SOME CONSERVATIVITY RESULTS IN REVERSE MATHEMATICS OF INTEREST TO HILBERT'S PROGRAM

GABRIEL DAY

Abstract. In this paper, various formal proof systems from the subject known as reverse mathematics in mathematical logic are introduced, including the primitive recursive system **PRA** and various subsystems of second order arithmetic. A proof that the system $\mathbf{WKL}_0$ is conservative over **PRA** for Π^0_2 sentences is presented, and an extension to the system $\mathbf{WKL}_0^+$ is discussed. Along the way, relevance of these results to Hilbert's Program in the foundations and philosophy of mathematics is addressed.

Contents

1. Introduction

In all areas of mathematics, we start with previous results and basic axioms (perhaps set theory axioms, etc) to prove new theorems. Of course, the previous results come originally from the axioms, so the axiomatic system itself is the foundation of rigorous mathematics. We could potentially choose lots of statements as axioms, and there are many schools of thought on why and how they should be chosen. For instance, David Hilbert thought that the basic axioms should consist of "finitistic" mathematics, essentially very simple statements which seem indubitable. We will give a characterization of what finitism consists of, namely the system known as **PRA**, in Section 3. Hilbert hoped to show that all theorems of mathematics are provable from these basic axioms, and crucially, are

Date: September 2019.

provably consistent. Gödel's Incompleteness Theorem shattered hopes of realizing this program, known as Hilbert's Program, and the question remained: what axioms should be used to ground math?

The area of reverse mathematics asks a slightly different set of questions about axiomatic systems: What are the weakest set of axioms needed to prove some given result? And what axioms imply other axioms? Reverse mathematics considers axiomatic subsystems of second order arithmetic, such as $\mathbf{RCA}_0$ and $\mathbf{WKL}_0$, which we will define in Section 2. This method allows us to ask, if Hilbert's finitist system **PRA** isn't able to prove all of mathematics, what sorts of theorems is it strong enough to prove?

The main result that will be discussed is that $\mathbf{WKL}_0$ is *conservative* over **PRA** for Π^0_2 sentences; that is the following theorem:

Theorem 1.1 (Conservativity)**.**
*(1) $\mathbf{WKL}_0$ is at least as strong as **PRA**. That is, if PRA proves a sentence, then $\mathbf{WKL}_0$ proves that sentence.*
*(2) If φ is a Π^0_2 sentence (i.e., of the form $\forall x \exists y \theta(x,y)$ for a quantifier-free formula θ) and $\mathbf{WKL}_0$ proves φ, then **PRA** also proves φ.*

Part (1) of the theorem is relatively straightforward to show; it turns out that even systems much weaker than $\mathbf{WKL}_0$ are stronger than **PRA**, and the primary involvement of **PRA** here will be to show that the ordinary operations of arithmetic can be coded into the nonstandard language of **PRA**. This result will be shown in Section 4.

Part (2) is rather surprising – it must exploit the nonstandard models of arithmetic that $\mathbf{WKL}_0$ must have, since it is not strong enough to guarantee enough induction to eliminate them. This method will be shown in Section 5 where the result is proved. This is the more interesting part of the theorem, not only because it is more difficult, but also because it leaves open questions such as whether conservativity can be established for higher levels of quantifier complexity or stronger subsystems.

In the Section 6, we will answer one of these questions in the affirmative, showing that this conservativity result can be extended to the stronger system $\mathbf{WKL}_0^+$.

Some familiarity with basic first order logic is presumed, such as the completeness and compactness theorems. [1] or any other basic logic textbook should be sufficient to fill in this background. Prior knowledge of reverse mathematics is not presumed.

2. Second Order Arithmetic and Some of its Subsystems

Second order arithmetic is an axiomatic system designed to state and prove results about the natural numbers.[1] The system has the following language:

[1]It may seem perplexing, then, that second order arithmetic and its subsystems prove many results which apparently have nothing to do with the natural numbers. For instance, certain subsystems can prove theorems in real analysis and topology. This is true because it is possible to encode real numbers, topological spaces, and other objects formally in systems of arithmetic.

Definition 2.1 (Language for Second-Order Arithmetic, L_2)**.** Several types of symbols: $+, \cdot, 0, 1, <$ should be thought of as their usual interpretations as constants, relations, and binary functions on the natural numbers.

Propositional logic symbols: $\wedge, \vee, \neg, \to$ represent "and," "or," "negation of" (or "not"), and "implies" (the existence of these basic logical symbols, as well as "=", will be presumed in all languages).

Quantifiers $\forall$ and $\exists$. However, there are two sorts of both of these things, numerical quantifiers (denoted $\forall x$ with lower case variables) and set quantifiers (denoted $\exists X$ with upper case variables).

Finally, we have as many set and number variables as we need, which will be countably many.

The language of First Order Arithmetic, L_1, will also come up on occasion. It is just L_2 without set quantifiers or variables.

Reverse mathematics considers *formal systems*, i.e., a language along with a list of axioms. In particular, it looks at subsystems of Z_2, the formal system of *Second Order Arithmetic*. It should be noted that this system is actually a *two-sorted first order* system, not truly second order, because quantifiers range only over some specified collection of "subsets" of any given model, not *all* subsets, as a second order system would require; a two-sorted first order system can actually be interpreted as an ordinary first order system, though it is easier to think of it in the conventional way. The primary upshot is that all theorems for first order logic, such as the completeness theorem, will apply here.

Notation 2.2 (Models of Second-Order Arithmetic)**.** Models of second order arithmetic involve a specification of subsets of the model's universe set. This will be denoted by S_M for a model M. In full formality, a model M of second order arithmetic is written

$$\langle M, S_M, +_M, \cdot_M, <_M, 0_M, 1_M \rangle.$$

The axioms of Second Order Arithmetic, called Z_2, are as follows:

(1) The "basic axioms" defining the symbols of L_2: for all numbers m and n,
  - $m + 1 \neq 0$
  - $m + 1 = n + 1 \to m = n$
  - $m + 0 = m$
  - $m + (n + 1) = (m + n) + 1$
  - $m \cdot 0 = 0$
  - $m \cdot (n + 1) = (m \cdot n) + m$
  - $\neg(m < 0)$
  - $m < n + 1 \leftrightarrow (m < n) \vee (m = n)$

(2) *Induction Axiom* $(0 \in X \wedge \forall n(n \in X \to n + 1 \in X)) \to \forall n(n \in X)$

(3) *Comprehension scheme* $\exists X \forall n(n \in X \leftrightarrow \varphi(n))$, where $\varphi(n)$ is any L_2 formula in which X doesn't occur freely.

Such codings will be discussed briefly in Section 4, and [2] contains many proofs of apparently non-arithmetic facts in subsystems of second order arithmetic.

It is an easy consequence of the Induction and Comprehension schemes that Z_2 implies the full second order induction scheme

$$(\varphi(0) \wedge \forall n(\varphi(n) \rightarrow \varphi(n+1))) \rightarrow \forall n \varphi(n) \tag{1}$$

for any L_2 formula φ. These axioms are very strong, and the project of reverse mathematics is roughly to see how much we can weaken them and still be able to prove certain results in ordinary mathematics. We want to maintain the Basic Axioms, as these ensure we are really talking about something we could call "arithmetic." All subsystems of second order arithmetic will include these basic axioms. So we instead restrict the induction and comprehension schemes in all weaker subsystems of Z_2.

Before introducing $\mathbf{RCA}_0$ and $\mathbf{WKL}_0$, a quick note on the notation Σ_i^j, Π_i^j, and Δ_i^j: These are labels for types of formulas. Σ indicates a formula starting with $\exists$, Π a formula starting with $\forall$, and Δ a formula that can be written in either way. The superscript indicates the order of the quantifier (first- vs. second-order typically, confusingly denoted 0 and 1 respectively) while the subscript denotes, in a particular sense, the complexity of the formula. Namely, a Π_k^0 formula is one of the form $\forall n_1 \exists n_2 \forall n_3 \cdots Q n_k \theta(n_1, \cdots, n_k)$, where Q is either $\forall$ or $\exists$, depending on the parity of k, and θ is a quantifier-free formula or one with only bounded quantification, that is, only with quantifiers of the form $\forall x < m$ for a fixed number m. Σ_k^0 formulas are of the analogous form, but beginning with a $\exists$, and again alternating the type of quantifier. Such formulas for first-order arithmetic are said to live on the *arithmetic hierarchy.*[2] The *analytic hierarchy* consists of formulas with superscripts of 1, which have set quantifiers. These are of the corresponding forms $\forall X_1 \exists X_2 \forall X_3 \cdots Q X_k \theta$, for instance, but this time, θ can be any formula with only first-order quantifiers (such formulas are called *arithmetic*). Finally, it is common to refer to sets which are definable in a model by means of a given level of quantifier complexity by the same name as that sort of formula; e.g., if a set X is definable by means of a Π_3^0 formula, then X itself is called Π_3^0.

Now we introduce the systems $\mathbf{RCA}_0$ and $\mathbf{WKL}_0$.

Informally, $\mathbf{RCA}_0$ corresponds to "computable mathematics." The name stands for "Recursive Comprehension Axiom." In addition to the basic arithmetic axioms, $\mathbf{RCA}_0$ allows for Σ_1^0-induction and Δ_1^0-comprehension; i.e., the induction schema (1) holds for Σ_1^0 formulas φ, and comprehension for formulas that can be written both as Σ_1^0 and as Π_1^0. It is a basic result in computability theory that the Δ_1^0-definable sets are the computable ones, so we could equivalently say that $\mathbf{RCA}_0$ has comprehension for computable sets.

$\mathbf{RCA}_0$ is generally used as the base theory in reverse mathematics, in the sense that weaker systems are rarely considered (**PRA** being one exception), and when two axioms are said to be equivalent, the implication is that this means "equivalent

[2]The hierarchy consists of Σ_k^0 and Π_k^0 being incomparable, Δ_k^0 encompassing both, and both Σ_{k+1}^0 and Π_{k+1}^0 including Δ_k^0. It is truly a hierarchy because a Σ_k^0 sentence (for instance) is equivalent to a sentence of any higher type by means of adding dummy quantifiers which range over variables not otherwise appearing in the formula.

over $\mathbf{RCA}_0$." Still, $\mathbf{RCA}_0$ is strong enough on its own to prove, among other things, the intermediate value theorem, the completeness theorem for first-order logic, the existence of algebraic closures of countable fields, and many other results (see [2] for a more complete list).

To define the system $\mathbf{WKL}_0$, a bit of notation for binary trees must be established. Using the conventional abbreviation $\{0, 1\} = 2$, let $2^{<\omega}$ denote the collection of all finite binary strings, such as 011101010101. A subset of $2^{<\omega}$ is called a *tree* if it is closed under taking initial segments. Similarly, let 2^ω be the collection of infinite binary strings. A *path* through a tree is an infinite binary sequence such that every finite initial segment is an element of the tree. It is simple to code the finite binary strings as natural numbers and trees as sets, or vice versa, by means of a binary representation, so L_2 formulas may be thought to quantify over and refer to binary strings as "numbers" and to trees as "sets."

With these definitions, we can state:

Theorem 2.3 (Weak König's Lemma (WKL))**.** *Every infinite binary tree has a path.*

Though WKL seems rather intuitively obvious, it is not provable in $\mathbf{RCA}_0$. Adding WKL to $\mathbf{RCA}_0$ yields a significantly stronger system; this system is precisely $\mathbf{WKL}_0$. That is,$\mathbf{WKL}_0$ is $\mathbf{RCA}_0 + \text{WKL}$.

In addition to proving anything $\mathbf{RCA}_0$ can prove, $\mathbf{WKL}_0$ is equivalent (over $\mathbf{RCA}_0$) to the Bolzano–Weierstrass theorem in real analysis, that every countable commutative ring has a maximal ideal, and many other results which can be found in [2].

3. The Finitist System, PRA

PRA is an axiomatic system based on a collection of functions known as *primitive recursive* (sometimes we will abbreviate by p.r.). As with the subsystems of second-order arithmetic we have considered, **PRA** is generally thought of as a theory of the natural numbers.

First, what functions are considered primitive recursive?

- The zero function (for each x, $Z(x) = 0$)
- The successor function
- Projection functions, from any number of variables onto any coordinate ($P^n_k(x_1, \cdots, x_n) = x_k$)
- Compositions of other p.r. functions
- Functions defined by primitive recursion on other p.r. functions, i.e., a function f defined from p.r. functions g, h by: $f(0, x_1, \cdots, x_n) = g(x_1, \cdots, x_n)$, and $f(y + 1, x_1, \cdots, x_n) = h(y, f(y, x_1, \cdots, x_n), x_1, \cdots, x_n)$.

The language of **PRA**, $L_{\mathbf{PRA}}$, consists of constant 0 and function symbols corresponding to all the p.r. functions.

PRA is a system in this language. It consists of the following axioms:

(1) The typical successor axioms, such as $\forall x \neg S(x) = 0$.
(2) The axiom $\forall x Z(x) = 0$ which defines the zero function.

(3) The assertions that all symbols for projection functions in fact project onto their corresponding variables.
(4) The assertions that the function symbols which are thought of as compositions and primitive recursions of other functions are to be interpreted as such.
(5) The induction scheme for quantifier-free $\theta(x)$ in $L_{\mathbf{PRA}}$:

$$(\theta(0) \wedge \forall x(\theta(x) \rightarrow \theta(S(x))) \rightarrow \forall x \theta(x).$$

In order to compare **PRA** with $\mathbf{RCA}_0$, $\mathbf{WKL}_0$, and other subsystems of Z_2, it is necessary to fix a canonical interpretation of the language L_1 in terms of $L_{\mathbf{PRA}}$. This is straightforward; for instance, $+$ can be defined as a binary p.r. function by: $x + 0 = x$, $x + S(y) = S(x + y)$. The p.r. definitions of other L_1 symbols may be found in Section IX.3 of [2]. This canonical coding allows for models of **PRA** to also model some L_1 or L_2 sentences, which allows us to say, for instance, "$\mathbf{RCA}_0$ is stronger than **PRA**."

We conclude this section with a brief remark on the claim that **PRA** is what Hilbert thought of as "finitism." This claim is essentially a philosophical one, and is known as "Tait's Thesis," after it was defended by William Tait in [3]. Tait goes through the sorts of reasoning which might be regarded as finitistic, based in Hilbert's writings, and concludes that they are encapsulated in **PRA**. We note, however, that this claim has been disputed, for instance in [4]. Yet most such doubts have suggested that finitism is actually *stronger* than **PRA**, and so the results presented in this paper, and perhaps stronger ones, would still hold if these critiques are valid.

4. PRA is Weaker than $\mathbf{RCA}_0$

The following definition is crucial to the model-theoretic arguments used in this section and later in Section 6.

Definition 4.1 (ω-submodel)**.** An L_2 model M is an *ω-submodel* of another L_2 model M' if M is a submodel of M' and they have the same first-order part; that is, the sets $M = M'$, and the interpretations of relations, functions, and constants are identical. However, the collections of subsets S_M and $S_{M'}$ will be different in general. This relation is denoted $M \subseteq_\omega M'$.

Lemma 4.2. *Let M be any L_2-structure satisfying Σ^0_1-**PA**, that is, the basic arithmetic axioms and Σ^0_1-induction. Then M is an ω-submodel of some model of $\mathbf{RCA}_0$.*

Proof. For this proof, we will need the following useful formula, known as the Bounding Principle: For a Σ^0_1 formula $\varphi(i, j)$ and natural number m, we have

$$(\forall i < m)\exists j \varphi(i, j) \rightarrow \exists n(\forall i < m)(\exists j < n)\varphi(i, j).$$

This formula essentially says that if for each of the finitely many values of i less than m, some j_i satisfies $\varphi(i, j_i)$, there is a bound n on these j_i. Formally, this follows from a simple application of Σ^0_1-induction, since the scheme results from only bounded quantification on a Σ^0_1 formula.

For a given M as in the hypothesis, we say that $X \subseteq M$ is a Δ^0_1 definable subset of M if it is definable in M by both a Σ^0_1 and a Π^0_1 formula.

Let M' be the L_2 model consisting of the same first-order part as M, and second order part $S_{M'} = \Delta^0_1\text{-Def}(M)$, that is, all Δ^0_1 definable subsets of M. Since M' has the same first-order part as M by definition, M is automatically an ω-submodel. It thus suffices to show that M' is a model of $\mathbf{RCA}_0$.

We need to show two claims, which justify the equivalence of formulas with set parameters in $S_{M'}$ with formulas with S_M parameters.

Claim 1: For any Σ^0_0 formula θ with parameters in $M \cup S_{M'}$ and no free set variables, we can find formulas θ_Σ and θ_Π, which are Σ^0_1 and Π^0_1 respectively, which have the same free variables as θ, only parameters from $M \cup S_M$, and are equivalent to θ in M'.

This is shown by induction on the complexity of θ. If θ is atomic of the forms $t_1 = t_2$ or $t_1 < t_2$ for terms t_1, t_2, then there are no parameters from $S_{M'}$, so just let $\theta = \theta_\Sigma = \theta_\Pi$. If it is atomic of the form $t \in X$, where $X \in S_{M'}$, then X is Δ^0_1 definable, meaning there is a Π^0_1 formula ψ and a Σ^0_1 formula φ, both of which define X over M, so we let $\theta_\Sigma = \varphi(t)$ and $\theta_\Pi = \psi(t)$. If θ is of the form $\neg\theta'$, then put $\theta_\Sigma = \neg\theta'_\Pi$ and $\theta_\Pi = \neg\theta'_\Sigma$ (this works because $\forall$" = "$\neg\exists\neg$ and $\exists$" = "$\neg\forall\neg$).

If $\theta = \theta' \wedge \theta''$, then we can write $\theta_\Sigma = \theta'_\Sigma \wedge \theta''_\Sigma$. Writing $\theta'_\sigma = \exists j \theta'_0(j)$ and $\theta''_\Sigma = \exists j \theta''_0(j)$, we can see that θ_Σ is, in fact, Σ^0_1, as $\theta'_\Sigma \wedge \theta''_\Sigma = \exists m((\exists i < m)\theta'_0(i) \wedge (\exists j'' < m)\theta''_0(j))$. Why is this equivalent? Well, if there exists something satisfying θ'_0 and something satisfying θ''_0, then we can bound these two elements to get the above bounded quantification statement.

Moreover, we can write $\theta_\Pi = \theta'_\Pi \wedge \theta''_\Pi = \forall j(\theta'_1 \wedge \theta''_1)$, where $\theta'_\Pi = \forall j \theta'_1(j)$, and $\theta''_\Pi = \forall j \theta''_1(j)$.

Finally, we must deal with the case where $\theta = (\forall i < t)\theta'$. If $\theta'_\Sigma = \exists j \theta'_0$ and $\theta'_\Pi = \forall j \theta'_1$, we can write: $\theta_\Sigma = \exists n(\forall i < t)(\exists j < n)\theta'_0$ and $\theta_\Pi = \forall j(\forall i < t)\theta'_1$. Here the equivalence of θ and θ_Σ formula follows from the bounding principle, while we can form θ_Π by moving the $\forall j$ to the front, as we can reorder quantifiers of the same type. Since all Σ^0_0 sentences can be built up from atomic formulas by negation, conjunction, and bounded quantification (all of which have been shown), Claim 1 has now been proved.

Claim 2: For any Σ^0_1 formula φ with parameters from $M \cup S_{M'}$ and no free set variables, there is an equivalent Σ^0_1 formula φ' with the same free variables and parameters from $M \cup S_M$. An equivalent claim holds for Π^0_1 formulas which can be shown by an analogous proof.

We can write $\varphi = \exists j \theta$, for a Σ^0_0 formula θ. By Claim 1, θ is equivalent to some θ_Σ with only parameters from $M \cup S_M$. $\theta_\Sigma = \exists m \theta_0$, and θ_0 is Σ^0_0. So our desired formula is $\varphi' = \exists j \theta_\Sigma = \exists j \exists m \theta_0$, which is Σ^0_1, and thus satisfies the claim.

Now, we can show that M' is a model of $\mathbf{RCA}_0$. Clearly it satisfies the basic arithmetic axioms, so only Σ^0_1-induction and Δ^0_1-comprehension need to be checked.

Let φ be a Σ_1^0 formula, and φ' be the equivalent formula from Claim 2. Then since $M \models (\varphi'(0) \wedge \forall n(\varphi'(n) \to \varphi'(n+1))) \to \forall n\varphi'(n)$, we must also have $M' \models (\varphi(0) \wedge \forall n(\varphi(n) \to \varphi(n+1))) \to \forall n\varphi(n)$ as the formulas are equivalent. Thus M' satisfies Σ_1^0-induction.

For Δ_1^0-comprehension, suppose $M' \models \forall n(\varphi(n) \leftrightarrow \psi(n))$ for Σ_1^0 φ and Π_1^0 ψ. By Claim 2, we may replace these by Σ_1^0 φ' and Π_1^0 ψ' such that $M' \models \forall n(\varphi(n) \leftrightarrow \varphi'(n))$, and the same with ψ. Thus, we have $M \models \forall n(\varphi'(n) \leftrightarrow \psi'(n))$, and so $X = \{a \in M : M \models \varphi'(n)\} = \{a \in M : M \models \psi'(n)\}$. So X is Δ_1^0 definable, i.e., $X \in S_{M'}$, and hence we have $M' \models \exists X \forall n(n \in X \leftrightarrow \varphi(n))$. □

Theorem 4.3. *An L_1-structure is the first-order part of some model of $\boldsymbol{RCA}_0$ if and only if it is a model of Σ_1^0-$\boldsymbol{PA}$.*

Proof. Since the axioms of $\mathbf{RCA}_0$ include those of Σ_1^0-**PA**, it is clear that the first-order part of any model of $\mathbf{RCA}_0$ satisfies Σ_1^0-**PA**. Conversely, we can view any model M of Σ_1^0-**PA** as an L_2 model by specifying some (perhaps empty) collection of sets to be S_M (which these are does not matter). Viewed in this way, M satisfies the hypothesis of the previous Lemma, and hence is an ω-submodel of a model of $\mathbf{RCA}_0$, that is, a submodel with the same first-order part. Thus viewed again as an L_1-structure, M is the first order part of a model of $\mathbf{RCA}_0$, as desired. □

The next result involves a coding of primitive recursive functions into $\mathbf{RCA}_0$. Done rigorously, this involves certain tedious coding results, the details of which may be found in Simpson, II.3 especially, as well as [1], which uses these codings to prove Gödel's Incompleteness Theorems and other related results. The most basic step in coding is to fix a natural number for each symbol of our language (for "(", "∀", "−", etc.). Then we can code sequences of symbols in our language as natural numbers by means of the following product: $\Pi_{i \in \mathbb{N}} p_i^{n_i}$, where p_i are primes in ascending order and n_i is the number for the ith symbol in the sequence. The natural numbers which are equal to such a product are "sequence numbers" and we may speak of "Seq" as the set of sequence numbers. We can also rigorously define a "function" as a kind of set in $\mathbf{RCA}_0$. We will prove that one can define functions by primitive recursion in $\mathbf{RCA}_0$; similarly, all other kinds of p.r. functions can be defined in $\mathbf{RCA}_0$.

Lemma 4.4. *Any model of Σ_1^0-$\boldsymbol{PA}$ can be expanded to a model of $\boldsymbol{PRA}$ in a way respecting the canonical interpretation of L_1 in the language of $\boldsymbol{PRA}$.*

Proof. By Theorem 4.3, any given model of Σ_1^0-**PA** is the first order part of some model M of $\mathbf{RCA}_0$. Now, we can "expand" M to a model of **PRA** by defining p.r. functions within $\mathbf{RCA}_0$ and assigning them to the corresponding function symbols of **PRA** in a way that respects the axioms of **PRA**.

For instance, if we have $f: \mathbb{N}^k \to \mathbb{N}$ and $g: \mathbb{N}^{k+2} \to \mathbb{N}$, there exists a unique $h: \mathbb{N}^{k+1} \to \mathbb{N}$ defined by primitive recursion, i.e., defined by $h(0, n_1, \cdots, n_k) = f(n_1, \cdots, n_k)$, and $h(m+1, n_1, \cdots, n_k) = g(m, h(y, n_1, \cdots, n_k), n_1, \cdots, n_k)$.

This is explained by the following argument. Define a formula $\theta(s, m, \langle n_1, \cdots, n_k\rangle)$ which say that for each $s \in$ Seq, the sequence s has length $m+1$ characters, $s(0) = f(n_1, \cdots n_k)$, and for $i < m$, $s(i+1) = g(s(i), i, n_1, \cdots, n_k)$. All of this is definable in $\mathbf{RCA}_0$. The formula

$$\exists s \theta(s, m, \langle n_1, \cdots, n_k\rangle)$$

is Σ^0_1, since all the stipulations of θ can be expressed with bounded quantification (this can be checked from the definitions of sequence number and the other codings used). Thus we can prove $\exists s\theta(s, m, \langle n_1, \cdots, n_k\rangle)$ for each fixed $\langle n_1, \cdots, n_k\rangle$, by the obvious Σ^0_1-induction on m. We can also prove, by induction on $i < m+1$, that if $\theta(s, m, \langle n_1, \cdots, n_k\rangle)$ and $\theta(s', m, \langle n_1, \cdots, n_k\rangle)$, then $s(i) = s'(i)$.

From these two facts, we can further prove that:

$$\exists s(\theta(s, m, \langle n_1, \cdots, n_k\rangle)) \wedge s(m) = j) \leftrightarrow \forall s(\theta(s, m, \langle n_1, \cdots, n_k\rangle) \rightarrow s(m) = j).$$

Notice that this is the formula for a set to be Δ^0_1, so by Δ^0_1-comprehension, there exists $h\colon \mathbb{N}^{k+1} \to \mathbb{N}$ such that $h(m, n_1, \cdots, n_k) = j$ if and only if

$$\exists s(\theta(s, m, \langle n_1, \cdots, n_k\rangle)\theta(s, m, \langle n_1, \cdots, n_k\rangle) \wedge s(m) = j).$$

It can easily be checked that h satisfies the properties of the recursive definition.

Notably, each interpretation of a new function f_M in our model (such as the h defined above) will be an element of S_M, since functions are formally defined as sets in $\mathbf{RCA}_0$ (specifically, sets of sequence numbers for ordered pairs, which represent pairs (a, b) such that $f(a) = b$). All of the basic axioms for $+, \cdot, 0, 1, <$ are theorems of $\mathbf{RCA}_0$, so clearly these symbols are interpreted "correctly" in this model. And **PRA** induction follows from Σ^0_1-induction (which is true in M as a model of $\mathbf{RCA}_0$) since all functions are defined in a Σ^0_1 way, and **PRA** induction is for quantifier-free formulas built from these functions. This completes the proof. □

Theorem 4.5. *If θ is an L_1 formula provable in **PRA**, then θ is provable in Σ^0_1-**PA**, and hence also in $\mathbf{RCA}_0$.*

Proof. Suppose θ is not provable in Σ^0_1-**PA**. The completeness theorem implies that there is an L_1 model M of Σ^0_1-**PA** in which θ is false. The previous lemma allows us to expand M to a model for **PRA** in a way respecting the normal interpretation of L_1. So we have a model of **PRA** in which θ fails. Thus, the soundness theorem (which is also provable in $\mathbf{RCA}_0$) implies that **PRA** does not prove θ.

□

5. PRA Proves Π^0_2 Sentences which $\mathbf{WKL}_0$ Proves

Definition 5.1. A formula in $L_{\mathbf{PRA}}$ is said to be *generalized* Σ^0_0 if it is built from atomic formulas of the form $t_0 = t_1$ and $t_0 < t_1$, where the t_i are terms, by means of propositional connectives and bounded quantification, where the bound on the quantification is a term t in $L_{\mathbf{PRA}}$.

The following is a technical lemma, allowing us to code simple formulas with p.r. functions. It allows us to replace generalized Σ_0^0 formulas with equivalent simpler, atomic formulas.

Lemma 5.2. *For any generalized Σ_0^0 formula $\theta(x_1, \cdots, x_k)$, there is a k-ary p.r. function $f := f_\theta$ such that* ***PRA*** *proves $f(x_1, \cdots, x_k) = 1 \leftrightarrow \theta(x_1, \cdots, x_k)$ and $f(x_1, \cdots, x_k) = 0 \leftrightarrow \neg\theta(x_1, \cdots, x_k)$*

Proof. The proof is by induction on the complexity of θ. The variables $x_1, \cdots x_k$ following θ and the corresponding f_θ will be omitted for convenience. If $\theta = \theta' \wedge \theta''$, then let $f_\theta = f_{\theta'} \cdot f_{\theta''}$. If $\theta = \neg\theta'$ then let $f_\theta = 1 - f_{\theta'}$.

Finally, if $\theta = (\forall y < t)\theta'(y)$, then let

$$f_\theta = \prod_{y<t} f_{\theta'}(y).$$

It is straightforward to verify that all of these operations can be carried out in **PRA**, so this concludes the proof. □

This lemma allows for the introduction of a k-ary p.r. predicate R defined by $R(x_1, \cdots, x_k) \leftrightarrow f(x_1, \cdots, x_k) = 1$.

While we typically think of models for **PRA** as ω, the models we need to prove the conservativity result will have to be nonstandard, consisting of a copy of the natural numbers, followed by some other elements. The successor axioms dictate that every such nonstandard element must have a successor and a predecessor, and thus lives on on "$\mathbb{Z}$-chain," or copy of $\mathbb{Z}$. Since such $\mathbb{Z}$-chains might exist in a model M for **PRA**, a set might be bounded above (by an element on a $\mathbb{Z}$-chain) and defined by a p.r. relation, and yet still have infinite cardinality. This motivates the following definition.

Definitions 5.3 (M-cardinality and M-finite sets)**.** A set $X \subseteq M$, for a model M, is *M-finite* if there is $b \in M$ and a p.r. relation R along with parameters $c_1, \cdots, c_k$ such that $X = \{a \in M : a <_M b \wedge R_M(a, c_1, \cdots, c_k)\}$. That is, X is a p.r. definable bounded subset of M.

The *M-cardinality* of an M-finite set X is defined by $\text{card}_M(X, 0) = 0$,

$$\text{card}_M(X, a+1) = \begin{cases} \text{card}_M(X, a) + 1 & \text{if } a \in X \\ \text{card}_M(X, a) & \text{if } a \notin X \end{cases},$$

where $\text{card}_M(X) = \text{card}_M(X, b)$ for some bound $b \in M$ for X. It is clear from the definition that $\text{card}_M(X, b)$ will be the maximum value of $\text{card}_M(X, c)$ when b is a bound.

The M cardinality of a set X, $\text{card}_M(X)$, should be thought of as a counting of elements of X within M, which is nontrivial in nonstandard models of arithmetic (i.e., those with $\mathbb{Z}$-chains).

It will also be necessary to know that the M-finite sets can be encoded as single elements of the model, in a primitive recursive manner. For brevity we omit this technical and fairly unenlightening argument, which is quite similar to other coding arguments in computability theory. Those interested can consult Lemma IX.3.9 in [2]. The takeaway is that we can associate unique elements of the model with M-finite sets, and do it in a primitive recursive way.

Definitions 5.4 (Cuts, Semiregular Cuts, etc.). (1) A *cut* is a set $I \subseteq M$ such that $1_M \in I \neq M$, and with the property that if $c <_M b$ and $b \in I$, then $c \in I$.
(2) For a cut I in M, $X \subseteq I$ is M-*coded* if there is an M-finite set X^* such that $X^* \cap I = X$. The collection of all M-coded subsets of I is denoted by $\text{coded}_M(I)$.
(3) A set X is *bounded* in a cut I if $X \subseteq \{a : a < b\}$ for some $b \in I$.
(4) A cut I is *semiregular* if, for all M-finite sets X such that $\text{card}_M(X) \in I$, $X \cap I$ is bounded in I.

It should be noted that a set may be a subset of a cut and yet not be bounded in it, for instance, the cut is not bounded in itself.

To illustrate how we can use the definition of a semiregular cut, suppose that I is a semiregular cut in a model M for **PRA**, and that $b, c \in I$. It is easy to see that $X = \{a : b \leq_M a <_M b +_M c\}$ has M-cardinality c, and hence, since $c \in I$, we must have that $X \cap I$ is bounded by some $d \in I$. Clearly $b +_M c <_M d$, and hence $b +_M c \in I$ (this is actually how we show that semiregular cuts are closed under $+_M$ in the proof of Key Lemma 2 below).

It should be noted that due to the presence of $\mathbb{Z}$-chains, cuts in models of **PRA** might not be finite initial segments, but rather initial segments ending on some $\mathbb{Z}$-chain, and thus infinite in size, and with infinite distance between some elements. In fact, all semiregular cuts must be infinite, and thus of this form. If not, the cut consists of the integers 0 through n. But in this case, the set $\{n+1\}$, which is clearly M-finite, with M-cardinality $1 \in [0, n]$. Yet $\{n+1\}$ is clearly not bounded in the cut. So it is not semiregular.

The next definition provides a description of a kind of "space" between elements of a model of **PRA** which will allow us to guarantee the existence of semiregular cuts.

Definition 5.5 ($<<_M$). For $b, c \in M$, a model of **PRA**, we say that $b <<_M c$ if $f_M(b) < c$ for every 1-ary p.r. function symbol f.

We note in passing that any non-ω model of **PRA** will have $b <<_M c$ for some $b, c \in M$. Just take b and c on different $\mathbb{Z}$-chains, and since $f(b) - b$ can only be finite, we will have $f(b) <_M c$ for any p.r. function f.

Lemma 5.6 (Key Lemma 1). *Let M be a countable model of **PRA**, and $b, c \in M$ such that $b <<_M c$. Then there exists a semiregular cut I in M which contains b but not c.*

Proof. We begin by recursively defining a notion of "n-bigness" for intervals $[b, c)$. Such an interval is 0-big if $b < c$, and $(n+1)$-big if, for every finite set X of cardinality $\leq b$, there are b', c' with $b < b' < c' < c$, and $[b', c')$ is n-big and disjoint from X.

We can formalize this notion with a primitive recursive predicate, say $B(x, y, z)$ (indicating that $[y, z)$ is x-big). This is done by recursion on x: We have $B(0, y, z) \leftrightarrow y < z$, and $B(S(x), y, z)$ if and only if the corresponding definition is satisfied; note that this involves quantifying over the finite sets, which is possible using a bounded quantification by means of the coding lemma mentioned above.

Now, define the p.r. functions g_n by $g_0(y) = y + 1$, and

$$g_{n+1}(y+1) = \underbrace{g_n g_n \cdots g_n}_{y+1 \text{ times}}(y+1) + 1.$$

For each $n < \omega$, it is provable in **PRA** that, for all y, z $g_n(y) \leq z \rightarrow B(n, y, z)$.

Now we have the tools to prove the lemma. Let M be a model of **PRA** as in the hypothesis. Since $f_M(b) < c$ for all p.r. functions f, we have in particular that $g_{n_M}(b) < c$ for each n, so $B(n, b, c)$ holds in M. It is clear from the definition of n-bigness that $[b, c)$ cannot be n-big for all n (though it might be for all $n < \omega$). So take the greatest $k \in M$ such that M models $B(k, b, c)$. Thus for all "standard" natural numbers n, $n < k$.

Since M was assumed to be a countable model, there are countably many M-finite sets. Thus they may be listed by $\langle X_n : n < \omega \rangle$. We may also assume that this listing contains each of the sets infinitely many times, such that at any point in the enumeration, every set will appear again.

We now construct two sequences, one ascending and one descending, of the form

$$b = b_0 <_M b_1 <_M \cdots <_M b_n <_M \cdots <_M c_n <_M \cdots <_M c_1 <_M c_0 = c$$

where all of the b_i are less than the c_j. The construction goes as follows. Let $b_0 = b$, and $c_0 = c$. For a given n, suppose we have defined

$$b_0 <_M b_1 <_M \cdots <_M b_n <_M c_n <_M \cdots <_M c_1 <_M c_0.$$

Consider the M-finite set X_n from our listing. If $\text{card}_M(X_n) \geq b_n$, then set $b_{n+1} = b_n + 1$. Otherwise, $\text{card}_M(X_n) <_M b_n$, and so since $M \models [b_n, c_n)$ is $(k - n)$-big, there are b_{n+1}, c_{n+1} such that $b_n <_M b_{n+1} <_M c_{n+1} <_M c_n$, and $M \models [b_{n+1}, c_{n+1})$ is $(k - n - 1)$-big and disjoint from X_n.

Now, set $I = \{a \in M : a <_M b_n \text{ for some } n < \omega\}$. It is easy to see that this satisfies the downward-closedness property and other properties of a cut. To see it is also semiregular, suppose X is an M-finite set with $\text{card}_M(X) \in I$. Since X appears arbitrarily late in the list of finite sets, we can find an n such that $X = X_n$ and $\text{card}_M(X) <_M b_n$. By construction, $M \models [b_{n+1}, c_{n+1})$ is disjoint from X, and so $X \cap I \subseteq \{a : a <_M b_{n+1}\}$, hence $X \cap I$ is bounded in I. Thus I is semiregular, and the proof is complete. □

Now that we have the existence of semiregular cuts, we make use of them. The result that models of **PRA** restricted to semiregular cuts model $\mathbf{WKL}_0$ is more surprising, quite technical, and strongly uses the definition of semiregularity. It will employ the following lemma, which makes the connection between the definition of $\mathbf{WKL}_0$ in terms of binary trees, and proof-theoretic properties of models which are easier to work with.

A brief notational note concerning binary strings: if σ is a binary string, $\sigma^\frown\langle 0\rangle$ is σ with a 0 added at the end.

We also define the condition on a theory known as Σ^0_1-separation, which means: for φ_0, φ_1 Σ^0_1 formulas, if $\neg\exists x(\varphi_0(x) \wedge \varphi_1(x))$, then

$$\exists X \forall n((\varphi_0(n) \to n \in X) \wedge (\varphi_1(n) \to n \notin X)).$$

Lemma 5.7 (Σ^0_1 Separation)**.** *Over* $\boldsymbol{RCA}_0$*,* Σ^0_1 *separation implies* $\boldsymbol{WKL}_0$*. (In fact, they are equivalent over* $\boldsymbol{RCA}_0$*, though only this direction is relevant to this paper.)*

Proof. Take an infinite tree $T \subseteq 2^{<\omega}$. Let

$$\theta(n, \sigma) = \exists\tau(\mathrm{lh}(\tau) = n \wedge \tau \in T \wedge \tau \supseteq \sigma);$$

in English this says that there is a string τ on the tree T of length n which extends σ. Notice that this is really a bounded Σ^0_0 sentence, since it need only look at the finitely many sequences of length n. Then, for $i \in \{0, 1\}$, let $\varphi_i(\sigma)$ be the Σ^0_1 formula

$$\exists n(\theta(n, \sigma^\frown\langle i\rangle) \wedge \neg\theta(n, \sigma^\frown\langle 1 - i\rangle)).$$

These formulas say, "there is an n such that there is a τ in T of length n which extends $\sigma^\frown\langle i\rangle$, but no such τ which extends $\sigma^\frown\langle 1-i\rangle$ in T." It is clear from this definition that $\neg\exists\sigma(\varphi_0(\sigma) \wedge \varphi_1(\sigma))$, so we may take these as the two disjoint Σ^0_1 formulas for Σ^0_1-separation. By assumption then, we have a set X such that

$$\forall n((\varphi_0(\sigma) \to \sigma \in X) \wedge (\varphi_1(\sigma) \to \sigma \notin X)).$$

Now, define a sequence of finite binary sequences $\sigma_0 \subseteq \sigma_1 \subseteq \cdots$ in the following way: Let σ_0 be the empty sequence, and $\sigma_{k+1} = \sigma_k^\frown\langle 0\rangle$ if $\sigma_k \in X$, otherwise let $\sigma_{k+1} = \sigma_k^\frown\langle 1\rangle$.

We claim that $\theta(n, \sigma_k)$ holds whenever $k \leq n$; this is easy to check from the definitions by inducting on $k \leq n$ for fixed n. In particular, this gives that $\theta(n, \sigma_n)$ holds, and so each $\sigma_n \in T$. But then, $P = \bigcup\{\sigma_n\}$ is a path through T. Since T was arbitrary, this proves Weak König's Lemma. □

Lemma 5.8 (Key Lemma 2)**.** *Let* M *be a model of* $\boldsymbol{PRA}$ *and* I *be a semiregular cut in* M*. Then*

$$(I, \mathit{Coded}_M(I), +_M \restriction I, \cdot_M \restriction I, <_M\restriction I, 0_M, 1_M)$$

is a model of $\boldsymbol{WKL}_0$*.*

Proof. We must first show that this model, I, is closed under $+_M$ and $\cdot_M$. We have shown the $+_M$ case above, and the $\cdot_M$ case is similar. Towards a contradiction, suppose $b, c \in I$ but $b \cdot_M c \notin I$. Then the set $X = \{b \cdot_M a : a <_M c\}$ has M-cardinality c, yet $Y \cap I$ is unbounded in I, a contradiction. Hence I is closed under $\cdot_M$.

We must now show that I satisfies the Σ^0_1-induction scheme. Using the p.r. induction scheme, we have that every M-finite set has a $<_M$-least element (if the set is defined by a p.r. relation $R(x)$, induct on $\neg R(x)$ and seek a contradiction).

Let $\varphi(x)$ be a Σ^0_1 formula with parameters from $I \cup \mathrm{coded}_M(I)$, and no additional free variables besides x. We must show that I satisfies the induction schema (1) for φ. If I satisfies $\varphi(c)$ for every $c \in I$, then $\forall x \varphi(x)$ is true in I and there is nothing to prove. Otherwise, there is some $c \in I$ with $I \models \neg\varphi(c)$. This allows us to form the set $Y = \{a : a <_M c \text{ and } I \models \varphi(a)\}$.

We claim that Y is M-finite. Since every set parameter X appearing in φ is in $\mathrm{coded}_M(I)$, by definition there is an M-finite set X' with $X' \cap I = X$. We can make the formula $\varphi'(x) = \exists y \theta'(x, y)$ by replacing all such X in φ by the corresponding X'. So $\theta'(x, y)$ will be generalized Σ^0_0 with parameters only from the set M.

Now, fix $d \notin I$ (this must exist, as it is a cut). Define the subset $Z \subseteq I \times M$ by:

$$Z = \{(a, b) : a <_M c, b <_M d, b \text{ is the } <_M\text{-least } b' \text{ such that } M \models \theta'(a, b')\}$$

Let Z' be the set formed by projecting Z onto its first coordinate. Lemma 5.2 gives that this Z' is M-finite, since it is built up from the generalized Σ^0_0 formula θ' in a straightforward way. Also, since there is only one pair (a, b) in Z for each $a < c$, Z' has M-cardinality less than or equal to $c \in I$. By semiregularity of I, $Z' \cap I$ is bounded in I. Thus $Z' \cap I$ is M-finite. Finally, observe that Y can be written as $Z' \cap I$, and so Y is M-finite.

As Y is M-finite, we may use our above observation to find a $<_M$-least element b of $I \backslash Y$ (since $c \notin Y$, this set is nonempty). If $b = 0_M$, then $I \models \neg\varphi(0_M)$ and thus I models the induction schema with φ. Otherwise, there is some b' with $b = S(b')$, and since b was least in $I \setminus Y$, $\varphi(b')$ is true in I. Hence $I \models \neg\forall x(\varphi(x) \to \varphi(x+1))$, and so I models the induction schema for φ. Hence the schema is satisfied in all cases.

We now show that I satisfies Σ^0_1 separation. Let $\varphi_0(x)$ and $\varphi_1(x)$ be Σ^0_1 formulas with parameters from $I \cup \mathrm{coded}_M(I)$, where x is the only free variable. Let $A_i = \{a \in I : I \models \varphi_i(a)\}$ for $i \in \{0, 1\}$; assume that $A_0 \cap A_1 = \emptyset$. We must show that these sets can be separated by an M-coded subset of I.

As above, write $\varphi^*_i(x) = \exists y \theta^*_i(x, y)$ by replacing all coded set parameters X in φ_i by the corresponding X' such that $X' \cap I = X$. So again, the θ^*_i are generalized Σ^0_0. And finally, fix $d \in M \setminus I$. Define

$$Y^* = \{a : a <_M d \wedge (\exists b <_M d)(\theta^*_1(a, b) \wedge (\forall b' <_M b)\neg\theta^*_0(a, b')\}.$$

We claim this Y^* separates the A_i. Why does the definition of Y^* imply $A_1 \subseteq Y^*$ and $A_0 \cap Y^* = \emptyset$?

Suppose $a \in A_1$. Then $a \in I$ and $\varphi_1(a) = \exists b \theta(a, b)$, where $b \in I$ since that is the universe set over which quantifiers range. Then $a < d$, $b < d$, and since $a, b \in I$, θ^*_1 is effectively just θ_1, so $\theta^*_1(a, b)$ holds. If there was b' violating the second conjunct of Y^*'s definition, it would clearly violate $A_0 \cap A_1 = \emptyset$, since everything would be in I. Hence $a \in Y^*$.

Suppose $a \in A_0$. Then $a \in I$, and $\varphi(a) = \exists b \theta_0(a, b)$ holds, in particular, there is such a $b \in I$. If, in addition, $a \in Y^*$, then the $b < d$ making the first conjunct true must not be in I, otherwise that would violate $A_0 \cap A_1 = \emptyset$, since everything would be in I. Thus the second conjuct implies that every $b' \in I$, since it is less than b, fails to satisfy $\theta_0^*(a, b')$, and so $\neg\exists b\theta_0(a, b)$ is true in I, so $a \notin A_0$, a contradiction.

So $A_1 \subseteq Y^*$ and $A_0 \cap Y^* = \emptyset$. Moreover, since Y^* is defined by p.r. relations and is bounded above by d, Y^* is an M-finite set. Putting $Y = Y^* \cap I$, we get an M-coded subset of I which separates A_0 and A_1. Thus the model I satisfies Σ_1^0 separation.

Now Σ_1^0 separation implies Δ_1^0-comprehension. Suppose $\varphi(x)$ and $\psi(x)$ are Σ_1^0 and Π_1^0 respectively, and are equivalent. Then $\neg\psi(x)$ is Σ_1^0, and

$$\{x\colon \varphi(x) \wedge \neg\psi(x)\} = \emptyset,$$

so Σ_1^0 separation gives a set which separated them; this is preciely the set whose existence is required for Δ_1^0-comprehension.

Hence I models $\mathbf{RCA}_0$, and thus by our last lemma, since it also models Σ_1^0 separation, it is a model for $\mathbf{WKL}_0$. □

Theorem 5.9. *If a Π_2^0 sentence ψ is provable in* $\boldsymbol{WKL}_0$*, then it is provable in* ***PRA****.*

Proof. We again prove the contraposative, supposing that **PRA** does not prove ψ. So by the completeness theorem, there is a (countable) model M of **PRA** where ψ is false. Since ψ is Π_2^0, we can write $\psi = \forall x\exists y\theta(x, y)$, for a Σ_0^0 formula θ. Then there is some $b \in M$ such that $M \models \neg\exists y\theta(b, y)$.

We now introduce constants $\mathbf{b}$ and $\mathbf{c}$, considering the theory T consisting of **PRA** plus $\neg\exists y\theta(\mathbf{b}, y)$ and $f(\mathbf{b}) < \mathbf{c}$ for every one-ary p.r. function symbol f.

For any finite subset $T_0 \subseteq T$, we can find a $c_0 \in M$ which is greater than $f(b)$ for the finitely many function symbols f mentioned in T_0. Then, interpreting $b = \mathbf{b}$ and $c_0 = \mathbf{c}$, we have $M \models T_0$. Hence the compactness theorem implies that T has a countable model, call it N.

Then N is a model of **PRA** with distinguished elements $b', c' \in N$ such that $b' << c'$ and $N \models \neg\exists y\theta(b', y)$. By Key Lemma 1, there is a semiregular cut $I \subseteq N$ containing b' but not c'. Then Key Lemma 2 allows us to get that

$$(I, \mathrm{Coded}_M(I), +_M \restriction I, \cdot_M \restriction I, <_M \restriction I, 0_M, 1_M)$$

is a model for $\mathbf{WKL}_0$. But since $b' \in I$, this model also satisfies $\neg\exists y\theta(b', y)$, and hence satisfies $\neg\psi$. By the soundness theorem, $\neg\psi$ is then consistent with $\mathbf{WKL}_0$, and hence ψ is not provable in $\mathbf{WKL}_0$, as desired. □

Now, we have proved the result we set out to. What does this get us? At the least, it gives some indication of what **PRA**, and hence finitism, is strong enough to prove. However, the ability to prove Π_2^0 sentences (and hence, *a fortiori*, Π_1^0 sentences) is of particular interest for Hilbert's Program. This is because proofs of consistency were of special interest to Hilbert, and statements expressing consistency are Π_1^0. They can be expressed by means of the sort of coding mentioned in Section 4, since we can code not just formulas, but formal proofs in arithmetic languages such as **PRA**. And we can also code a provability predicate. Hence consistency statements are of the form

$$\forall x \neg ((x \text{ is a sequence number for a sentence } \psi) \ \wedge ((\psi \wedge \neg\psi) \text{ is provable})),$$

which is a Π^0_1 sentence. That consistency proofs must be finitistic implied a certain form of reliability to Hilbert. Thus, as Simpson explains in [6], "reducing to finitism" means, for Hilbert, proving that stronger proof systems are Π^0_1 conservative over **PRA**.

It is worth considering, if we are reducing to **PRA** for the sake of its greater epistemic integrity, does our proof of this reduction itself possess this greater certainty? Now, the proof presented here requires the completeness theorem, among other things, which places us at the level of $\mathbf{RCA}_0$. However, as Simpson writes in [6], others have shown that conservativity can in fact be proved in **PRA**, albeit by a different, more proof-theoretic method. Thus the reduction of $\mathbf{WKL}_0$ to finitism is as indubitable as finitism itself.

Now, we will conclude with a sketch of an extension of conservativity to a new system, $\mathbf{WKL}_0^+$.

6. Upgrading Conservativity to $\mathbf{WKL}_0^+$

The system $\mathbf{RCA}_0^+$ appears in Simpson's study of the reverse mathematics of the Baire Category Theorem (BCT) in [5]. It turns out that $\mathbf{WKL}_0$ is not strong enough to prove BCT for separable metric spaces, but $\mathbf{RCA}_0$ plus the new axiom scheme (*) is enough. Suppose σ, τ are variables ranging over $2^{<\omega}$ and X over 2^ω. Let φ be any formula with only first order quantifiers. Then (*) is the following formula:

$$(*)\ \ \forall n \forall \sigma \exists \tau (\tau \supseteq \sigma \wedge \varphi(n,\tau)) \rightarrow \exists X \forall n \exists k (\varphi(n, X[k]))$$

where $\tau \supseteq \sigma$ means that the string σ is an initial segment of the string τ, and $X[k]$ indicates the string consisting of the first k digits of the infinite sequence X. The antecedent of the formula in the axiom indicates a dense collection of strings in $2^{<\omega}$, namely all of the τs. The consequent guarantees the existence of a path, X, which intersects all such dense sets. $\mathbf{RCA}_0^+$ is $\mathbf{RCA}_0$ plus the (*) schema, and $\mathbf{WKL}_0^+$ is $\mathbf{WKL}_0$ plus the (*) schema. As might be guessed, $\mathbf{WKL}_0$ and $\mathbf{RCA}_0^+$ are incomparable, and of course, $\mathbf{WKL}_0^+$ is stronger than both.

We will give an outline of the extension of conservativity to $\mathbf{WKL}_0^+$, listing the requisite lemmas along with some explanation and proof sketches. Complete proofs may mostly be found in [5] with a few from Section IX.2 of [2].

The new material presented in this section will be a proof that $\mathbf{WKL}_0^+$ is conservative over $\mathbf{RCA}_0$ for Π^1_1 sentences. It is as simple matter to combine with the results of the previous sectin to get Π^0_2 conservativity over **PRA**. The general procedure for this proof will be to show that models of $\mathbf{RCA}_0$ are ω-submodels of models with more stringent conditions.

We will need a couple of new definitions relating to binary trees in order to complete this proof. Let $2^{<\omega}_M$ denote the collection of all M-finite binary sequences, and recall that a set is *M-definable* if it is definable by a formula with parameters from $M \cup S_M$.

Definition 6.1. (1) A collection $D \subseteq 2^{<\omega}_M$ is *dense* if, for each $\sigma \in 2^{<\omega}_M$, there is some $\tau \in D$ such that $\tau \supseteq \sigma$.
(2) A set $G \subseteq M$ is *M-generic* if, for each M-definable dense set D, we have $D \cap G \neq \emptyset$.

Lemma 6.2. *Let M be a countable model of $\boldsymbol{RCA}_0$. Then there is a countable model M' such that $S_{M'}$ contains some M-generic set G.*

This first lemma is both the most technical and the most interesting in the extension to $\mathbf{WKL}_0^+$. We note that the argument is essentially forcing, in the sense of Paul Cohen, so the proof is likely to seem familiar to those with a background in set theory. The forcing conditions are trees, and the generic set is, well, the M-generic set in the sense of trees. First, it must be shown that an M-generic set G exists. We start with a model M'' which is just the first-order part of M, with $S_{M''} = S_M \cup G$. The meat of the proof is to show that this model M'' satisfies Σ^0_1 induction. Once that has been shown, Lemma 4.2 serves to extend to a model M' of $\mathbf{RCA}_0$ such that $M \subseteq_\omega M'' \subseteq_\omega M'$, which completes the proof.

Lemma 6.3. *Let M be a countable model of $\boldsymbol{RCA}_0$. Then there is a countable model M' of $\boldsymbol{WKL}_0$ such that M is an ω-submodel of M'.*

It is an easy corollary of Lemma 6.2 that given a model M of $\mathbf{RCA}_0$ and a tree T definable in M, there is a path through T, namely G. Then, we can apply this corollary repeatedly to get an ascending chain of ω-submodels

$$M = M_0 \subseteq_\omega M_1 \subseteq_\omega \cdots \subseteq_\omega M_i \subseteq_\omega \cdots \qquad (i < \omega)$$

such that each models that more trees have paths. Then, we let M' be the union of all the M_i (really, we need only take the union of the second-order parts S_{M_i}.) Lastly, just check that $M \subseteq_\omega M'$ and $M' \models \mathbf{WKL}_0$.

Though we will not discuss this further, it is an immediate corollary of Lemma 6.3 that $\mathbf{WKL}_0$ is conservative over $\mathbf{RCA}_0$ for Π^1_1 sentences, and also that Σ^0_1-$\mathbf{PA}$ is the first order part of $\mathbf{WKL}_0$, as it is for $\mathbf{RCA}_0$ (these results can be found in Section IX.3 of [2]).

Lemma 6.4. *Let M be a countable model of $\boldsymbol{RCA}_0$. Then there is a countable model M' of $\boldsymbol{WKL}_0^+$ such that M is an ω-submodel of M'.*

To prove this last lemma, we must construct another chain of ω-submodels

$$M = M_0 \subseteq_\omega M_1 \subseteq_\omega \cdots \subseteq_\omega M_i \subseteq_\omega \cdots \qquad (i < \omega),$$

this time satisfying the following conditions:

(1) $M_{2i+1} \models \mathbf{RCA}_0 + \exists X(D \cap X \neq \emptyset))$, for all M_{2i}-definable dense sets D; and
(2) $M_{2i} \models \mathbf{WKL}_0$.

This can be done by alternately applying Lemmas 6.2 and 6.3. Then check, as Simpson does in [5], that the union of these M_i satisfies $\mathbf{WKL}_0^+$.

With these lemmas in hand, the desired theorem is an easy corollary, proved almost exactly as Theorem 5.9 was.

Theorem 6.5. *$\mathbf{WKL}_0^+$ is conservative over $\mathbf{RCA}_0$ for Π^1_1 sentences (and hence for Π^0_2 sentences as well).*

To prove this, assume $\mathbf{RCA}_0$ doesn't prove some Π^1_1 sentence $\varphi = \forall X \theta(X)$; so it proves $\exists X \neg\theta(X)$. Take a model for $\mathbf{RCA}_0 + \exists X \neg\theta(X)$. Use the lemmas to extend it to an ω-supermodel which still contains this X and models $\mathbf{WKL}_0^+$, and this gives the result.

Corollary 6.6. *$\mathbf{WKL}_0^+$ is conservative over $\mathbf{PRA}$ for Π^0_2 sentences.*

Proof. Clearly $\mathbf{WKL}_0^+$ is stronger than $\mathbf{PRA}$. Now, if ψ is a Π^0_2 sentence provable in $\mathbf{WKL}_0^+$, then by Theorem 6.5, ψ is provable in $\mathbf{RCA}_0$ and thus in the stronger $\mathbf{WKL}_0$. Since ψ is provable in $\mathbf{WKL}_0$, then by Theorem 5.9, it is provable in $\mathbf{PRA}$, as desired. □

This completes the extension of Π^0_2 conservativity to $\mathbf{WKL}_0^+$. It is interesting to observe that the "bottleneck" in the power of the different systems appears to be not between $\mathbf{RCA}_0$ and stronger systems like $\mathbf{WKL}_0$ and $\mathbf{WKL}_0^+$, which permit at least Π^1_1 conservativity (and hence conservativity for *all* arithmetic sentences, and more), but rather between $\mathbf{RCA}_0$ and $\mathbf{PRA}$, which cuts us down to a very limited selection of arithmetic sentences. This gives some indication of just how limiting Hilbert's finitism is.

The last thing we note is that $\mathbf{WKL}_0^+$ is strong enough to prove some powerful theorems of functional analysis, such as the open mapping theorem and the closed graph theorem for separable Banach spaces. This makes the fact that this system is finitistically reducible particularly surprising and interesting from the perspective of the foundations of mathematics.

Acknowledgements

Many thanks to my mentor, Isabella Scott, for helping me understand the difficult proofs, especially because we were mostly learning this material for the first time together, and for being very patient. I would also like to thank Professor Denis Hirschfeldt, who suggested the topic of conservativity theorems, and has offered helpful explanations along the way. Finally, my thanks to Professor Peter May for organizing the 2019 REU program, which made this learning experience possible.

References

[1] Herbert B. Enderton. A Mathematical Introduction to Logic. Academic Press. 2001.
[2] Stephen G. Simpson. Subsystems of Second Order Arithmetic. Springer. 1999.
[3] William Tait. Finitism. Journal of Philosophy, Vol.78 No.9 (1981) pp.524-546.

[4] Schirn, Matthias Niebergall, Karl-Georg. Finitism = PRA? On a thesis of W. W. Tait. Reports on Mathematical Logic. 2005.

[5] Douglas K. Brown, Stephen G. Simpson. The Baire Category Theorem in Weak Subsystems of Second-Order Arithmetic. The Journal of Symbolic Logic, Vol. 58, No. 2 (Jun., 1993), pp. 557-578.

[6] Stephen G. Simpson. Partial Realizations of Hilbert's Program. The Journal of Symbolic Logic, Vol. 53, No. 2 (Jun., 1988), pp. 349-363.