u}_k,\mathbf{v}_k)|$. Let $a, b \in \mathbb{N}$ be given by $|[\mathbf{u}_k,\mathbf{v})_k| = a * \omega^b$. This means that for exactly b instances of i, $v_{k,i} = \omega$. Each m-box that is made up of $[u_{k,i}, j_{k,i})$ for at least one of these b choices of i will contribute less than ω^b to the volume. The remaining m-boxes will contribute some multiple $a' * \omega^b$ of ω. However, this a' must be strictly less than a because, ignoring all the infinite dimensions, these remaining $(m-b)$-boxes make up some strict subset of the finite $m-b$ dimensional portion of the original m-box. Therefore, $\eta_{k+1} < \omega^b + a' * \omega^b \leq a * \omega^b = \eta_k$.□

Proof of Main Theorem II. We have shown the following working in RCA_0. By Theorem II.1, the Hilbertianness of $A[x_1, \ldots, x_m]$ implies that ω^m is well-ordered. By Theorem II.4, if ω^m is well-ordered, then for every ring A, the polynomial ring $A[x_1, \ldots, x_m]$ satisfies condition $(*')$. Therefore, by Theorem II.3, every polynomial ring satisfies condition $(*)$. Hence, by Theorem II.2, $A[x_1, \ldots, x_m]$ is Hilbertian for any ring A. Thus, Theorems II.2-4 have shown that the well-orderedness of ω^m implies the Hilbertianness of $A[x_1, \ldots, x_m]$ for arbitrary A. The theorem follows from the remarks.□

Appendix to Chapter II

While we showed in Chapter II that Hilbert's basis theorem and the well-ordering of ω^ω are equivalent over RCA_0, we said nothing of whether these theorems can be proved in RCA_0. It turns out that they cannot, and that furthermore they cannot be proved in WKL_0. The complete proof of these facts is beyond the scope of this thesis. Therefore, we will use the following lemma without proof.[6]

Lemma A-1. Any function f that is provably recursive in WKL_0 and hence in RCA_0 is primitive recursive.

Let the Ackermann function $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined recursively by

$$A(n, m) = \begin{array}{l} n+1, \text{ if } m = 0 \\ A(m-1, 1), \text{ if } m > 0 \text{ and } n = 0 \\ A(m-1, A(m, n-1)), \text{ if } m > 0 \text{ and } n > 0 \end{array}$$

It is a well known fact that the Ackermann function is not primitive recursive (see, for example, [6]). Therefore, we have

Corollary A-2. The Ackermann function is not provably recursive in WKL_0 or RCA_0.

However, we also have the following lemma

Lemma A-3. The well-ordering of ω^ω implies the existence of the Ackermann function over RCA_0.

Proof Sketch. The Ackermann function $A(m, n)$ is computed by repeated "calls" to the function itself with different parameters. In order to prove that the function exists, it is sufficient to show that the calculation terminates after a finite number of steps. This can be done for a fixed value of m by associating a call to $A(m, n)$ with $(n+1) * \omega^m$ and noting that successive calls are always to lesser ordinals. Therefore, the well-ordering of ω^{m+1} implies that the function $A_m(n) = A(m, n)$ exists. The well-ordering of ω^ω implies the well-ordering of ω^m for all m, and hence the existence of the Ackermann function. For a complete proof see [7].

Thus, we have

Theorem A-4. The well-ordering of ω^ω and Hilbert's basis theorem cannot be proved in WKL_0 or RCA_0.

[6] For a model-theoretic proof, see [1]. For a proof-theoretic approach, see [5].

Chapter III- The Reverse Mathematics of the Hahn Embedding Theorem

The Hahn embedding theorem is an important result in abstract algebra that describes ordered abelian groups. Namely it says that every ordered abelian group is isomorphic to an ordered subgroup of some sum of copies of $(\mathbb{R}, \leq_{\mathbb{R}})$, the real numbers under the standard ordering. In this chapter, we will study the reverse mathematics of a formalization of Hahn's embedding theorem in second order arithmetic. In particular, we will show that Hahn's embedding theorem implies ACA_0 over RCA_0, and hence that the theorem is not effective. That is, there exists a computable ordered abelian group for which one cannot construct a computable embedding into a sum of copies of $\mathbb{R}$. The results in this chapter and their presentation follow primarily [8] with some additions from [9].

Definitions. An *abelian group* is a tuple $(|G|, +_G, |0_G|)$ where $|G| \subset \mathbb{N}$ is the set of codes for elements of the group, $+_G : |G| \times |G| \to |G|$ is a binary operation with identity $|0_G| \in |G|$ satisfying the usual axioms of an abelian group. Subgroups $H \lhd G$, cosets $g + H$ and quotient groups G/H are also defined as usual. A *linear order* is a tuple $(|T|, \leq_T)$ where $|T| \subset \mathbb{N}$ is a set of codes for elements of T, and $\leq_T$ is a relation between elements of T satisfying the usual axioms of a total linear ordering. An *ordered abelian group* is a tuple $(|G|, +_G, |0_G|, \leq_G)$ such that $(|G|, +_G, |0_G|)$ is an abelian group and $(|G|, \leq_G)$ is a linear order.

The *positive cone of an ordered abelian group* G, $P \subset G$ is defined to be the set $P = \{g \in G \,|\, 0 \leq g\}$, which exists for any given G by Σ^0_0 comprehension with $\leq_G$ acting as a parameter. We may also define an ordering on an abelian group G by specifying its positive cone by taking $g \leq h$ just in case $h - g \in P$. Indeed, it is easy to see that any subgroup $P \subset G$ such that P is *pure*, i.e. $P \cap \{g \in G \mid -g \in P\} = \{0\}$, and *full*, i.e. $P \cup \{g \in G \mid -g \in P\} = G$, is the positive cone for some ordering on G.

For a linear order T, a subset $S \subset T$ is said to be *well-ordered* provided that any subset $U \subset S$ has a T-minimal element u_0, i.e. $u \in U$ implies $u_0 \leq_T u$. Furthermore, S is said to be *convex* provided that for any $a, b, t \in T$ if a and b are in S and $a \leq t \leq B$, then t is in S as well. If H is a convex subgroup of a ordered abelian subgroup G, then we may define the *induced order* $\leq_{G/H}$, on G/H by $a + H \leq_{G/H} b + H$ if and only if $a + H = b + H$ or $a <_G b$.

For any ordered abelian group G with positive cone P, we may define the *absolute value* function to be $|g| = g$ if $g \in P$, and $|g| = -g$ if $g \notin P$. For $n \in \mathbb{N}$ and $g \in G$, ng is defined to be the sum of n copies of g. For $a, b \in G$ we say that a is *Archimedean less than* b, denoted $a \ll b$, if $|na| < |b|$ for all $n \in \mathbb{N}$. If neither $a \ll b$ nor $b \ll a$, then we say that a and b are *Archimedean equivalent*, denoted $a \approx b$. Note that $a \ll b$ is a Π^0_1 formula while $a \approx b$ is Σ^0_1. If $a \approx b$ for all $a, b \in G - \{0_G\}$, then we say that G is an *Archimedean ordered group*. A special case of Hahn's embedding theorem is Hölder's theorem which says that any any Archimedean ordered group is isomorphic to a subgroup of $\mathbb{R}$. For a proof of Hölder's theorem in RCA_0 see [10].

Finally, for an ordered abelian group G, we say that $X \subset G$ is a *set of Archimedean representatives for* G if:

(1) For all $g \in G$, there exists $x \in X$ such that $x \approx g$, and
(2) for all $x, y \in X$ such that $x \neq y$, $x \not\approx y$.

We may now begin our study of the reverse mathematics of Hahn's embedding theorem by showing that a crucial part of the theorem, the existence of a set of Archimedean representatives for G, is equivalent to ACA_0 over RCA_0.

Lemma III.1. For any ordered abelian group G, the following are equivalent over RCA_0

(i) There exists a set of Archimedean representatives for G.

(ii) The set $A = \{(g,h) \in G \times G \,|\, g \approx h\}$ exists.

Proof. To see that (i) implies (ii), we begin by defining a function $\mathit{Rep} : G \to X$ defined by

$$\begin{aligned} \mathit{Rep} &= \{(g,x) \,|\, x \in X \wedge \exists n, m < 0(|g| \leq_G |nx| \wedge |x| \leq_G |mg|)\} \\ &= \{(g,x) \,|\, x \in X \wedge \forall y \in X(y \neq x \to (\forall n > 0(|g| \leq_G |ny|) \vee \forall n > 0(|y| \leq_G |ng|)))\}, \end{aligned}$$

which exists by Δ^0_1 comprehension with X acting as a parameter. Rep assigns to any element $g \in G$ its Archimedean representative in X. Therefore, we can simply define

$$A = \{(g,h) \in G \times G \,|\, \mathit{Rep}(g) = \mathit{Rep}(h)\},$$

which exists by Σ^0_0 comprehension.

To see that (ii) implies (i) simply note that the set

$$\{g \in |G| \,|\, \forall h <_{\mathbb{N}} g(h \in |G| \to (g,h) \notin A)\},$$

which exists by Σ^0_0 comprehension is a set of Archimedean representatives for G.□

Theorem III.2. The following are equivalent over RCA_0

(i) ACA_0.

(ii) For any ordered abelian group G, there exists a set of Archimedean representatives for G.

Proof. To see that (i) implies (ii) note that the set

$$\{g \in G \,|\, \forall n \in \mathbb{N}(n <_{\mathbb{N}} g \to (n \notin G \vee n \not\approx g))\},$$

which exists by Π^0_1 comprehension in ACA_0, is a set of Archimedean representatives for G.

Let $f : \mathbb{N} \to \mathbb{N}$ be an arbitrary function. To show that (ii) implies (i), we will construct an ordered abelian group G using the function f, and then use the existence of a set of Archimedean representatives for G to show that the range of f exists, which is sufficient to prove arithmetical comprehension by Lemma I.4.

Because the divisors of a given number are bounded by the number itself, primality can be expressed using a Σ^0_0 formula. Therefore, by Corollary I.3, we may enumerate the odd prime numbers as $\{p_m\}_{m\in\mathbb{N}}$. We will define G as an abelian group with countably infinitely many generators x_n satisfying the relations $p_m x_{2n} = x_{2n+1}$ if $f(m) = n$. To define this formally we encode the elements of G as finite sequences $g = (g_0, \dots, g_\ell)$ representing $\sum_{n=0}^{\ell} g_n x_n$. We further require that elements of G are *reduced*, that $g_\ell \neq 0$ and that there does not exist $2n < \ell$ and $p_m < |2g_{2n}|$ such that $f(m) = n$. The identity element 0_G, is given by the empty sum. Since the condition of being reduced is Σ^0_0, G is well-defined as a set.

Reducing an arbitrary sum is a straightforward process. For each $2n < \ell$ check if there is a prime $p_m < |2g_{2n}|$ such that $f(m) = n$. If we have $f(m) = n$, and $g_{2n} = cp_m + r$ where $|r| < \frac{p_m}{2}$, then set g_{2n} to r and add c to g_{2n+1}. Because the function which sums two elements of G (in the natural way) and then reduces the result is primitive recursive, G is also well-defined as an abelian group by Theorem I.1. Note that for a reduced sum $g = \sum_n g_n x_n$, we have simply $-g = \sum_n -g_n x_n$, which is already reduced by definition.

We will define an order on G by giving its positive cone $P \subset G$. Let

$$P = \{0_G\} \cup \{\sum_n g_n x_n \in G \,|\, g_\ell > 0\}.$$

Intuitively, P is the positive cone of the lexicographic ordering on G. To show that P in fact defines a valid positive cone, note that P contains the identity, and is both pure and full because $-g = \sum_n -g_n x_n$. Therefore, it only remains to be shown that P is closed under $+_G$. That is given two elements of P, $g = \sum_{n=0}^{\ell_g} g_n x_n$ and $h = \sum_{n=0}^{\ell_h} h_n x_n$ where $g_{\ell_g} > 0$ and $h_{\ell_h} > 0$, we must show that the reduced sum $g +_G h = \sum_{n=0}^{\hat{\ell}} s_n x_n$ satisfies $s_{\hat{\ell}} > 0$. We proceed in three cases:

Case 1: $\ell_g \neq \ell_h$. Without loss of generality we take $\ell_g < \ell_h$. Clearly if $s_{\hat{\ell}} = s_{\ell_h}$ is not effected by the reduction process, then $g +_G h \in P$. The only way for s_{ℓ_h} to be effected is if $\ell_g = 2j$ and $\ell_h = 2j + 1$, and there exists $p_k < |2a_{2j} + 2b_{2j}|$ such that $f(k) = j$. However, since a_{2j} and b_{2j} come from reduced sums and since $a_{2j} > 0$, this could only happen if $2a_{2j} + 2b_{2j} > p_k$. Thus, $s_{\hat{\ell}} \geq b_{\ell_h} > 0$, so $g +_G h \in P$.

Case 2: $\ell_g = \ell = \ell_h$, ℓ is odd. Because $a_{\ell-1}$ and $b_{\ell-1}$ come from reduced sums, we have $s_{\hat{\ell}} = s_\ell \geq a_\ell + b_\ell - 1 > 0$, so $g +_G h \in P$.

Case 3: $\ell_g = \ell = \ell_h$, ℓ is even. We either have $s_{\hat{\ell}} = s_{\ell+1} > 0$ because $a_\ell + b_\ell > 0$, or $s_{\hat{\ell}} = s_\ell = a_\ell + b_\ell > 0$. Either way $g +_G h \in P$.

We have shown that G is an ordered abelian group, so by (ii) and Lemma III.1, the set $A = \{(g, h) \in G \times G \,|\, g \approx h\}$ exists. We claim that the range of f is given by $\{n \,|\, (x_{2n}, x_{2n+1}) \in A\}$. If n is in the range of f, that is if $f(m) = n$ for some m, then $p_m x_{2n} = x_{2n+1}$, so $x_{2n} \approx x_{2n+1}$, and $(x_{2n}, x_{2n+1}) \in A$. If, on the other hand, n is not in the range of f, then for all m, mx_{2n} is already reduced, so $mx_{2n} < x_{2n+1}$. Thus $x_{2n} \ll x_{2n+1}$, so $(x_{2n}, x_{2n+1}) \notin A$.□

Definitions. In order to state Hahn's embedding theorem in second order arithmetic, we must define a Hahn subgroup and the notion of an isomorphism between a Hahn subgroup and an ordered abelian group in the strict sense of second order arithmetic defined above.

If $(T, \leq_T)$ is a linear ordering and $\{K_t\}_{t\in T}$ is a sequence of Archimedean ordered abelian groups indexed by T, then a *subgroup of* $\sum_T K_t$ *indexed by* I, is a sequence of functions $F = \{f_i : T \to \cup_T K_t\}_{i\in I}$ such that:

1. $f_i(t) \in K_t$ for all $i \in I$ and $t \in T$,
2. there exists $i \in I$ such that $f_i(t) = 0_{K_t}$ for all $t \in T$,
3. there exists a $j \in I$ such that $f_j = -f_i$ for all $i \in I$, i.e. $f_j(t) = -f_i(t)$ for all $t \in T$,
4. there exists a $k \in I$ such that $f_k = f_i + f_j$ for all $i, j \in I$, and
5. there exists $t \in T$ such that $f_i(t) \neq f_j(t)$ for all $i, j \in I$ such that $i \neq j$.

It is clear from the definition that F itself has the structure of an abelian group. However, it should be noted that F is not an abelian group in the sense of second order arithmetic because it is a sequence of functions encoded as sets rather than a set of elements encoded as natural numbers. Moreover, the group operation on F and the inverse operation are not guaranteed to exist as computable functions.

If the set $\{t \,|\, f_i(t) \neq 0_{K_t}\}$ is well-ordered for every $i \in I$, then we may further define an order $<_F$ by $f_i <_F f_j$ if and only if $f_i(t_0) <_{K_{t_0}} f_j(t_0)$ where t_0 is the T-minimal element of $\{t \,|\, (f_i - f_j)(t) \neq 0_{K_t}\}$. If this order respects the group operation on F, i.e. if $f_i <_F f_j$ implies that $f_i + f_k <_F f_j + f_k$ for all $i, j, k \in I$, then F has the structure of an ordered abelian group. We may define the absolute value, multiplication by $n \in \mathbb{N}$, and notions of Archimedean order and equivalence for F just as we did for ordered abelian groups in the strict sense of second order arithmetic.

A *Hahn subgroup* is a subgroup of $\sum_T K_t$ that has the structure of an ordered abelian group in the way just described and that satisfies a closure property called the cut property. The cut property need not be used for the reversal of Hahn's embedding theorem, but we present its definition here for the sake of completeness.

For every $t_0 \in T$ we define a *cut* C_{t_0} which associates functions in F with other functions from T to $\cup_T K_t$. For a given f_i, $Cf_i(t)$ is defined to be $f_i(t)$ if $t <_T t_0$ and 0_{K_t} otherwise. We say that F has the *cut property* if for every $t_0 \in T$ and every $i \in I$, there exists a $j \in I$ such that $f_j = C_{t_0} f_i$, i.e. $f_j(t) = C_{t_0} f_i(t)$ for all $t \in T$.

Finally, we must define a notion of isomorphism between ordered abelian groups in the strict sense of second order arithmetic and Hahn subgroups. We say that an ordered abelian group G is *isomorphic to a Hahn subgroup of* $\sum_T K_t$ if there exists a Hahn subgroup of $\sum_T K_t$ indexed by G such that:

1. $f_{0_G}(t) = 0_{K_t}$ for all $t \in T$,
2. $f_{g+h} = f_g + f_h$ for all $g, h \in G$,
3. $f_{-g} = -f_g$ for all $g \in G$, and
4. $g <_G h \leftrightarrow f_g <_F f_h$ for all $g, h \in G$.

We can now state Hahn's embedding theorem in second order arithmetic and prove that it implies ACA_0 over RCA_0.

Main Theorem III. *Hahn's embedding theorem* states that for every ordered abelian group G, there is a linear order T and a sequence of Archimedean ordered subgroups $K_t \subset G$ such that G is isomorphic to a Hahn subgroup of $\sum_T K_t$. Hahn's embedding theorem implies ACA_0 over RCA_0.

Proof. Let $f : \mathbb{N} \to \mathbb{N}$. Define G as in the proof to Theorem III.2. As was shown in that proof, the range of f is given by $\{n \mid x_{2n} \approx x_{2n+1}\}$. Therefore by Lemma I.4, showing this set exists is sufficient to prove arithmetical comprehension.

By Hahn's embedding theorem, there exists an isomorphism $\{f_g\}_{g \in G}$ between G and some Hahn subgroup of $\sum_T K_t$. We claim that

$$x_{2n} \approx x_{2n+1} \leftrightarrow \forall t \in T(f_{x_{2n+1}}(t) \neq 0_{K_t} \to f_{x_{2n}} \neq 0_{K_t}).$$

This claim suffices to prove the result because this condition is Π^0_1 and the usual condition for $x_{2n} \approx x_{2n+1}$ is Σ^0_1, so the range of f would exist by Δ^0_1 comprehension.

Note that either $x_{2n} \ll x_{2n+1}$ or $x_{2n} \approx x_{2n+1}$. If $x_{2n} \ll x_{2n+1}$, then $f_{x_{2n}} \ll_F f_{x_{2n+1}}$ by the definition of the isomorphism. By definition this means that $f_{x_{2n}}(t_0) \ll_{K_{t_0}} f_{x_{2n+1}}(t_0)$ where t_0 is the T-minimal element of $\{t \in T \mid f_{x_{2n}}(t) \neq f_{x_{2n+1}}(t)\}$. However, K_{t_0} is Archimedean, so we must have that $f_{x_{2n+1}}(t_0) \neq 0_{K_{t_0}}$ while $f_{x_{2n+1}}(t_0) = 0_{K_{t_0}}$.

If on the other hand, $x_{2n} \approx x_{2n+1}$, then for some odd prime p_m we have $p_m x_{2n} = x_{2n+1}$, so for every $t \in T$, $p_m f_{x_{2n}}(t) = f_{x_{2n+1}}(t)$. Thus $f_{x_{2n+1}}(t) \neq 0_{K_t}$ implies $f_{x_{2n}}(t) \neq 0_{K_t}$.□

Corollary to Main Theorem III. There exists a computable ordered abelian group G such that there is no computable embedding of G into a Hahn subgroup.

Proof. We note that REC, the natural numbers along with the recursive sets, forms a model of $\mathrm{RCA}_0 + \neg$arithmetical comprehension. Indeed, there exist recursive functions whose ranges are recursively enumerable but not recursive sets, so arithmetical comprehension cannot hold in REC by Lemma I.4. Given any such function f, the group G constructed from f in the proof of Theorem III.2 cannot be computably embedded into a Hahn subgroup because then its range would be recursive by the proof of the Main Theorem. However, G must be computable because its existence can be proven in RCA_0, and REC is a model of RCA_0.□

Hahn's embedding theorem is also provable within ACA_0, and hence is equivalent to ACA_0 over RCA_0. The proof of Hahn's embedding theorem in ACA_0 is essentially the standard proof (found in [11]) modified to avoid induction on a non-arithmetic formula, and is not of direct interest to us here. It can be found in [8].

BIBLIOGRAPHY

[1] Stephen G. Simpson. *Subsystems of Second Order Arithmetic.* Springer-Verlag, 1999.

[2] Hartley Rodgers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967.

[3] Walter Rudin. *Principles of Mathematical Analysis.* McGraw-Hill, 1976.

[4] Stephen G. Simpson. “Ordinal Numbers and the Hilbert Basis Theorem.” *The Journal of Symbolic Logic*, Vol. 53, No. 3 (Sep., 1988), pp. 961-974.

[5] W. Sieg. “Fragments of arithmetic.” *Annals of Pure and Applied Logic.* vol. 28 (1985), pp. 33-71.

[6] S.C. Kleene. *Introduction to Metamathematics.* Van Nostrand, 1964.

[7] Zohar Manna. *Mathematical Theory of Computation.* McGraw-Hill, 1974.

[8] Rodney G. Downey and Reed Solomon. “Reverse Mathematics, Archimedean Classes, and Hahn’s Theorem”. *Reverse Mathematics 2001.* Association for Symbolic Logic, 2005, pp. 147-163.

[9] L. Fuchs. *Partially Ordered Algebraic Systems.* Pergamon Press, 1963.

[10] Reed Solomon. “Reverse Mathematics and fully ordered groups.” *Notre Dame Journal of Formal Logic*, vol. 39 (1998), pp. 157-189.

[11] M. Hausner and J.G. Wendel. “Ordered vector spaces.” *Proceedings of the American Mathematical Society*, vol. 3 (1952), pp. 977-981.