REVERSE MATHEMATICS:
CALIBRATING LOGICAL STRENGTH IN MATHEMATICS

by

Noah A. Hughes

Honors Thesis

Appalachian State University

Submitted to the Department of Mathematical Sciences
and The Honors College
in partial fulfillment of the requirements for the degree of

Bachelor of Science

May, 2014

Approved by:

Jeffry L. Hirst, Ph.D., Thesis Director

Brad R. Conrad, Ph.D., Second Reader

Vicky W. Klima, Ph.D., Director, Departmental Honors

Leslie Sargent Jones, Ph.D., Director, The Honors College

Abstract

In this work we introduce the reader to the program of reverse mathematics. This is done by discussing second order arithmetic and constructing the *big five* subsystems of second order arithmetic used in reverse mathematics. These five subsystems may be used to classify mathematical theorems in terms of their logical strength. A theorem independent of this classification is considered as well. The work concludes with an original article by Hirst and Hughes in which *marriage theorems* are analyzed via the language of reverse mathematics.

Acknowledgements

I owe my gratitude to more people than I could hope to list here. First and foremost, I would like to acknowledge and thank Professor Jeff Hirst, my advisor, for all he has taught me in the past year while I prepared this work. This project has inspired me to follow mathematical logic in my graduate studies and career and I am indebted to Dr. Hirst for introducing me to this field.

I would also like to thank the entire mathematics faculty at Appalachian State University. My interest in theoretical mathematics was inspired by them and due to their influence I am further than I ever would have expected to be when I began my undergraduate studies.

Finally I would like to thank my wonderful family and friends for all the help they've provided me along the way.

I Introduction

Mathematics, since its inception, has played a very important role in scientific thought, aiding in the development and expansion of human knowledge. Though this was the case, it was not until the 19th century and the abstraction of modern mathematics that mathematicians began looking deeper into what we call *foundations of mathematics.* Questions regarding some of the most basic mathematical concepts were brought to light: what is a number, a function, or a set? What are the appropriate axioms for use of numbers, functions, and sets? And how do we classify an "appropriate" set of axioms? This attention to foundational questions gave rise to the field of mathematical logic within which strict formalization gives us better insight into the inner workings of mathematics.

Much progress has been made in this field, but there are always more questions to be answered. One such pervading question is *"what is the appropriate axiomatization of mathematics?"* This is an extremely difficult question due to its shear scope. In an effort to gain insight into this question, let us ask something more specifc. We can divide mathematics into two subcategories, that of set theoretic mathematics and non-set theoretic mathematics. We will refer to the latter category as *ordinary* mathematics. We may make this distinction because set theoretic mathematics in general requires a much "stronger" axiomatization than ordinary mathematics.

The de facto axiomatization for set theoretic mathematics are the *Zermelo-Fraenkel* axioms, or ZF. Zermelo proposed the first axiomatic set theory in 1908 [21] but it was not until the early 1920s that Fraenkel would bolster this axiom system to what we know today as ZF [4]. As these are the axioms for set theoretic mathematics, they must assert the existence of some extremely sophisticated sets. For instance, if $\mathcal{P}(X)$ is the set containing every subset of X, then ZF can verify the existence of the set $\{Z_0, \mathcal{P}(Z_0), \mathcal{P}(\mathcal{P}(Z_0)), \dots\}$ for any infinite set Z_0. Therefore, if we rank the strength of an axiom system by the *set*

comprehension (how many sets that can be proven to exist) we see that ZF is extremely strong. It turns out that for the majority of ordinary mathematics, this extensive set comprehension is not needed. In fact, much weaker axiom systems can be used.

In the 1930s, Hilbert and Bernays published *Grundlagen der Mathematik* (Foundations of Mathematics) Volumes I [10] and II [11] which introduced *second order arithmetic*. This is an alternative foundation within which one can formalize much, but not all, of mathematics. Second order arithmetic is much weaker than ZF; we may only assert the existence of *countable* sets. It is interesting that a large amount of mathematics can be done with this little set comprehension. Indeed, even weaker systems than second order arithmetic can be used to do a substantial amount of mathematics. This provides a natural motivation for comparing mathematical theorems via the amount of set comprehension needed to state and prove them. Let us examine a possible strategy for "calibrating" the logical strength of mathematics via set comprehension.

Consider a weak axiom system $\mathcal{B}$ in which we are afforded little set comprehension. We will refer to $\mathcal{B}$ as the *base theory*. Suppose we have two mathematical theorems ζ_1 and ζ_2 such that ζ_1 is provable in $\mathcal{B}$ and ζ_2 is not. Suppose that instead an additional axiom A', appending more set comprehension to $\mathcal{B}$, is needed to prove ζ_2. We have that

$$\mathcal{B} \vdash \zeta_1 \qquad \text{and} \qquad \mathcal{B} + A' \vdash \zeta_2.$$

We may immediately conclude that ζ_2 is a stronger theorem than ζ_1 relative to our base theory because ζ_2 requires more set comprehension to be proven. Note that $\mathcal{B} + A' \vdash \zeta_2$ is equivalent to stating $\mathcal{B} \vdash A' \rightarrow \zeta_2$.

We have gained a small amount of insight into appropriate axiomatizations for the theorems ζ_1 and ζ_2 but we can do better. This is where the notion of "reversing" mathematics comes into play. We know the additional set comprehension afforded by A'

is needed to prove ζ_2 but it could be the case that A' provides more set comprehension than needed. (There could be a weaker axiom that proves ζ_2 when added to $\mathcal{B}$.) We can see if this is the case by deriving A' from the system $\mathcal{B} + \zeta_2$, that is, proving that

$$\mathcal{B} \vdash \zeta_2 \to A'.$$

If we can do this, we will have shown that

$$\mathcal{B} \vdash A' \leftrightarrow \zeta_2,$$

which implies that A' appends the exact amount of set comprehension needed to prove ζ_2. We now have clearly measured the difference in the logical strength of ζ_1 and ζ_2.

We call deriving A' from $\mathcal{B} + \zeta_2$ *reversing* ζ_2 to A'. The name *reversal* comes from the idea that we are doing mathematics backwards. The usual practice is to derive mathematical theorems from a set of axioms and we instead derived an axiom from a mathematical theorem.

Suppose we consider a third theorem ζ_3 and after some analysis find that the axiom A'' is needed in order to prove ζ_3 in the base theory. Assume we have found the reversal of ζ_3 to A'' as well. So,

$$\mathcal{B} \vdash A'' \leftrightarrow \zeta_3.$$

We conclude ζ_3 is stronger than ζ_1 but more information is needed to understand the relationship between ζ_2 and ζ_3. We need to know how the axioms A' and A'' compare.

At this point, we may wonder if this is a lucrative strategy. Determining the relationship between A' and A'' may be very difficult and as we study more and more theorems we may find that an unmanageable amount of axioms are needed to classify their logical strength. The insight at the heart of *reverse mathematics* is that with the correct base

theory, only four additional axioms are needed to classify an enormous amount of ordinary mathematics. Moreover, the systems obtained from appending each of these axioms to the base theory form a natural hierarchy with which we may categorize mathematical theorems. We call the program dedicated to classifying mathematical theorems with these five systems the *program of reverse mathematics*.

Friedman introduced the five systems and the program of reverse mathematics in the 1970s. The base theory is denoted RCA_0 and the four additional systems obtained from appending set comprehension axioms are

$$\mathsf{WKL}_0 \qquad \mathsf{ACA}_0 \qquad \mathsf{ATR}_0 \qquad \Pi^1_1 - \mathsf{CA}_0.$$

Each is a *subsystem* of second order arithmetic. From left to right, the systems increase in logical strength. Friedman introduced prototypes for these five systems in [5]. Later, in [6], Friedman introduced the systems we use today which have less induction than the originals. These systems are commonly referred to as the *big five*.

Reconsider our three theorems in the setting of reverse mathematics. Suppose we find that

$$\mathsf{RCA}_0 \vdash \zeta_1,$$

$$\mathsf{RCA}_0 \vdash \mathsf{WKL}_0 \leftrightarrow \zeta_2,$$

$$\mathsf{RCA}_0 \vdash \mathsf{ATR}_0 \leftrightarrow \zeta_3.$$

We then know exactly how strong each theorem is and how they relate. ζ_1 is the weakest theorem, ζ_2 is one level stronger on our scale and ζ_3 is the strongest at level four of our hierarchy.

This analysis can be done for a remarkable amount of ordinary mathematics. Other systems may be used to the same end and there are many theorems which lie outside

this classification, but an impressive amount can be learned from this program. The classification has flourished over the past forty years and encompasses many theorems from algebra and analysis as well as topology, mathematical logic and many other fields.

On a grander scale, reverse mathematics can be done with very strong axiom systems. Friedman has done work using ZFC (ZF with the *axiom of choice*) as the base theory to consider theorems which are independent of the usual axiomatization of mathematics. This allows conclusions to be made as to whether these theorems are reasonable to accept or not. We will not consider reverse mathematics of this type. See Friedman's work on boolean relation theory.

In this work we will first consider the system of second order arithmetic before constructing each of the big five subsystems and analyzing the mathematics classified by them. In §II.7 we consider a theorem that is independent of this classification. The last section, §III, presents an original article written by Hirst and Hughes in which several *marriage theorems* (as defined in the article) are analyzed and classified via the program of reverse mathematics. This article has been submitted to the Archive for Mathematical Logic.

II Touring the Subsystems

II.1 Second Order Arithmetic

The machinery of Friedman's program of reverse mathematics is realized in *second order arithmetic*. Second order arithmetic can be described in terms of its *language*, that is the symbols we can use to build formulae and its *models* which serve as the semantic interpretation for the words and formulae we form using the syntax of our language.

We will denote the *language of second order arithmetic* by L_2. L_2 is a two sorted

language, meaning there are two types of variables which range over two distinct classes of objects. The first type are *number variables*, denoted by lower-case roman letters, for example i, j, k, m, and n. The second are *set variables*, denoted by upper-case roman letters, *e.g.* X, Y, and Z. Canonically, the number variables are intended to range over the set of *natural numbers* denoted $\omega = \{0, 1, 2, \dots\}$, and the set variables are intended to range over the collection of subsets of ω denoted $\mathcal{P}(\omega)$.

The remaining elements of L_2 are used to define *terms* and *formulae*. In L_2, there are two binary operation symbols, $+$ and $\cdot$, and two constant symbols, 0 and 1. *Numerical terms* are number variables, the symbols 0,1, and $t + t'$ and $t \cdot t'$ where t and t' are numerical terms. There are three *atomic formulae* in L_2, namely: $t = t'$, $t < t'$, and $t \in X$ where X is any set variable. (Numerical terms are meant to denote natural numbers, in which case these formulae take on the usual meaning, *i.e.* t equals t', t is less than t', and t is an element of X.) Using the logical connectives $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$ (and, or, not, implies, if and only if), *number quantifiers*, $\exists n$, $\forall n$ (there exists n, for all n) and *set quantifiers*, $\exists X$, $\forall X$, we may form other formulae from the three atomic formulae. Variables which are not quantified are called *free*. A formula with no free variables is called a *sentence*. The *universal closure* of a formula φ is the sentence obtained by adding a universal quantifier ($\forall$) for every free variable in φ.

Definition 1 (L_2-models)**.** A *model* for L_2 is an ordered 7-tuple

$$M = (M', \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$$

where M' is a set and $\mathcal{S}_M$ is a set of subsets of M which are respectively the range of number variables and set variables, $+_M$ and $\cdot_M$ are binary operations on M', 0_M and 1_M are specific elements in M', and $<_M$ is a binary relation on M'. M' and $\mathcal{S}_M$ are understood to be nonempty disjoint sets.

We may find many such models for L_2 but the intended model, which coincides with the canonical interpretations of expressions in L_2 mentioned above, is

$$(\omega, \mathcal{P}(\omega), +, \cdot, 0, 1, <)$$

where ω and $\mathcal{P}(\omega)$ are as above and $+, \cdot, 0, 1, <$ take on their natural interpretation. In general, an *ω-model* differs from the intended model only by replacing $\mathcal{P}(\omega)$ with some set $\mathcal{S}$ so that $\varnothing \neq \mathcal{S} \subseteq \mathcal{P}(\omega)$. There are still other types of models of L_2, but they reach beyond the scope of this treatise. See Part B of Simpson [18].

Using the preceding discussion, we may formulate the axiom system for full second order arithmetic.

Definition 2 (Second Order Arithmetic)**.** The universal closure of the following L_2-formulae along with classical predicate calculus make up the *axioms of second order arithmetic*:

(i) basic axioms:

Classical predicate calculus with equality.

$n + 1 \neq 0$	$m \cdot 0 = 0$
$m + 1 = n + 1 \to m = n$	$m \cdot (n + 1) = (m \cdot n) + m$
$m + 0 = m$	$\neg\, m < 0$
$m + (n + 1) = (m + n) + 1$	$m < n + 1 \leftrightarrow (m < n \vee m = n)$

(ii) induction axiom:

$$(0 \in X \wedge \forall n\,(n \in X \to n + 1 \in X)) \to \forall n\,(n \in X)$$

(iii) comprehension scheme:

$$\exists X \, \forall n \, (n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ is any formula of L_2 in which X does not occur freely.

This system is extremely rich in the amount of mathematics that it can express. The comprehension scheme asserts the existence of the set X which is defined by $\varphi(n)$. If $\varphi(n)$ was to be the formula $\exists m(m + m + m = n)$ then the comprehension scheme ensures the existence of the set of multiples of three. Free variables may appear in $\varphi(n)$ in which case they are referred to as *parameters*.

It turns out that in any ω-model of L_2 the *full second order induction scheme* is satisfied, that is, the universal closure of

$$(\varphi(0) \wedge \forall n \, (\varphi(n) \rightarrow \varphi(n+1))) \rightarrow \forall n \, \varphi(n)$$

where $\varphi(n)$ is any formula of L_2.

A *formal system* is defined by specifying a language and a set of axioms, we then call a *theorem* any formula of the given language which is logically deducible from the axioms. Thus, by the *system* of second order arithmetic $\mathbf{Z}_2$ we mean the formal system in L_2 made up of the axioms in Definition 2 and any and all formulae of L_2 which may be deduced from the axioms. We use predicate calculus for this deduction, including the usual equality axioms and the law of excluded middle. For a thorough treatment of predicate calculus see Hamilton [9].

We may now define a *subsystem* of $\mathbf{Z}_2$ by any formal system in L_2 whose axioms are each a theorem of $\mathbf{Z}_2$. $\mathbf{Z}_2$ has infinitely many subsystems but we will be concerned with very few of them, that is *the big five*. Each subsystem we will investigate will consist of the basic axioms of $\mathbf{Z}_2$ with limitations imposed upon the induction and set comprehension

schemata. The differences in the limitations of each subsystem yields a hierarchy in the five systems through which we may calibrate the logical strength of theorems in ordinary mathematics.

In order to discuss our base subsystem RCA_0, we need to define some categories of formulae.

Definition 3 (Bounded Quantifiers)**.** Let φ be a formula of L_2, n a number variable, and t a numerical term in which n does not occur. The formulae $\exists n(n < t \wedge \varphi)$ and $\forall n(n < t \to \varphi)$ are abbreviated $(\exists n < t)\varphi$ and $(\forall n < t)\varphi$ respectively. The quantifiers $\exists n < t$ and $\forall n < t$ are *bounded quantifiers.*

Definition 4 (Σ^0_k and Π^0_k formulae)**.** An L_2 formula is Σ^0_0 if it consists of only atomic formulae, logical connectives and bounded quantifiers. For $k \in \omega$, an L_2 formula is Σ^0_k, respectively Π^0_k, if it is of the form $\exists n_1 \forall n_2, \exists n_3, \ldots, n_k \varphi$ respectively $\forall n_1 \exists n_2, \forall n_3, \ldots, n_k \varphi$ where φ is Σ^0_0.

Thus a Π^1_0 formula is of the form $\forall n\ \theta$ with θ being Σ^0_0. Though these formulae contain no set quantifiers, they may contain free set variables. It is important to note that the negation of a Σ^0_k formula is Π^0_k and vice versa. Now that we have established the differences between formulae in L_2 we are ready to begin our tour of the subsystems.

II.2 Recursive Comprehension: RCA_0

RCA_0 plays a pivotal role in reverse mathematics by serving as the "weak base theory" we work over. (Though it is the weakest of *the big five* there are still weaker subsystems over which theorems may be proven equivalent to RCA_0.)

RCA stands for "recursive comprehension axiom". This is because the set comprehension of RCA_0 is only powerful enough to assert the existence of *recursive* sets of natural numbers. (These sets are sometimes referred to as *computable.*) An example of a set that

is recursive is $X = \{2n \mid n \in \omega\}$, *i.e.* the set of even natural numbers. To show this set is recursive we need two Σ_1^0 formulae, one to delineate $n \in X$ and one to delineate $n \notin X$, that is

$$\varphi(n) \quad \text{denotes } n \text{ is an element of } X, \text{ and}$$

$$\psi'(n) \quad \text{denotes } n \text{ is not an element of } X.$$

In our example φ describes even numbers while ψ' describes odd numbers; let φ be the formula $\exists m\,(2 \cdot m = n)$ and ψ be the formula $\exists m\,(2 \cdot m + 1 = n)$. We may now algorithmically compute X by checking to see for which $n \in \omega$ $\varphi(n)$ or $\psi'(n)$ holds. This will determine which n belong to X. This ability to verify both what is in and what is not in X is what makes it recursive; we could ask a computer to calculate X by starting at $n = 0$ and working its way through ω. The following formula asserts the existence of X:

$$\forall n\,(\varphi(n) \leftrightarrow \neg\psi'(n)) \rightarrow \exists X\,\forall n\,(n \in X \leftrightarrow \varphi(n)).$$

To simplify this, let $\psi(n)$ denote the negation of $\psi'(n)$ so that

$$\psi(n) = \neg\psi'(n) = \neg\exists m\,(2 \cdot m + 1 = n) = \forall m\,\neg(2 \cdot m + 1 = n).$$

Notice this makes $\psi(n)$ a Π_1^0 formula and we may restate the formula asserting the existence of X:

$$\forall n\,(\varphi(n) \leftrightarrow \psi(n)) \rightarrow \exists X\,\forall n\,(n \in X \leftrightarrow \varphi(n)).$$

We will say $\varphi(n)$ is Δ_1^0 because it is equivalent to both a Σ_1^0 and a Π_1^0 formula. We are ready to present the set comprehension scheme for RCA_0.

Definition 5 (Δ_1^0 Comprehension)**.** The scheme of Δ_1^0 *comprehension* consists of all

axioms of the form

$$\forall n\,(\varphi(n) \leftrightarrow \psi(n)) \rightarrow \exists X\,\forall n\,(n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ is Σ^0_1, $\psi(n)$ is Π^0_1, and X is not free in $\phi(n)$.

The subscript 0 in RCA_0 indicates limited induction in this system, specifically, what we call Σ^0_1 induction. In general, we define Σ^0_k and Π^0_k induction as follows.

Definition 6 (Σ^0_k and Π^0_k Induction)**.** For each $k \in \omega$, the scheme of Σ^0_k induction (respectively Π^0_k induction) consists of all axioms of the form

$$(\varphi(0) \wedge \forall n\,(\varphi(n) \rightarrow \varphi(n+1))) \rightarrow \forall n \varphi(n)$$

where $\varphi(n)$ is any Σ^0_k (respectively Π^0_k) formula of L_2.

With definitions 5 and 6 taken care of we are ready to formally define RCA_0.

Definition 7 (The subsystem RCA_0)**.** RCA_0 is the formal system in the language L_2 whose axioms consist of the basic axioms from Definition 2(i) plus the schemata of Σ^0_1 induction and Δ^0_1 comprehension.

The *minimum ω-model* of RCA_0 is the collection of all recursive subsets of ω, more formally, the collection

$$\mathrm{REC} = \{X \subseteq \omega \mid X \text{ is recursive}\}.$$

Within RCA_0 we can develop a startling amount of mathematics though it has such weak set comprehension. Basic properties regarding the *natural, rational,* and *real* number systems can be shown. For instance, we define $\mathbb{N}$, the natural numbers, to be the unique set X such that $\forall n\,(n \in X)$ and can easily verify the following properties.

Lemma 1. *The following are provable in* RCA_0. *With* $m, n, p \in \mathbb{N}$, *we have*

(i) $0 + m = m$

(ii) $1 + m = m + 1$

(iii) $m + n = n + m$ (addition is commutative)

(iv) $m + p = n + p \to m = n$

(v) $0 \cdot m = 0$

(vi) $1 \cdot m = m$

(vii) $m \cdot n = n \cdot m$ (multiplication is commutative)

(viii) $m \cdot (n + p) = m \cdot n + m \cdot p$

(ix) $(m + n) \cdot p = m \cdot p + n \cdot p$ (the distributive properties)

(x) $(m < n \wedge n < p) \to m < p$ ($<$ is a *transitive* relation)

(xi) $m < n \vee m = n \vee n < m$ (the *trichotomy* of natural numbers)

Note that this is only a sample of the arithmetical properties which can be proven about $\mathbb{N}$. Each property can be verified using straightforward induction on the alphabetically last variable appearing in the statement. Some statements require previous statements for proof. With the addition of several more basic properties of $\mathbb{N}$, we may show the *natural number system* is a *semiring* (a ring whose elements need not have an additive inverse).

Theorem 2. *The following in provable in* RCA_0. *The natural number system*

$$\mathbb{N}, +, \cdot, 0, 1, <, =$$

is a commutative ordered semiring with cancellation.

For the full list of properties needed to prove Theorem 2 see §II.2 of Simpson [18]. We will assume familiarity with terminology used in basic abstract algebra. An excellent reference is Dummit and Foote [3].

This is only the beginning of the elementary number theory which may be expressed in RCA_0. We may encode sets, ordered tuples, and finite sequences as single natural numbers and similarly encode infinite sequences and the Cartesian products as sets. Though the coding of these objects can be cumbersome, once this is done, we can work with the objects naturally. For instance, a function $f : X \to Y$ may be encoded in the usual manner using the Cartesian product $X \times Y$. If X and Y are sets of natural numbers and

$$X \times Y = \{(i, j) \mid i \in X, j \in Y\},$$

then we may define f to be set of all ordered pairs (i, j) so that $f(i) = j$. This definition of a function is rather cavalier, so let us ensure that RCA_0 asserts the existence of these sets.

First we define the code for an ordered pair, that is the *pairing map* defined by

$$(i, j) = (i + j)^2 + i$$

where $n^2 = n \cdot n$. We may prove in RCA_0 that i and j are both less than the (numerical code of the) pair (i, j) and that the pairing map is an *injection* (one-to-one) map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. Note that (i, j) is simply notation, and is not asserting the existence of $\mathbb{N} \times \mathbb{N}$ which is a consequence of the following definition.

Definition 8 (Cartesian Products)**.** Let X and Y be sets of natural numbers. The

Cartesian product of X and Y, denoted $X \times Y$ is the set of all k such that

$$\exists i \leq k \, \exists j \leq k (i \in X \wedge j \in Y \wedge (i, j) = k).$$

This set exists by Σ_0^0 comprehension (this formula is Σ_0^0 because only bounded quantifiers appear).

We write $A \subseteq B$ if and only if $\forall n \, (n \in A \to n \in B)$.

Definition 9 (Functions)**.** A set $f \subseteq X \times Y$ is a *function* if

$$\forall i \, \forall j \, \forall k \, (((i, j) \in f \wedge (i, k) \in f) \to j = k) \text{ and,}$$

$$\forall i \, \exists j \, (i \in X \to (i, j) \in f).$$

If f is a function we write $f : X \to Y$ and let $f(i)$ denote the unique j such that $(i, j) \in f$.

If $f : X \to Y$ and $g : Y \to Z$ are functions on sets of natural numbers, RCA_0 proves the existence of their composition $h = g \circ f : X \to Z$.

Within RCA_0 we may define k-ary functions (functions whose input is a k-tuple and whose output is a natural number) since ordered tuples may be encoded as single natural numbers. These functions are of the form $f : \mathbb{N}^k \to \mathbb{N}$. We define

$$\mathbb{N}^k = \underbrace{\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \times \mathbb{N}}_{k-\text{times}}$$

This leads to a very important result, that of *primitive recursion.*

Theorem 3 (Primitive Recursion, Theorem II.3.4 Simpson [18])**.** *Given $f : \mathbb{N}^k \to \mathbb{N}$ and*

$g : \mathbb{N}^{k+2} \to \mathbb{N}$, RCA_0 *proves the existence of a unique* $h : \mathbb{N}^{k+1} \to \mathbb{N}$ *defined inductively by*

$$\begin{aligned} h(0, n_1, \ldots, n_k) &= f(n_1, \ldots, n_k), \\ h(m+1, n_1, \ldots, n_k) &= g(h(m, n_1, \ldots, n_2), m, n_1, \ldots, n_k). \end{aligned}$$

The proof is omitted but may be found in [18]. This result implies that *elementary function arithmetic* may be developed straightforwardly within RCA_0. For example, we may use Theorem 3 to prove the existence of the exponential function $f(m, n) = m^n$ defined inductively by $f(m, 0) = 1$ and $f(m, n+1) = f(m, n) \cdot m$. Furthermore, within RCA_0 we can prove certain basic properties including $(m_1 m_2)^n = m_1^n m_2^n$ and $m^{n_1} m^{n_2} = m^{n_1+n_2}$. We can also state and prove fundamental results such as the uniqueness of prime factorization.

Many intricate arguments in elementary number theory, finite combinatorics, and finite group theory can be formalized within RCA_0. This is the case as long as the arguments in question make no essential use of infinite sets or of induction on complicated formulae. These finitistic arguments can usually be developed within even weaker systems than RCA_0. We will see that a portion of infinitary mathematics can be developed within RCA_0. As an example we define the *integers*, *rationals* and *reals* after discussing the notion of an *equivalence relation*.

We define an *equivalence relation* as follows. Let $\sim$ be a relation on $\mathbb{N}$. We call $\sim$ an equivalence relation if it is *reflexive*, $a \sim a$, and is *symmetric*, $a \sim b \to b \sim a$ and is *transitive*, $a \sim b \wedge b \sim c \to a \sim c$. The *equivalence class* of an element a is informally the set $\{b \in \mathbb{N} \mid a \sim b\}$. Equivalence classes *partition* the set they are defined on.

We will now define the ring of integers using equivalence classes of ordered pairs (m, n) in $\mathbb{N} \times \mathbb{N}$. Working formally in RCA_0, we introduce new relations on $\mathbb{N} \times \mathbb{N}$ which will encode the structure of $\mathbb{Z}$.

$$
\begin{aligned}
(m,n) +_{\mathbb{Z}} (p,q) &= (m+p, n+q) \\
(m,n) -_{\mathbb{Z}} (p,q) &= (m+q, n+p) \\
(m,n) \cdot_{\mathbb{Z}} (p,q) &= (m \cdot p + n \cdot q, m \cdot q + n \cdot p) \\
(m,n) <_{\mathbb{Z}} (p,q) &\leftrightarrow m + q < n + p \\
(m,n) =_{\mathbb{Z}} (p,q) &\leftrightarrow m + q = n + p
\end{aligned}
$$

It is clear $=_{\mathbb{Z}}$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$. We define an *integer* to be any element of $\mathbb{N} \times \mathbb{N} \subseteq \mathbb{N}$ which is the least element of its equivalence class. "Least" refers to the ordering of $\mathbb{N}$. We may identify $m \in \mathbb{N}$ with $(m, 0) \in \mathbb{Z}$ and $(m, n) =_{\mathbb{Z}} m - n$. We can prove the set $\mathbb{Z}$ of all integers exists within RCA_0 and then define $+, -, \cdot, 0, 1, <$ on $\mathbb{Z}$ accordingly. For instance, for every $a, b \in \mathbb{Z}$ we define $a + b$ to be the unique $c \in \mathbb{Z}$ such that $c =_{\mathbb{Z}} a +_{\mathbb{Z}} b$. From this we can prove $\mathbb{Z}$ is an ordered *integral domain* (a commutative ring in which the product of any two nonzero elements is nonzero). The proof of the following theorem can be done in the same manner as Theorem 2, using statements like those in Lemma 1.

Theorem 4 (Theorem II.4.1 of Simpson [18])**.** *The following is provable in* RCA_0*. The system*

$$\mathbb{Z}, +, -, \cdot, 0, 1, <$$

is an ordered integral domain.

In a very similar fashion we may define the field $\mathbb{Q}$ of rational numbers. With $\mathbb{Z}^+$ the set of positive integers, we define the following operations and relations on $\mathbb{Z} \times \mathbb{Z}^+$ taking (a, b), $(c, d) \in \mathbb{Z} \times \mathbb{Z}^+$.

$$
\begin{aligned}
(a,b) +_{\mathbb{Q}} (c,d) &= (a \cdot d + b \cdot c, b \cdot d) \\
(a,b) -_{\mathbb{Q}} (c,d) &= (a \cdot d - b \cdot c, b \cdot d)) \\
(a,b) \cdot_{\mathbb{Q}} (c,d) &= (a \cdot c, b \cdot d)) \\
(a,b) <_{\mathbb{Q}} (c,d) &\leftrightarrow a \cdot d < b \cdot c \\
(a,b) =_{\mathbb{Q}} (c,d) &\leftrightarrow a \cdot d = b \cdot c
\end{aligned}
$$

As before $=_{\mathbb{Q}}$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^+$. We define a *rational number* to be any element of $\mathbb{Z} \times \mathbb{Z}^+ \subseteq \mathbb{N}$ which is the least element of its equivalence class. The set of all rational numbers is denoted by $\mathbb{Q}$ and we define $+, -, \cdot, 0, 1, <$ on $\mathbb{Q}$ accordingly. We can prove in RCA_0 that $\mathbb{Q}$ is an ordered *field* after defining r/s to be the unique $q \in \mathbb{Q}$ such that $q \cdot s = r$.

The real number system is easy to develop from $\mathbb{Q}$ using a slight modification of the usual definition by Cauchy sequences of rational numbers. We denote the *absolute value* of a rational number $q \in \mathbb{Q}$ by $|q|$ where $|q| = q$ if $q \geq 0$, and $|q| = -q$ otherwise.

Definition 10 (Sequences of rational numbers)**.** A *sequence of rational numbers* is defined in RCA_0 to be a function $f : \mathbb{N} \to \mathbb{Q}$. Such a sequence is denoted by $\langle q_k \mid k \in \mathbb{N} \rangle$ where $q_k = f(k)$.

We adapt the usual definition of a Cauchy sequence to define real numbers in RCA_0.

Definition 11 (The real number system)**.** A *real number* is defined in RCA_0 to be a sequence of rational numbers $\langle q_k \mid k \in \mathbb{N} \rangle$ such that

$$\forall k \, \forall i \, (|q_k - q_{k+i}| \leq 2^{-k+1}).$$

Two real numbers $\langle q_k \mid k \in \mathbb{N} \rangle$ and $\langle q'_k \mid k \in \mathbb{N} \rangle$ are said to be *equal* if $\forall k \ (|q_k - q'_k| \leq 2^{-k+1})$.

The letter $\mathbb{R}$ is a useful shorthand for the colletion of all rapidly converging Cauchy sequences of rationals. In models of second order arithmetic, the collection $\mathbb{R}$ of *all* real numbers is not a member of the set universe (it is a set of sets). However, many statements about real numbers and analysis can be formulated without making use of the set of all reals.

It is interesting to consider alternative definitions of a real number. For instance, we could define a real number to be an equivalence class of rapidly converging Cauchy sequences or a representative of an equivalence class. Both are erroneous choices for our goal. Equivalence classes require the language of third order arithmetic and we would need a strong from of the axiom of choice to select representatives for the reals. In fact, this form of choice is not available even in full second order arithmetic $\mathbf{Z}_2$.

We have only begun to scratch the surface of the mathematics we may formalize in RCA_0. We have already seen that Theorems 2, 3, and 4 are provable in RCA_0. From here we could formulate *complete separable metric spaces*, *continuous* real-valued functions, weak forms of basic results in mathematical logic or countable fields. As an illustration of the substantial amount of ordinary mathematics we can develop in RCA_0 we present Theorem 5.

Theorem 5. *The following are provable in* RCA_0.

(i) *The system* $\mathbb{Q}, +, -, \cdot, 0, 1, <$ *is an ordered field.*

(ii) The uncountability of $\mathbb{R}$. *For any sequence of real numbers* $\langle x_n \mid n \in \mathbb{N} \rangle$ *there exists a real number* y *such that* $\forall n \, (x_n \neq y)$.

(iii) The intermediate value theorem on continuous real-valued functions. *If* $\phi(x)$ *is a continuous real-valued function on the unit interval* $0 \leq x \leq 1$ *and* $\phi(0) < 0 < \phi(1)$, *then there exists* c *such that* $0 < c < 1$ *and* $\phi(c) = 0$.

(iv) *Basics of real linear algebra, including Gaussian Elimination.*

(v) *Every countable field has an algebraic closure.*

(vi) *Every countable ordered field has a real closure.*

(vii) A soundness theorem. *If X is a set of sentences of some countable language L and there exists a countable model M such that $M(\phi) = 1$ for all $\phi \in X$, then X is consistent.*

Each of these statements can be found in Simpson [18]: part (i) is Theorem II.4.2; part (ii) is Theorem II.4.9; part(iii) is Theorem II.6.6; part (iv) is Exercise II.4.11; part (v) is Theorem II.9.4; part (vi) is Theorem II.9.7; and part (vii) is Corollary II.8.6.

RCA_0 may be viewed as a formal version of computable mathematics. Since RCA_0 uses classical logic as opposed to intuitionistic logic it differs from constructive mathematics, see Bishop and Bridges [1].

Some, but not all, mathematical theorems can be formulated and proven in RCA_0. This is what makes RCA_0 such a wonderful base theory. There is a non-trivial portion of mathematics which we can formalize within RCA_0 yet we will see that many of the most important theorems require stronger axiom systems. We will also see examples of theorems which fall outside the usual hierarchy of *the big five.* These exceptions are of great interest in reverse mathematics. *Ramsey's theorem for pairs in two colors* is one such exception and will be considered in more detail in § II.7. We conclude this section by presenting two results which are *not* provable within RCA_0. The first statement is Example I.8.7 in Simpson [18] and the second follows from work done by Hirst in [13].

Theorem 6. *The following are not provable in* RCA_0.

(i) The maximum principle. *Every continuous real-valued function on* $[0, 1]$ *attains a supremum.*

(ii) The Infinite Pigeonhole Principle. *If we color each natural number using a finite number of colors, there exists an infinite set such that every element of that set is the same color.*

II.3 Weak König's Lemma: WKL_0

We have seen that a considerable portion of mathematics may be straightforwardly formalized in RCA_0, but the vast majority of ordinary mathematics remains outside the comprehension of RCA_0. In order to reach more and more mathematics we will need to strengthen the system we are working in. We will now present WKL_0, the next of the *big five* subsystems. WKL_0 is relatively simple extension of RCA_0. The axioms of WKL_0 are simply those of RCA_0 with *weak König's lemma* appended (see Theorem 13(ii) and Definition 14). The acronym WKL should now be self-explanatory. In order to state any version of König's lemma we must first introduce the notion of *sequences, initial segments* and *trees.*

First, $\mathbb{N}^{<\mathbb{N}}$ is the set of codes for finite sequences of elements of $\mathbb{N}$. Hence, for $k \in \mathbb{N}^{<\mathbb{N}}$ we have

$$k = (k_0, k_1, k_2, \ldots, k_\ell) \qquad \text{with } k_i \in \mathbb{N}.$$

We consider $k = (k_0, k_1, k_2, \ldots, k_\ell)$ to be a *finite sequence* of natural numbers. We thus consider $\mathbb{N}^{<\mathbb{N}}$ to be the set of (codes for)[1] all finite sequences of natural numbers. To avoid confusion we use the symbols σ, τ and μ to denote arbitrary sequences. We also use angle brackets to denote a sequence, *e.g.*, $\mu = \langle u_0, u_1, \ldots, u_n \rangle$. If $\sigma, \tau \in \mathbb{N}^{<\mathbb{N}}$,

[1] As noted in §II.2, ordered k-tuples (and thus finite sequences) may be encoded as single natural numbers in $\mathbf{Z}_2$. Informally, $\mathbb{N}^{<\mathbb{N}}$ *is* the set of all finite sequences of natural numbers but for sake of formality we must remember we are actually using the encodings of these mathematical objects.

$\sigma = \langle s_0, s_1, \ldots, s_m \rangle$ and $\tau = \langle t_0, t_1, \ldots, t_n \rangle$ we define the *concatenation* of σ and τ as

$$\sigma^\frown\tau = \langle s_0, s_1, \ldots, s_m, t_0, t_1, \ldots, t_n \rangle.$$

If there exists a sequence μ (possibly *null*, $\langle\,\rangle$) such that $\sigma^\frown\mu = \tau$, we call σ an *initial segment* of τ, denoted by $\sigma \subseteq \tau$. Finally, the *length* of $\sigma = \langle s_0, s_1, \ldots, s_m \rangle$ is denoted by $\mathrm{lh}(\sigma)$. In this case $\mathrm{lh}(\sigma) = m + 1$. The formal definition of sequences as sets of natural numbers (from which their code is derived) and the length function can be found in §II.2.6 of Simpson [18].

Definition 12 (Trees)**.** The following is defined within RCA_0. A *tree* is a set $T \subseteq \mathbb{N}^{<\mathbb{N}}$ such that any initial segment of a sequence in T is contained in T, that is

$$\forall\sigma\,\forall\tau\,((\sigma \subseteq \tau \wedge \tau \in T) \to \sigma \in T).$$

T is said to be *finitely branching* if each element in T has only finitely many immediate successors, that is

$$\forall\sigma\,(\sigma \in T \to \exists n\,\forall m\,(\sigma^\frown\langle m\rangle \in T \to m < n)).$$

A *path* through T is a function $g : \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $g[n] \in T$ where $g[n]$ is the initial sequence defined by

$$g[n] = \langle g(0), g(1), \ldots, g(n-1) \rangle.$$

We call T' a *subtree* of T if $\forall\sigma\,(\sigma \in T' \to \sigma \in T)$.

We use $\{0,1\}^{<\mathbb{N}}$ or $2^{<\mathbb{N}}$ to denote the full binary tree, that is, the set of all (codes for) finite sequences of 0's and 1's. We may now present the *full* statement of König's lemma

and *weak König's lemma*.

Definition 13 (Full and Weak König's Lemma)**.**

(i) **König's Lemma.** Every infinite, finitely branching tree T has at least one infinite path.

(ii) **Weak König's Lemma.** Every infinite subtree of $2^{<\mathbb{N}}$ has an infinite path.

It is very important to note the distinction between the full statement of König's lemma and *weak* König's lemma. In Theorem 13, statement (ii) basically says "big, skinny trees are tall" while statement (i) says "a big tree with finite levels is tall." We will see in Theorem 19 that König's lemma is equivalent to ACA_0 over RCA_0.

Though it may be difficult to see how this statement increases the logical strength of RCA_0, the addition of weak König's lemma adds much to RCA_0. It will allow us to assert the existence of non-recursive sets via what is called Σ^0_1 separation (see Theorem 8) and prove many important nonconstructive theorems of mathematics that do not hold in the model REC of RCA_0. We now formally introduce WKL_0.

Definition 14 (The subsystem WKL_0)**.** WKL_0 is the formal system in the language L_2 whose axioms consist of those of RCA_0 together with *weak König's lemma*.

As an immediate example of the strength of WKL_0 we have:

Theorem 7 (Theorem IV.2.3 part 5 of Simpson [18])**.** *The maximum principle: every continuous real-valued function on* $[0, 1]$ *attains a supremum, is provable in* WKL_0.

We recall that the maximum principle is not provable in RCA_0 (see Theorem 6 (i)). The addition of weak König's lemma remedies this and provides us our first opportunity for a *reversal*. It can be shown that, working over RCA_0, Theorem 7 implies weak König's lemma. Thus, these two statements have a biconditional relationship (if and only if) and

are as a consequence provably equivalent over RCA_0. This is important; if we were to show Theorem 7 implies any other mathematical statement, we could immediately conclude the theorem provable in WKL_0. Similarly, if any theorem implies Theorem 7, it must imply weak König's lemma as well. This will provide a new strategy for finding reversals to WKL_0. It turns out that the maximum principle is not very useful in this endeavor, but there are provably equivalent characterizations of WKL_0 which will be of immense use.

Theorem 8 (Σ^0_1 Separation, Lemma IV.4.4 of Simpson [18])**.** *The following are pairwise equivalent over* RCA_0.

(i) WKL_0.

(ii) (Σ^0_1 separation)[2] *Let* φ_0 *and* φ_1 *be* Σ^0_1 *formulae in which* X *does not occur freely. If* $\neg\exists n\,(\varphi_0(n) \wedge \varphi_1(n))$ *then*

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

(iii) *If* $f, g : \mathbb{N} \to \mathbb{N}$ *are one-to-one with* $\forall m\,\forall n\,(f(m) \neq g(n))$*, then*

$$\exists X\,\forall m\,(f(m) \in X \wedge g(m) \notin X).$$

Both statements (ii) and (iii) assert the existence of sets, and are therefore invaluable. Statement (ii) is used for many reversals to WKL_0. In §III, another tool was employed to find a reversal to WKL_0. In order to prove Theorem 9 which appears on page 52, the contrapositive of weak König's lemma was used. The contrapositive states that if a subtree of $2^{<\mathbb{N}}$ has no infinite path, it must be a finite tree.

[2] RCA_0 suffices to prove Π^0_1 separation: For any Π^0_1 formulae ψ_0 and ψ_1 in which Z does not occur freely,

$$\neg\exists n\,(\psi_0(n) \wedge \psi_1(n)) \to \exists Z\,\forall n\,((\psi_0(n) \to n \in Z) \wedge (\psi_1(n) \to n \notin X)).$$

Theorem 8 provides us with more tools to find reversals to WKL_0 but there are also more tools that can help us *prove* theorems in WKL_0. One such example is *bounded König's lemma.*

Definition 15 (Bounded Trees)**.** Within RCA_0, a tree $T \subseteq \mathbb{N}^{<\mathbb{N}}$ is said to be *bounded* if there exists a function $g : \mathbb{N} \to \mathbb{N}$ such that for all $\tau \in T$ and $m < \mathrm{lh}(\tau)$, we have $\tau(m) < g(m)$ where $\tau(m)$ is the m^{th} natural number in the sequence τ.

Bounded König's lemma is the assertion that every bounded infinite tree $T \subseteq \mathbb{N}^{<\mathbb{N}}$ has an infinite path.

Theorem 9 (Lemma IV.1.3 of Simpson [18])**.** *Weak König's lemma is provably equivalent over* RCA_0 *to bounded König's lemma.*

Because *bounded* and *weak* König's lemma are equivalent, we may use them interchangeably in an argument. This proves useful when generalizing results provable in WKL_0 since bounded König's lemma is itself a generalization of weak König's lemma.

We now consider the topic of *differential equations,* namely Peano's theorem for the existence of solutions for ordinary differential equations. We use the usual terminology for differential equations, that is y' denotes the derivative of some unknown y, a function of x, and $f(x, y)$ is a bivariate function in x and y. Peano's theorem says that if $f(x, y)$ is continuous in a neighborhood about the origin, then the initial value problem

$$y' = f(x, y), \qquad y(0) = 0$$

has a solution $y = \phi(x)$ which is continuously differentiable in some neighborhood of $x = 0$. This theorem may be formalized and proven in WKL_0 as shown by Simpson in [18].

Theorem 10 (Peano's theorem in WKL_0, Theorem IV.8.1 of Simpson [18])**.** *The following is provable in* WKL_0*. Let* $f(x, y)$ *be a continuous real-valued function on the rectangle*

$-a \leq x \leq a, -b \leq y \leq b$ *where* $a, b > 0$. *Then the initial value problem*

$$\frac{dy}{dx} = f(x, y), \qquad y(0) = 0$$

has a continuously differentiable solution $y = \phi(x)$ *on the interval* $-\alpha \leq x \leq \alpha$ *where* $\alpha = \min\left(a, \frac{b}{M}\right)$ *and*

$$M = \max\{|f(x, y)| \; \big| \; -a \leq x \leq a, -b \leq y \leq b\}.$$

Using Σ^0_1 separation we may show this statement is equivalent to WKL_0 over RCA_0. This result is of major historical significance. The long standing proof of Peano's theorem relied on what is known as the *Ascoli lemma*. In [19], Simpson showed Ascoli's lemma was not needed and that Peano's theorem was in fact provably weaker than the Ascoli lemma. It turns out that while WKL_0 proves Peano's theorem, WKL_0 cannot prove the Ascoli lemma. We will see in Theorem 19 that the Ascoli lemma is equivalent to ACA_0 over RCA_0.

The addition of weak Konig's lemma to RCA_0 increases the logical strength of RCA_0 a great deal. Surprisingly, WKL_0 and RCA_0 prove exactly the same first order formulas. In the terminology of Simpson [18], their first order part is Σ^0_1-PA, which is Peano arithmetic with induction restricted to Σ^0_1 formulas. More information about Peano arithmetic appears in the next section. When we regard the two systems in the second order setting however, WKL_0 is much stronger and can prove many classical mathematical results that RCA_0 cannot. To observe directly that RCA_0 is strictly weaker than WKL_0 we take note that REC (the minimum ω-model of RCA_0) does not satisfy weak König's lemma and as a result is not an ω-model of WKL_0. Thus, RCA_0 does not prove weak König's lemma. This implies that RCA_0 is a *proper* (strictly weaker) subsystem of WKL_0.

We have already seen *the maximum principle* from Theorem 7, statements (ii) and (iii) of Theorem 8, Theorem 10 and *bounded König's lemma* as examples of theorems for which the full strength of WKL_0 is needed. Each of these theorems are provably equivalent to WKL_0 over RCA_0. We now present Theorem 11 as further example of the mathematics which may be formalized within WKL_0.

Theorem 11. *One can prove the following statements equivalent to* WKL_0 *over* RCA_0.

(i) The Heine/Borel Theorem for [0,1]: *Given sequences of real numbers* $c_i, d_i, i \in \mathbb{N}$, *if*

$$\forall x\,(0 \leq x \leq 1 \rightarrow \exists i\,(c_i < x < d_i)),$$

then

$$\exists n\,\forall x\,(0 \leq x \leq 1 \rightarrow \exists i\ \leq n(c_i < x < d_i)).$$

(ii) The Heine/Borel Theorem for compact metric spaces.

(iii) *Every continuous real-valued function on* $[0,1]$ *is bounded.*

(iv) *For every continuous function* $\phi(x)$ *on a closed bounded interval* $a \leq x \leq b$, *the Riemann integral* $\int_a^b \phi(x)dx$ *exists and is finite.*

(v) Gödel's completeness theorem: *Every countable consistent set* X *of sentences has a model,* i.e., *there exists a countable model* M *such that* $\forall\sigma\,(\sigma \in X \rightarrow M(\sigma) = 1)$.

(vi) Gödel's compactness theorem: *If each finite subset of* X *has a model then* X *has a model.*

(vii) *Every countable commutative ring has a prime ideal.*

(viii) *Every countable field has a unique algebraic closure.*

(ix) Brouwer's fixed point theorem: *Every uniformly continuous function* $\phi : [0,1]^n \to [0,1]^n$ *has a fixed point.*

Each of these statements can be found in Simpson [18]: part (i) is Lemma IV.1.1; part (ii) is Theorem IV.1.5; part (iii) is part 3 of Theorem IV.2.3; part (iv) is Theorem IV.2.7; parts (v) and (vi) are parts 3 and 4 Theorem IV.3.3; part (vii) is part 2 of Theorem IV.6.4; part (viii) is Theorem IV.5.2; and part (ix) is Theorem IV.7.6.

We conclude with several remarks on Theorem 11. We previously discussed the maximum principle and WKL_0. Here we see WKL_0 proves (iii) and (iv) which are intuitively stronger statements than the maximum principle. Theorem 5 (viii) asserts the existence of an algebraic closure for every countable field, which is provable in RCA_0. Theorem 11 (viii) asserts that this algebraic closure is *unique*. These examples exemplify how WKL_0 is strictly stronger than RCA_0. Statement (v) is generalized to (vi) via use of *bounded König's lemma.*

II.4 Arithmetical Comprehension: ACA_0

The next subsystem we will be concerned with is ACA_0, which adds comprehension for *arithmetically definable sets* to RCA_0. The acronym ACA stands for "arithmetical comprehension axiom." To discuss arithmetically definable sets we must first define *arithmetical formulae.*

Definition 16 (Arithemetical Formulae)**.** If φ is a formula of the language L_2, we say that φ is *arithmetical* if and only if φ contains no set quantifiers. Note that φ may contain free set variables.

A set X then is arithmetically definable if and only if there exists some φ such that φ is arithmetical and

$$\forall n \, (n \in X \leftrightarrow \varphi(n)).$$

The formal definition of ACA_0 is relatively simple.

Definition 17 (The subsystem ACA_0)**.** The axioms of ACA_0 are the basic axioms and induction axiom from Definition 2 along with comprehension axioms

$$\exists X \, \forall n \, (n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ is any arithmetical formula in which X does not occur freely.

A model of ACA_0 is any L_2-structure

$$M = (M', \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$$

that satisfies the arithmetical comprehension scheme, that is, $\mathcal{S}_M$ contains all subsets of M' which are arithmetically definable with parameters from $M' \cup \mathcal{S}_M$.

Within ACA_0, we have as a consequence of arithmetical comprehension and the induction axiom, the *arithmetical induction scheme*:

$$(\varphi(0) \wedge \forall n \, (\varphi(n) \rightarrow \varphi(n+1))) \rightarrow \forall n \; \varphi(n)$$

where φ is any arithmetical formula.

It is obvious that the addition of arithmetical comprehension gives ACA_0 significantly more set comprehension than RCA_0 but we see that much more induction is available in ACA_0 as well due to arithmetical comprehension. It seems intuitive that ACA_0 is a stronger subsystem than RCA_0 but to verify this we simply note that the model REC of RCA_0 does not contain every arithmetical set and therefore cannot be a model of ACA_0. Hence, ACA_0 can not be proven in RCA_0. It can also be shown that ACA_0 is stronger than WKL_0.

There is a very close relationship between ACA_0 and first order arithmetic $\mathbf{Z}_1$. If we define L_1 to be the *language of first order arithmetic* (*i.e.* L_2 with the set variables omitted), then we say *first order arithmetic* is the formal system $\mathbf{Z}_1$ whose language is L_1 and whose axioms are the basic axioms from Definition 2 with the *first order induction scheme* (induction on first order formulae of L_1). First order arithmetic is often referred to as *Peano arithmetic*, PA. It can be shown that for any model of ACA_0, say

$$(M', \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M),$$

its first order part

$$(M', +_M, \cdot_M, 0_M, 1_M, <_M)$$

is a model of $\mathbf{Z}_1$. Conversely, we may also take any countable model of $\mathbf{Z}_1$, say

$$(M', +_M, \cdot_M, 0_M, 1_M, <_M),$$

and find an appropriate $\mathcal{S}_M \subseteq \mathcal{P}(M')$ (the set of all subsets of M') such that

$$(M', \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$$

is a model of ACA_0. This implies that for any L_1-sentence σ, σ is a theorem of (provable in a model of) ACA_0 if and only if σ is a theorem of $\mathbf{Z}_1$. We say then that ACA_0 is a *conservative extension* of first order arithmetic, *i.e.*, the first order part of ACA_0 is $\mathbf{Z}_1$. This property of ACA_0 aids us in studying what is provable in PA. For instance, proving *Fermat's last theorem* within ACA_0 would show it is a theorem of Peano arithmetic. This has not been done but would be a quite remarkable result.

We discussed in §II.3 that WKL_0 is equivalent to Σ^0_1 separation and that this equivalence

is of great use in finding reversals to WKL_0. This was presented in Theorem 8. In a similar fashion, there are statements provably equivalent to ACA_0 which in many cases make finding a reversal easier. Two of these are given in the following theorem.

Theorem 12 (Lemma III.1.3 of Simpson [18])**.** *The following are pairwise equivalent over* RCA_0.

(i) ACA_0

(ii) Σ^0_1 comprehension*, i.e.,* $\exists X \, \forall n \, (n \in X \leftrightarrow \varphi(n))$ *restricted to* Σ^0_1 *formulas* $\varphi(n)$ *in which* X *does not occur freely.*

(iii) *For all one-to-one functions* $f : \mathbb{N} \to \mathbb{N}$ *there exists a set* $X \subseteq \mathbb{N}$ *such that* $\forall n \, (n \in X \leftrightarrow \exists m \, (f(m) = n))$*, that is,* X *is the range of* f*.*

The implications (i) $\to$ (ii) and (i) $\to$ (iii) are immediate by use of arithmetical comprehension. For (ii) $\to$ (i), we note that any arithmetical formula is equivalent to a Σ^0_k formula for some $k \in \omega$. It can be shown by induction that Σ^0_1 comprehension implies Σ^0_k comprehension for any $k \in \omega$. Hence, (ii) $\to$ (i). (iii) $\to$ (i) is not as simple and requires a lemma in RCA_0 regarding recursive functions and their ranges, see [18].

ACA_0 is sufficiently strong to prove several results concerning *countable abelian groups, countable commutative rings,* and *countable vector spaces.* RCA_0 is sufficient to define these objects but the definitions are fairly technical. As example of this we define countable abelian groups and omit the definitions of countable commutative rings and countable vector spaces.

Definition 18 (Countable Abelian Groups within RCA_0)**.** Within RCA_0, we define a *countable Abelian group* A to be a set $A' \subseteq \mathbb{N}$ together with a binary operation $+_A : A' \times A' \to A'$, a unary operation $-_A : A' \to A'$, and a distinguished element $0_A \in A'$ such that the system $A', +_A, -_A, 0_A$ obeys the usual Abelian group axioms of *closure,*

identity, inverses, associativity, and *commutativity.* We use primitive recursion to define $f : \mathbb{N} \times A' \to A'$ by $f(0, a) = 0$, $f(n + 1, a) = f(n, a) + a$ and set $na = f(n, a)$. Thus

$$na = \underbrace{a + a + \cdots + a}_{n\text{-times}}.$$

The definitions of countable commutative rings and countable vector spaces are set up similarly. For example, to define a ring R we will need two binary operations $+_R, \cdot_R : R' \times R' \to R'$ and two distinguished elements $0_R, 1_R \in R'$ for obvious reasons. We can define a countable vector space V by taking an abelian group $V', +_V, -_V, 0_V$ and a countable field K (a special case of the countable commutative ring) and defining a function $\cdot_V : K' \times V' \to V'$ that models scalar multiplication.

For our first example of an algebraic result within ACA_0 we consider the *torsion elements* of a countable Abelian group A. We call any element of a countable Abelian group A a torsion element if it is of finite order, that is $a \in A$ is a torsion element if $\exists n\,(n \geq 1 \wedge na = 0)$.

Theorem 13 (Torsion Subgroup, Theorem III.6.2 of Simpson [18])**.** ACA_0 *is equivalent over* RCA_0 *to the assertion that every countable Abelian group A has a subgroup consisting of the torsion elements.*

To prove the assertion of a torsion subgroup from ACA_0 is fairly simple. We may use arithmetical comprehension to form the set T of torsion elements in A. By letting $\varphi(m)$ be the formula

$$m \in A \wedge \exists n\,(n \geq 1 \wedge nm = 0)$$

we obtain T from arithmetical comprehension, *i.e.*,

$$\exists T\, \forall m\,(m \in T \leftrightarrow \varphi(m)).$$

From here it is not difficult to verify T is a subgroup of A. The *reversal* is a degree more difficult. In view of Theorem 12, we need only consider an arbitrary injection $f : \mathbb{N} \to \mathbb{N}$ and use the existence of torsion subgroups to compute the range of f. To do this though we need to discuss T in terms of its *generators* and *relations* which are notions not discussed in this work.

Theorem 14 gives example of two more algebraic results provable in and equivalent to ACA_0. We say an ideal M of a ring R is *maximal* if the quotient ring R/M is a field. (See Dummit and Foote [3] for a discussion on the algebraic structures mentioned in this work.)

Theorem 14. *The following assertions are pairwise equivalent over* RCA_0.

(i) ACA_0

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

(iii) *Every countable vector space over a countable field has a basis.*

Part (ii) of Theorem 14 is part 2 of Theorem III.5.5 of Simpson [18] while part (iii) is part 2 of Theorem III.4.3.

We turn now from countable algebraic structures to infinitary combinatorics. *König's lemma*, as stated in Theorem 13(i), is a basic result equivalent to ACA_0 over RCA_0. König's lemma though, is a very general statement about some finitely branching infinite tree $T \subseteq \mathbb{N}^{<\mathbb{N}}$. Note that there is no upper bound on the number of immediate successors any node in T can have. We may place a bound on this number and yield results which remain equivalent to ACA_0 as illustrated by the following theorem.

Theorem 15 (Theorem III.7.2 part 3 of Simpson [18])**.** ACA_0 *is provably equivalent over* RCA_0 *to König's lemma restricted to tress* $T \subseteq \mathbb{N}^{<\mathbb{N}}$ *such that* $\forall \sigma \in T$, σ *has at most two immediate successors in* T.

This reversal is done via the equivalence of ACA_0 to statement Theorem 12(iii) as in [18]. This statement is similar to weak König's lemma (Theorem 13(ii)) but note that weak König's lemma not only places a bound on the number of branches attached to each node, but also bounds the *labels* which can be used for each node. It is this further restriction which allows for only 0 and 1 labels that causes weak König's lemma to be weaker than ACA_0.

Ramsey's theorem is another basic result of infinitary combinatorics that has been studied in reverse mathematics. Before we can state the theorem we need to introduce a small bit of notation (defined in RCA_0). For any $X \subseteq \mathbb{N}$ and $\ell \in \mathbb{N}$, we define $[X]^\ell$ to be the set of all increasing sequences of length ℓ in X. RCA_0 proves that for each X and ℓ, $[X]^\ell$ exists.

Theorem 16 (Ramsey's theorem for exponent ℓ)**.** Ramsey's theorem for exponent ℓ *or* $\mathrm{RT}(\ell)$ *states that for all* $\ell \in \mathbb{N}$ *and all* $f : [\mathbb{N}]^\ell \to \{0, 1, \ldots, k-1\}$*, there exist* $c < k$ *and an infinite set* $X \subseteq \mathbb{N}$ *such that* $f(m_1, \ldots, m_\ell) = c$ *for all* $\langle m_1, \ldots, m_\ell \rangle \in [X]^\ell$*.*

There are many ways to state and interpret Ramsey's theorem. Here we may think of coloring all of the ordered (increasing) ℓ-tuples of natural numbers with k many colors. Ramsey's theorem guarantees the existence of an infinite set X such that every ℓ-tuple within $[X]^\ell$ has the the same color c.

ACA_0 suffices to prove $\mathrm{RT}(\ell)$ for every $\ell \in \omega$. This is implied by the following lemma.

Lemma 17 (Lemma III.7.4 of Simpson [18])**.** ACA_0 *proves* $\mathrm{RT}(0)$ *and*

$$\forall \ell \, (\mathrm{RT}(\ell) \to (\mathrm{RT}(\ell + 1)).$$

Proving $\mathrm{RT}(0)$ is trivial. If we assume $\mathrm{RT}(\ell)$ to induct on ℓ we may prove $\mathrm{RT}(\ell+1)$ by a careful application of König's lemma as in [18]. We cannot carry out Ramsey's original

proof within ACA_0 though it is relatively simple.

Considering the reversal yields interesting results. Similar to König's lemma for trees, cases of Ramsey's theorem have different logical strength depending on the the structure of the sequences in question, namely, their length. We can obtain the following reversal by use of Theorem 12(ii).

Lemma 18 (Lemma III.7.5 of Simpson [18])**.** *It is provable in* RCA_0 *that* RT(3) *implies* ACA_0.

We formalize the equivalence between ACA_0 and Ramsey's theorem below in Theorem 19(i). The cases where $\ell \leq 2$ are interesting exceptions to the usual results in reverse mathematics. RT(1) and RT(2) are both independent of the *big five* subsystems as we will see in §II.7. It is interesting to note the statement $\forall k\, \mathrm{RT}(k)$ is not provable in ACA_0, but instead is provable in the system of ACA_0^+ which appends an existence axiom for ω-jumps.

We conclude our treatment of ACA_0 with Theorem 19. Statement (vii), the Ascoli lemma, was remarked on in §II.3 with respect to Peano's theorem for ordinary differential equations. Note that statement (vi), the *Bolzano/Weierstraß theorem*, is the special case of (vii) in which $\hat{A}$ and $\hat{B}$ are closed bounded intervals and each f_n is a constant function.

Theorem 19. *One can prove the following statements equivalent to* ACA_0 *over* RCA_0.

(i) $\mathrm{RT}(\ell)$ *for* $\ell \geq 3$.

(ii) *Every countable integral domain has a maximal ideal.*

(iii) *Every countable field has a strong algebraic closure.*

(iv) *For every pair of countable fields* $K \subseteq L$ *there exists a transcendence base for* L *over* K.

(v) *Every countable vector space over an infinite countable field either is finite dimensional or contains an infinite linearly independent set.*

(vi) *The Bolzano/Weierstraß theorem: Every bounded sequence of real numbers contains a convergent subsequence.*

(vii) *The Ascoli lemma: Let $\hat{A}$ and $\hat{B}$ be compact metric spaces. If $\langle f_n : n \in \mathbb{N} \rangle$ is a sequence of continuous functions $f_n : \hat{A} \to \hat{B}$ then there exists a uniformly convergent subsequence $\langle f_{n_k} : k \in \mathbb{N} \rangle$ where for every k, $n_k < n_{k+1}$.*

Each of the these statements can be found in Simpson [18]: part (i) is Theorem III.7.6; part (ii) is Theorem III.5.5 part 3; part (iii) is Theorem III.3.2 part 2; part (iv) is Theorem III.4.6 part 2; part (v) is Theorem III.4.4 part 3; parts (vi) and (vii) are Theorem III.2.9 parts 2 and 3.

II.5 Arithmetical Transfinite Comprehension: ATR_0

ATR_0 is by far the most technical subsystem of the *big five* to define. ATR stands for "arithmetical transfinite recursion." This is because ATR_0 allows for the iteration of arithmetical comprehension a *transfinite* number of times. We use the term transfinite to designate orderings that include a copy of $\mathbb{N}$ as an initial segment. ATR_0 can be characterized as the weakest system in which one can develop a decent theory of *countable well orderings*. ATR_0 is a vastly stronger system than ACA_0 as will be evident from the set comprehension axiom given in its defintion, Definition 20.

To define the system we will first need to formalize the notion of a countable well ordering. These are the transfinite objects we will iterate arithmetical comprehension along. Recall that in §II.2 we encoded $\mathbb{N} \times \mathbb{N}$ as a subset of $\mathbb{N}$ via the pairing map

$$(i, j) = (i + j)^2 + i.$$

This proved vital in the construction of number systems within RCA_0 and with many other coding endeavors including functions and sequences. Identifying $\mathbb{N} \times \mathbb{N}$ this way allows us to discuss binary relations on $\mathbb{N}$ as subsets of $\mathbb{N} \times \mathbb{N}$. We say a set $X \subseteq \mathbb{N} \times \mathbb{N}$ is *reflexive* if for every i and j we have that

$$(i, j) \in X \to ((i, i) \in X \wedge (j, j) \in X).$$

If X is reflexive then we write $\text{field}(X) = \{i \mid (i, i) \in X\}$ We write

$$i \leq_X j \leftrightarrow (i, j) \in X, \text{ and}$$

$$i <_X j \leftrightarrow ((i, j) \in X \wedge (j, i) \notin X)$$

for reasons which will become obvious after Definition 19.

Definition 19 (Countable Well Orderings)**.** The following definitions are made within RCA_0. Let $X \subseteq \mathbb{N}$ be *reflexive*.

(i) We say that X is *well founded* if it has no infinite descending sequence, that is, there is no $f : \mathbb{N} \to \text{field}(X)$ such that $f(n+1) <_X f(n)$ for all $n \in \mathbb{N}$. We let $\text{WF}(X)$ be the formula that states X is well founded.

(ii) We say that X is a *countable linear ordering* if it is a reflexive linear ordering of its field, that is,

$$\forall i \, \forall j \, \forall k \, ((i \leq_X j \wedge j \leq_X k) \to i \leq_X k),$$

$$\forall i \, \forall j \, ((i \leq_X j \wedge j \leq_X i) \to i = j),$$

$$\forall i \, \forall j \, (i, j \in field(X) \to (i \leq_X j \vee j \leq_X i)).$$

We let $\text{LO}(X)$ be the formula that states X is a countable linear ordering.

(iii) We say that X is a *countable well ordering* it is simultaneously a countable linear ordering and well founded. We let $\mathrm{WO}(X)$ be the formula that states X is a countable well ordering.

Now we can define arithmetical transfinite recursion. Suppose we have some arithmetical formula $\theta(n, Y)$ and a countable well ordering X. We wish to associate a set Y_j to each $j \in \mathrm{field}(X)$. We do this by defining the Y_j's via transfinite recursion along X. Assuming that Y_i has been defined for all $i <_X j$, we define

$$Y^j = \{(m, i) \mid i <_X j \wedge m \in Y_i\}$$

and

$$Y_j = \{n \mid \theta(n, Y^j)\}.$$

Intuitively, Y^j is the cumulative result of comprehension by θ applied repeatedly along X up to j. Y_j is then the result of applying θ one more time.

Formally, we define $\mathrm{H}_\theta(X, Y)$ to be the formula which states $\mathrm{LO}(X)$ and that Y is the set of all pairs (n, j) such that for every $j \in \mathrm{field}(X)$ we have $\theta(n, Y^j)$ where $Y^j = \{(m, i) \mid i <_X j \wedge (m, i) \in Y\}$. Basically, $\mathrm{H}_\theta(X, Y)$ says that Y records the entire computation of iterating θ along each $j \in \mathrm{field}(X)$.

We note that ACA_0 suffices to prove that if X is a countable well ordering then there is at most one Y such that $\mathrm{H}_\theta(X, Y)$ before presenting the formal definition of ATR_0.

Definition 20 (The subsystem ATR_0)**.** ATR_0 is the formal system in the language L_2 whose axioms consist of those of ACA_0 plus all instances of

$$\forall X \, (\mathrm{WO}(X) \to \exists Y \, \mathrm{H}_\theta(X, Y))$$

where θ is arithmetical.

We have seen that defining the system ATR_0 is no menial task. In order to avoid being burdened by the technical details we next present an expression equivalent to ATR_0, that is Σ^1_1 *seperation*. We saw in §II.3 that WKL_0 was equivalent to Σ^0_1 seperation, here we have Theorem 20.

Theorem 20 (Theorem V.5.1 of Simpson [18])**.** *The following are equivalent over* RCA_0.

(i) *Arithmetical transfinite recursion.*

(ii) *The* Σ^1_1 separation principle: *For any* Σ^1_1 *formulas* $\varphi_1(n)$ *and* $\varphi_0(n)$ *in which* $Z \subseteq \mathbb{N}$ *does not occur freely, we have*

$$\neg\exists n\,(\varphi_1(n) \wedge \varphi_0(n)) \rightarrow$$

$$\exists Z\,\forall n\,((\varphi_1(n) \rightarrow n \in Z) \wedge (\varphi_0(n) \rightarrow n \notin Z)).$$

It is known that ATR_0 lies strictly between ACA_0 and $\Pi^1_1 - \mathsf{CA}_0$. We can think of this as an analogous postion to WKL_0 between RCA_0 and ACA_0 in terms of logical strength. We should note though that there is a vast jump in strength when moving from the principle of Σ^0_1 seperation to Σ^1_1 seperation.

Just as with WKL_0, Theorem 20(ii) is used in many reversals to ATR_0. Many theorems provable in ATR_0 mention sets which are usually defined by arithmetical transfinite recursion. Proving reversals of these theorems shows that the use of transfinite recursion is logically necessary. For example, transfinite recursion is necessary in the construction of comparison maps for well orderings, as shown by the following theorem.

Theorem 21 (Friedman, appears as Theorem V.6.8 in Simpson [18].)**.** RCA_0 *can prove the following are equivalent:*

(i) ATR_0

(ii) Comparability of well orderings: *If $WO(X)$ and $WO(Y)$, then there is an order preserving bijection of X onto an initial segment of Y or of Y onto an initial segment of X.*

We finish with a short discussion on trees in ATR_0, the following results will parallel results in §II.6.

Theorem 22 (Theorem V.5.2 part 3 of Simpson [18])**.** *The following are equivalent over* RCA_0.

(i) *Arithmetical transfinite recursion.*

(ii) *For any sequence of trees $\langle T_i \mid i \in \mathbb{N}\rangle, T_i \subseteq \mathbb{N}^{<\mathbb{N}}$, if for every i, T_i has at most one path then*

$$\exists Z\, \forall i\, (i \in Z \leftrightarrow T_i \text{ has a path.}).$$

Note the restriction on each T_i, we will see in Theorem 25 that $\Pi^1_1 - \mathsf{CA}_0$ is equivalent to the same assertion with no restriction on the number of paths each T_i can have.

Definition 21 (Perfect Trees)**.** Within RCA_0, a finite sequence $\tau \in \mathbb{N}^{<\mathbb{N}}$ is said to be an *extension* of $\sigma \in \mathbb{N}^{<\mathbb{N}}$ if $\sigma \subseteq \tau$, that is,

$$\mathrm{lh}(\sigma) \leq \mathrm{lh}(\tau) \wedge \forall i\, (i < \mathrm{lh}(\sigma) \to \sigma(i) = \tau(i)).$$

Two finite sequences $\tau_1, \tau_2 \in \mathbb{N}^{<\mathbb{N}}$ are said to be *incompatible* if neither is an extension of the other, that is,

$$\exists i\, (i < \min(\mathrm{lh}(\tau_1), \mathrm{lh}(\tau_2)) \wedge \tau_1(i) \neq \tau_2(i)).$$

A tree $T \subseteq \mathbb{N}^{<\mathbb{N}}$ is said to be *perfect* if each element of T has a pair of incompatible

extensions in T, that is,

$$(\forall \sigma \ \in T)(\exists \tau_1, \tau_2 \in T)(\sigma \subseteq \tau_1 \wedge \sigma \subseteq \tau_2 \wedge \tau_1, \tau_2 \text{ are incompatible.}).$$

The statements in the following theorem are equivalent to what is known as the *perfect set theorem*. We will see in §II.6 that a similar, yet more specific theorem is equivalent to $\Pi^1_1 - \mathsf{CA}_0$.

Theorem 23 (Theorem V.5.5 part 4 of Simpson [18])**.** *The following are equivalent over* RCA_0.

(i) *Arithmetical transfinite recursion.*

(ii) *For every tree* $T \subseteq \mathbb{N}^{<\mathbb{N}}$*, if* T *has uncountably many paths, then* T *has a nonempty perfect subtree.*

We conclude this section with Theorem 24.

Theorem 24. *One can prove the following statements equivalent to* ATR_0 *over* RCA_0.

(i) *Any two well orderings are comparable,* i.e.,

$$\forall X \, \forall Y \, ((\, WO(X) \wedge \, WO(Y)) \rightarrow (|X| \leq |Y| \vee |Y| \leq |X|)).$$

(ii) *The* Σ^1_1 bounding principle: *For any* Σ^1_1 *formula* $\varphi(X)$*, if* $\forall X \, (\varphi(X) \rightarrow \, WO(X))$ *then*

$$\exists Y \, (\, WO(Y) \wedge \forall X \, (\varphi(X) \rightarrow |X| < |Y|)).$$

(iii) *For every tree* $T \subseteq 2^{<\mathbb{N}}$*, if* T *has uncountably many paths, then* T *has a nonempty perfect subtree.*

(iv) The perfect set theorem: *Every uncountable analytic set has a perfect subset.*

(v) *Every countable reduced Abelian p-group has an Ulm resolution.*

(vi) Ulm's theorem: *Any two countable reduced Abelian p-groups which have the same Ulm invariants are isomorphic.*

Each of these statements can be found in Simpson [18]: part (i) is Thereom V.6.8; part (ii) follows from part (i) and Lemma V.6.2; part (iii) is Theorem V.5.5 part 3; part (iv) is Theorem V.5.5 part 2; part (v) is Theorem V.7.3 part 2; and part (vi) is Theorem V.7.1.

II.6 Π^1_1 Comprehension: $\Pi^1_1 - \mathsf{CA}_0$

The last and strongest of the *big five* subsystems of $\mathbf{Z}_2$ is $\Pi^1_1 - \mathsf{CA}_0$. We have already seen that the system ATR_0 is very strong. $\Pi^1_1 - \mathsf{CA}_0$ is even stronger, yet still very much weaker than *full* second order arithmetic. Most theorems that need the set comprehension afforded in $\Pi^1_1 - \mathsf{CA}_0$ are extremely sophisticated and exceed the scope of this work. Because of this our treatment of $\Pi^1_1 - \mathsf{CA}_0$ is quite brief. The proof of each result can be found in [18].

Relative to ATR_0 this system is extremely simple to define. Paralleling the definition of ACA_0, we have Definition 22.

Definition 22 (The subsystem $\Pi^1_1 - \mathsf{CA}_0$)**.** $\Pi^1_1 - \mathsf{CA}_0$ is the formal system in the language L_2 whose axioms consist of the basic axioms and the induction axiom in Definition 2 together with comprehension axioms

$$\exists X \, \forall n \, (n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ is any Π^1_1 formula in which X does not occur freely.

Theorem 25 (Theorem VI.1.1 of Simpson [18]). *The following are equivalent over* RCA_0.

(i) Π^1_1 *comprehension.*

(ii) *For any sequence of trees* $\langle T_i \mid i \in \mathbb{N} \rangle$ *with* $T_i \subseteq \mathbb{N}^{<\mathbb{N}}$*, there exists a set* X *such that*

$$\forall i \, (i \in X \leftrightarrow T_i \text{ has a path.}).$$

We see that Theorem 25(ii) is essentially a generalization of Theorem 22(ii). Recall from Theorem 23 that ATR_0 is equivalent to the assertion that any tree with uncountably many paths must have a perfect subtree. The following theorem presents an analog for $\Pi^1_1 - \mathsf{CA}_0$. We will see that not only does $\Pi^1_1 - \mathsf{CA}_0$ guarantee the existence of a perfect subtree, it guarantees the existence of specific perfect subtrees.

For a tree $T \subseteq \mathbb{N}^{<\mathbb{N}}$, we define the *perfect kernel* of T in RCA_0 to be the union of all of the perfect subtrees of T, provided this union exists. Note that the perfect kernel of T is a perfect tree (if it exists) and in fact, is the unique largest perfect subtree of T.

Theorem 26 (Theorem VI.1.3 parts 1, 2 and 4 of Simpson [18]). *The following are equivalent over* RCA_0.

(i) *Arithmetical transfinite recursion.*

(ii) *For any tree* $T \subseteq \mathbb{N}^{<\mathbb{N}}$*, the perfect kernel of* T *exists.*

(iii) *For any tree* $T \subseteq \mathbb{N}^{<\mathbb{N}}$*, there is a perfect subtree* $P \subseteq T$ *such that the set of paths through* T *which are not paths through* P *is countable.*

Note that not only are these perfect subtrees very specific subtrees but they are subtrees of a very general tree T. Recall that in ATR_0, the existence of a perfect subtree is only guaranteed for trees with uncountable many paths. Here $\Pi^1_1 - \mathsf{CA}_0$ guarantees

the existence of the unique largest perfect subtree of T for any $T \subseteq \mathbb{N}^{<\mathbb{N}}$ as well as the existence of the specific subtree P mentioned in statement (iii). We will see in the following theorem that these statements hold for trees $T \subseteq 2^{<\mathbb{N}}$ as well.

Simpson uses theorems 25 and 26 to prove the equivalence of $\Pi^1_1 - \mathsf{CA}_0$ to the famous *Cantor/Bendixson theorem* in [18]. We conclude our treatment of $\Pi^1_1 - \mathsf{CA}_0$ with Theorem 27 in which the Cantor/Bendixon theorem and a number of other equivalent statements to $\Pi^1_1 - \mathsf{CA}_0$ are presented.

Theorem 27. *The following are provably equivalent to* $\Pi^1_1 - \mathsf{CA}_0$ *over* RCA_0.

(i) *The* Cantor/Bendixson theorem for $\mathbb{N}^{\mathbb{N}}$: *Every closed set in* $\mathbb{N}^{\mathbb{N}}$ *is the union of a perfect closed set and a countable set*

(ii) *The* Cantor/Bendixson theorem for $2^{\mathbb{N}}$.

(iii) *For any tree* $T \subseteq 2^{<\mathbb{N}}$, *the perfect kernel of* T *exists.*

(iv) *For any tree* $T \subseteq 2^{<\mathbb{N}}$, *there is a perfect subtree* $P \subseteq T$ *such that the set of paths through* T *which are not paths through* P *is countable.*

(v) *Every countable Abelian group is the direct sum of a divisible group and a reduced group.*

Each of these statements can be found in Simpson [18]: parts (i) and (ii) are Theorem VI.1.6 pars 2 and 3; parts (iii) and (iv) are Theorem VI.1.3 parts 3 and 5; and part (v) is Theorem VI.4.1 part 2.

II.7 Exceptions

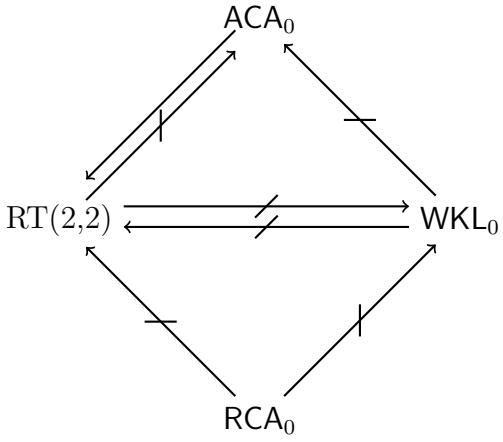
We have seen that a startling amount of mathematics is either provable in RCA_0 or provably equivalent to one of the stronger subsystems in the big five. There are theorems

that fall outside this hierarchy though. We will consider one such example, *Ramsey's theorem for pairs in two colors* or RT(2,2). We define a *complete* graph to be a graph such that there is an edge between every two vertices.

Theorem 28 (RT(2,2))**.** *Given an infinite complete graph, if we color each edge with one of two colors then there exists an infinite subgraph such that each edge is of the same color.*

In 1962, Specker showed that RCA_0 cannot prove RT(2,2) [20]. This begged the question if RT(2,2) was provable in a higher system. Jockusch's work in 1972 [15] verified that WKL_0 cannot prove RT(2,2) but that ACA_0 can. The remaining question was the reversal to ACA_0. Over two decades later, in 1995 Slaman and Seetapun showed that RT(2,2) does not prove ACA_0 [17]. This result was remarkable as it solidified the fact that RT(2,2) is not provably equivalent to any of the big five systems in reverse mathematics. One question was left, that is, whether WKL_0 was provable from RT(2,2) or not. It was not until very recently, in 2012, that Liu showed WKL_0 is *not* provable from RT(2,2) [16].

Thanks to the work over the last 50 years, we now know that RT(2,2) lies between ACA_0 and RCA_0 in terms of its logical strength but is incomparable with WKL_0. We summarize these relationships in the following figure.



There are many other theorems which cannot be classified using the usual hierarchy in reverse mathematics. For example, Hirschfeldt and Shore [12] give examples of principles weaker than RT(2,2) that fit this category.

Another such result, the *infinite pigeonhole principle* (Theorem 6(ii)), was shown to be equivalent to $\mathsf{B}\Sigma_2$, a bounding scheme for Σ^0_2 formula by Hirst in [13]. This result implies that the infinite pigeonhole principle lies between ACA_0 and RCA_0 and is incomparable to WKL_0.

III Original Results

We conclude this work with the original article *Reverse mathematics and marriage problems with unique solutions* written by Hirst and Hughes. The article has been submitted to the Archive for Mathematical Logic. The work was done during the summer and fall of 2013. The reverse mathematics done in this paper served as the inspiration for this thesis. A combined bibliography for the paper and this introduction appears as the last section.

Reverse mathematics and marriage problems with unique solutions

Jeffry L. Hirst and Noah A. Hughes[3]

January 28, 2014

Abstract

We analyze the logical strength of theorems on marriage problems with unique solutions using the techniques of reverse mathematics, restricting our attention to problems in which each boy knows only finitely many girls. In general, these marriage theorems assert that if a marriage problem has a unique solution then there is a way to enumerate the boys so that for every m, the first m boys know exactly m girls. The strength of each theorem depends on whether the underlying marriage problem is finite, infinite, or bounded.

Our goal is to analyze the logical strength of some marriage theorems using the framework of reverse mathematics. The subsystems of second order arithmetic used here are RCA_0, which includes comprehension for recursive (also called computable) sets of natural numbers, WKL_0, which appends a weak form of König's Lemma for trees, and ACA_0, which appends comprehension for arithmetically definable sets. Simpson's book [18] provides detailed axiomatizations of the subsystems and extensive development of the program of reverse mathematics.

We use the standard anthropocentric terminology for marriage theorems. A *marriage problem* consists of a set B of boys, a set G of girls, and a relation $R \subset B \times G$ where $(b, g) \in R$ means "b knows g." A *solution* of the marriage problem is an injection $f : B \to G$ such that for all $b \in B$, $(b, f(b)) \in R$. Informally, f assigns a spouse to each boy, chosen from among his acquaintances and avoiding polygamy. In general, marriage

[3]Authors' address: Department of Mathematical Sciences, Appalachian State University, Boone, NC 28608

Corresponding author: Jeffry L. Hirst `jlh@math.appstate.edu` TEL: 1-828-262-2861 FAX: 1-828-265-8617

Keywords: reverse mathematics, combinatorics, marriage theorems, transversal, SDR, unique matching

MSC Classification: Primary: 03B30, 03F35 Secondary: 05D15, 05C70

theorems provide necessary and sufficient conditions for the existence of solutions or, in our case, for the existence of unique solutions. These sorts of results are often expressed using other terminology such as transversals, systems of distinct representatives (SDRs), and matchings in bipartite graphs.

As a notational convenience, we use some set theoretic notation as abbreviations for more complicated formulas of second order arithmetic. If $b \in B$, we write $G(b)$ for $\{g \in G \mid (b, g) \in R\}$. In the marriage problems for this paper each boy knows at most finitely many girls, so for each b, RCA_0 can prove the existence of $G(b)$. Although $G(b)$ looks like function notation, it is not. In general, RCA_0 can prove the existence of a function uniformly mapping each boy to (the integer code for) the finite set $G(b)$ if and only if the marriage theorem is *bounded*, as defined after Theorem 2. We further abuse this notation by using formulas like $g \in G(B_0)$ to abbreviate $\exists b \in B_0((b, g) \in R)$. In settings that address more than one marriage problem, we write $G_M(B_0)$ to denote girls known by boys in B_0 in the marriage problem M. Cardinality notation like $|X| \leq |Y|$ abbreviates the assertion that there is an injection from X into Y. The formula $|X| < |Y|$ abbreviates the conjunction of $|X| \leq |Y|$ and $|Y| \not\leq |X|$. For finite sets, RCA_0 can prove many familiar statements about cardinality, for example, if X is finite and $y \notin X$ then $|X| < |X \cup \{y\}|$.

Given a marriage problem $M = (B, G, R)$ with a solution f, for any $B_0 \subset B$ the restriction of f is an injection of B_0 into $G(B_0)$. Consequently, RCA_0 proves that if M has a solution then $|B_0| \leq |G(B_0)|$ for every $B_0 \subset B$. Philip Hall [8] proved the converse for finite marriage problems. The following theorem shows that Philip Hall's result can be formalized and proved in RCA_0 and appears as Theorem 2.1 of Hirst [14].

Theorem 1. (RCA_0) *If $M = (B, G, R)$ is a finite marriage problem satisfying $|B_0| \leq |G(B_0)|$ for every $B_0 \subset B$, then M has a solution.*

Marshall Hall, Jr. [7] extended Philip Hall's theorem to infinite marriage problems. The following theorem shows that his result is equivalent to ACA_0 and appears as Theorem 2.2 of Hirst [14]. Marriage problems in which boys are allowed to know infinitely many girls are considerably more complex and not considered in this paper.

Theorem 2. (RCA_0) *The following are equivalent:*

1. ACA_0.
2. *If $M = (B, G, R)$ is a marriage problem such that each boy knows only finitely many girls and $|B_0| \leq |G(B_0)|$ for every finite $B_0 \subset B$, then M has a solution.*

Suppose that $M = (B, G, R)$ is a marriage problem in which B and G are subsets of $\mathbb{N}$. We say that M is *bounded* if there is a function $h : B \to G$ such that for each $b \in B$, $G(b) \subseteq \{0, 1, \ldots, h(b)\}$. The function h acts as a uniform bound on the girls that each boy knows, and also insures that each boy knows only finitely many girls. Given such a bounding function, recursive comprehension proves the existence of the function

mapping each b to (the code for) the finite set $G(b)$. As illustrated by the following theorem, bounded marriage theorems are often weaker than their unbounded analogs. The following appears as Theorem 2.3 of Hirst [14].

Theorem 3. (RCA_0) *The following are equivalent:*

1. WKL_0.
2. *If $M = (B, G, R)$ is a bounded marriage problem such that $|B_0| \leq |G(B_0)|$ for every finite $B_0 \subset B$, then M has a solution.*

Our goal is to analyze theorems on necessary and sufficient conditions for marriage problems to have unique solutions. A marriage problem with a single boy has a unique solution if and only if he knows exactly one girl. The following lemma shows that any finite marriage problem with a unique solution must contain such a boy.

Lemma 4. (RCA_0) *If $M = (B, G, R)$ is a finite marriage problem with a unique solution f, then some boy knows exactly one girl.*

Proof. Suppose we have M and f as above with $|B| = n$. Note that $|G_M(B)| = n$, since if $|G_M(B)| > n$ we could construct a new solution to M using a girl not in the range of f, contradicting the uniqueness of f.

Let s be the smallest number such that there is a $B_0 \subset B$ with $|B_0| = |G_M(B_0)| = s$. We know such an s exists by the Σ^0_0 least element principle, a consequence of Σ^0_1 induction. If $s = 1$ then we have proved the lemma. Suppose by way of contradiction that $s > 1$ and choose $b_0 \in B_0$. Since $s > 1$, $|G_M(b_0)| > 1$, so we may choose $g_1 \in G_M(b_0)$ such that $f(b_0) \neq g_1$. Consider $M' = (B_0 - \{b_0\}, G_M(B_0) - \{g_1\}, R')$ where R' is the restriction of R to the sets of M'. We claim that M' has no solution. To see this, let h be a solution of M′ and note that $h \cup (b_0, g_1)$ is a matching of $(B_0, G_M(B_0))$ distinct from f. Since $|B_0| = |G_M(B_0)|$, f matches boys not in B_0 to girls not in $G_M(B_0)$, so we may define

$$f'(b) = \begin{cases} g_1 & \text{if } b = b_0 \\ h(b) & \text{if } b \in B_0 - \{b_0\} \\ f(b) & \text{otherwise.} \end{cases}$$

This f' is a solution of M differing from f at b_0, contradicting the uniqueness of f. Thus M' has no solution. Apply Theorem 1 and find a set of boys $B_1 \subset B_0 - \{b_0\}$ who know too few girls, that is, $|B_1| > |G_{M'}(B_1)|$. Since f is a solution of M, $|B_1| \leq |G_{M'}(B_1) \cup \{g_1\}|$ so $|B_1| = |G_{M'}(B_1) \cup \{g_1\}| = |G_M(B_1)|$. However, $|B_1| < |B_0|$, contradicting the minimality of s. Therefore $s > 1$ cannot hold, completing the proof of the lemma. □

Now we can formulate a theorem on unique solutions to finite marriage problems. Clearly, if we can line up the boys $b_1, b_2, \ldots, b_n$ so that for each $m \leq n$ the first m boys know exactly m girls, then the marriage problem has a unique solution. This implication is provable in RCA_0, as is its extension to infinite marriage problems. The following

theorem shows that the converse for finite problems is provable in RCA_0. As noted by Chang [2], the combinatorial statement in the theorem is implicit in the work of Marshall Hall, Jr. [7].

Theorem 5. (RCA_0) *If $M = (B, G, R)$ is a finite marriage problem with n boys and a unique solution, then there is an enumeration of the boys $\langle b_i \rangle_{i \leq n}$ such that $|G(b_1, \ldots, b_m)|$ for every $1 \leq m \leq n$.*

Proof. Suppose M is as above. Working in RCA_0, we will construct a sequence of initial segments of $\langle b_i \rangle_{i \leq n}$. Apply Lemma 4 and let b_1 be the first boy (in some enumeration of B) such that $|G(b_1)| = 1$. Suppose that $t < n$, $\langle b_i \rangle_{i \leq t}$ is defined, and $|G(b_1, \ldots, b_t)| = t$. Since M has a unique solution, so does $M' = (B - \{b_1, \ldots b_t\}, G - G(b_1, \ldots, b_t), R')$, where R' is the restriction of R to the sets of M'. Apply Lemma 4 and let b_{t+1} be the first boy not in $\{b_1, \ldots, b_t\}$ such that $|G_{M'}(b_{t+1})| = 1$, completing the definition of $\langle b_i \rangle_{i \leq t+1}$. The desired enumeration is the n^{th} initial segment. □

In light of the comments preceding Theorem 5, it could be reformulated as a biconditional statement, giving a necessary and sufficient condition for the existence of unique solutions to finite marriage problems. The same reformulation could be carried out for Theorems 7 and 9 below. Now we will analyze a version of Theorem 5 in the infinite setting, using ACA_0 in its proof. Paralleling the proof of Theorem 5, we begin with a lemma.

Lemma 6. (ACA_0) *Suppose $M = (B, G, R)$ is a marriage problem such that every boy knows finitely many girls and M has a unique solution. For any $b \in B$ there is a finite set F such that $b \in F \subset B$ and $|G(F)| = |F|$.*

Proof. Suppose f is the unique solution of $M = (B, G, R)$. Let $b \in B$. If $|G(b)| = 1$, the set $F = \{b\}$ satisfies the conclusion of the lemma. If $|G(b)| > 1$, a more complicated construction is required.

Assume $|G(b)| > 1$ and let $g_0 = f(b)$ and $G(b) = \{g_0, g_1, \ldots, g_m\}$. Consider the marriage problem $M_1 = (B - \{b\}, G - \{g_1\}, R_1)$ where R_1 denotes the restriction of R to the sets of M_1. Given a solution f_1 of M_1, the function $f_1 \cup (b, g_1)$ would be a solution of M distinct from f. Thus M_1 has no solution. Using ACA_0, we may apply Theorem 2 and find a finite collection of boys $E_1 \subset B - \{b\}$ such that $|E_1| > |G_{M_1}(E_1)|$. Thus $|E_1| \geq |G_{M_1}(E_1) \cup \{g_1\}|$ and since $G_{M_1}(E_1) \cup \{g_1\} = G_M(E_1)$, we have $|E_1| \geq |G_M(E_1)|$. Since M has a solution, $|E_1| \leq |G_M(E_1)|$, so combining inequalities shows that $|E_1| = |G_M(E_1)|$. For each i with $1 < i \leq m$ and each $g_i \in G(b)$ search for a similar finite set, finding an $E_i \subset B$ with $|G(E_i)| = |E_i|$ and $g_i \in G(E_i)$. Since each E_i is a finite set with an integer code, recursive comprehension suffices to prove the existence of the sequence $E_1, E_2, \ldots, E_m$ and the union $F = \{b\} \cup_{i \leq m} E_i$. Since each E_i is finite, F is finite and $b \in F \subset B$.

To complete the proof, we need only show that $|F| = |G(F)|$. Suppose by way of contradiction that $|G(F)| > |F|$. In this case, since f maps F into but not onto

$G(F)$, we can choose $g \in G(F)$ such that for every $c \in F$, $f(c) \neq g$. Since $f(b) = g_0$, $g \neq g_0$. If $g \in G(b)$, then for some $i \geq 1$ we have $g = g_i$ and $g \in G(E_i)$. Since $G(F) = G(b) \cup \bigcup_{i \leq m} G(E_i)$, we may fix an i such that $g \in G(E_i)$. Since $|E_i| = |G(E_i)|$, f must map E_i onto $G(E_i)$, so for some $c \in E_i$, $f(c) = g$. This contradicts our choice of g, showing that $|G(F)| \leq |F|$. Since f is an injection of F into $G(F)$, we must have $|F| = |G(F)|$. □

Note that the only use of ACA_0 in the preceding proof is the application of Theorem 2. This will be useful in adapting our results to the bounded marriage theorem setting.

Now we can analyze the extension of Theorem 5 to infinite marriage problems. Like the result of Marshall Hall, Jr. analyzed in Theorem 2, this statement is equivalent to ACA_0.

Theorem 7. (RCA_0) *The following are equivalent:*

1. ACA_0.
2. *Suppose $M = (B, G, R)$ is a marriage problem such that every boy knows finitely many girls. If M has a unique solution then there is an enumeration of the boys $\langle b_i \rangle_{i \geq 1}$ such that $|G(b_1, \ldots, b_n)| = n$ for every $n \geq 1$.*

Proof. To prove that (1) implies (2), we will work in RCA_0, making each application of ACA_0 explicit. Let $M = (B, G, R)$ be a marriage problem as described in (2). Let $\langle b'_i \rangle_{i \geq 1}$ be an arbitrary initial enumeration of B. Search for a finite set $F_1 \subset B$ such that $b'_1 \in F_1$ and $|G_M(F_1)| = |F_1|$. Define $n_1 = |F_1|$. By Lemma 6, this search must succeed. Note that ACA_0 is used here in the application of Lemma 6 and to determine the value of $|G_M(F_1)|$. We claim that f restricted to F_1 is a unique solution of $(F_1, G(F_1), R)$. To see this, suppose f' is a solution of $(F_1, G(F_1), R)$ differing from f. Since f is injective and maps F_1 onto $G(F_1)$, f must map $B - F_1$ into $G - G(F_1)$, Thus the extension of f' defined by

$$f'(b) = \begin{cases} f'(b) & \text{if } \ b \in F_1 \\ f(b) & \text{if } b \in B - F_1 \end{cases}$$

is a solution of M differing from f, contradicting the uniqueness of f. Since $(F_1, G(F_1), R)$ has a unique solution, by Theorem 5, there is an enumeration of the boys $\langle b^1_1, b^1_2, \ldots, b^1_{n_1} \rangle$ of F_1 such that $|G(b^1_1, b^1_2, \ldots, b^1_m)| = m$ for every m with $1 \leq m \leq n_1$.

Suppose $F_1, \ldots, F_j$ are sequences that have been constructed so that for each $i \leq j$ and each $t \leq n_i$, $F_i = \langle b^i_1, b^i_2, \ldots, b^i_{n_i} \rangle$ and

$$|G(\{b^i_1, b^i_2, \ldots, b^i_t\} \cup \bigcup_{k<i} F_k)| = t + \sum_{k<i} n_k.$$

Note that f restricted to $B - \cup_{k \leq j} F_j$ is a unique solution of the marriage problem $M_{j+1} = (B - \cup_{k \leq j} F_k, G - \cup_{k \leq j} G(F_k), R)$. Let b' denote the first element (in our initial enumeration of B) appearing in $B - \cup_{k \leq j} F_k$. Search for a finite set $F_{j+1} \subset B - \cup_{k \leq j} F_k$

such that $b' \in F_{j+1}$ and $|G_{M_{j+1}}(F_{j+1})| = |F_{j+1}|$. Define $n_{j+1} = |F_{j+1}|$. As before, Lemma 6 insures that the search will succeed. ACA_0 is applied here in the use of Lemma 6 and in determining values of $|G_{M_{j+1}}(F_{j+1})|$. As before, f restricted to F_{j+1} is a unique solution of M_{j+1} restricted to F_{j+1}, so by Theorem 5 there is an enumeration of the boys $\langle b_1^{j+1}, b_2^{j+1}, \ldots, b_{n_{j+1}}^{j+1} \rangle$ in F_{j+1} such that $G_{M_{j+1}}(b_1^{j+1}, \ldots, b_t^{j+1})|$ for every t with $1 \leq t \leq n_{j+1}$. Consequently, for every $1 \leq t \leq n_{j+1}$,

$$|G(\{b_1^{j+1}, b_2^{j+1}, \ldots, b_t^{j+1}\} \cup \bigcup_{k \leq j} F_k)| = t + \sum_{k \leq j} n_k.$$

Given the existence of each finite sequence F_j, recursive comprehension suffices to prove the existence of the concatenation of the finite sequences $\langle \langle b_1^j, \ldots, b_{n_j}^j \rangle \mid j \geq 1 \rangle$, and this sequence satisfies the conclusion of item (2) in the statement of the theorem.

To prove that (2) implies (1), we will work in RCA_0 and assume (2). By Lemma III.1.3 of Simpson [18], it suffices to use (2) to prove the existence of the range of an arbitrary injection. Let $f : \mathbb{N} \to \mathbb{N}$ be an injection. Using recursive comprehension, construct the marriage problem $M = (B, G, R)$ with

- $B = \{c_n \mid n \in \mathbb{N}\} \cup \{d_n \mid n \in \mathbb{N}\}$,
- $G = \{g_n \mid n \in \mathbb{N}\} \cup \{r_n \mid n \in \mathbb{N}\}$,
- for every i, $(c_i, g_i) \in R$ and $(d_i, r_i) \in R$, and
- if $f(m) = n$ then $(c_n, r_m) \in R$.

Let $h : B \to G$ such that $h(d_i) = r_i$ and $h(c_i) = g_i$ for each $i \in \mathbb{N}$. Clearly, h is injective and a solution to M. Note that any solution must match each d_i with r_i, thus no c_i can be matched to a r_i and so every c_i must be matched with g_i. Hence, h is a unique solution to M.

Apply item (2) and let $\langle b_i \rangle_{i \geq 1}$ be an enumeration of B such that for every $n \geq 1$ we have $|G(b_1, \ldots, b_n)| = n$. Suppose $f(j) = k$. Then $(c_k, r_j) \in R$ and $G(c_k) = \{g_k, r_j\}$. Since $c_k \in B$, for some n we have $c_k = b_n$. If $d_j \notin \{b_1, \ldots, b_{n-1}\}$ then for each $i \leq n-1$, $G(b_i) \cap G(c_k) = \varnothing$. In this case,

$$|G(b_1, \ldots, b_n)| = |G(b_1, \ldots, b_{n-1})| + |G(c_k)| = (n-1) + 2 = n + 1,$$

contradicting $|G(b_1, \ldots, b_n)| = n$. Summarizing, whenever $f(j) = k$, d_j must appear before c_k in the enumeration of the boys. Thus k is in the range of f if and only if for some b appearing before c_k in the enumeration, $b = d_j$ and $f(j) = k$. Since we need only check finitely many values of f to see if k is in the range, recursive comprehension proves the existence of the range of f, completing the proof of the theorem. □

Like Theorem 5, the preceding theorem continues to hold if the implication in item (2) is changed to a biconditional. While such a formulation provides a complete characterization of the marriage problems with unique solutions, it weakens the statement of the reversal.

As noted in the introduction, bounded marriage problems are often weaker than their unbounded versions. This is also true for the following bounded analogs of Lemma 6 and Theorem 7, as shown by the next two results.

Lemma 8. (WKL_0) *Suppose $M = (B, G, R)$ is a bounded marriage problem and M has a unique solution. For any $b \in B$ there is a finite set F such that $b \in F \subset B$ and $|G(F)| = |F|$.*

Proof. Proceed exactly as in the proof of Lemma 6, replacing each application of Theorem 2 with an application of Theorem 3. □

Theorem 9. (RCA_0) *The following are equivalent:*

1. WKL_0.
2. *Suppose $M = (B, G, R)$ is a bounded marriage problem. If M has a unique solution then there is an enumeration of the boys $\langle b_i \rangle_{i \geq 1}$ such that $|G(b_1, \ldots, b_n)| = n$ for every $n \geq 1$.*

Proof. To prove that (1) implies (2), repeat the corresponding portion of the proof of Theorem 7, replacing uses of ACA_0 with uses of WKL_0 as follows. First, substitute Lemma 8 for Lemma 6 everywhere. Note that the bounding function for M also acts as a bounding function for any marriage problem created by deleting sets of boys and girls from M. Consequently, we may use the bounding function and recursive comprehension to compute $G(F)$ for each finite set F whenever required.

The reversal requires a completely new argument. We will use (2) to prove that any binary tree (with nodes labeled 0 or 1) with no infinite paths is finite. Toward this end, suppose T is a binary tree with no infinite paths. As in section III.7 of Simpson [18], we can identify each node of T with a binary sequence, $\sigma \in 2^{<\mathbb{N}}$. Construct the marriage problem $M = (B, G, R)$ by letting $B = \{b_\sigma \mid \sigma \in T\}$, $G = \{g_\sigma \mid \sigma \in T\}$, and

$$R = \{(b_\sigma, g_\sigma) \mid \sigma \in T\} \cup \{(b_\sigma, g_{\sigma^\frown i}) \mid \sigma \in T \wedge \sigma^\frown i \in T\}.$$

Note that since $G(b_\sigma) = \{g_\sigma, g_{\sigma^\frown 0}, g_{\sigma^\frown 1}\} \cap G$ for all σ, M is a bounded marriage problem.

Define $f : B \to G$ by $f(b_\sigma) = g_\sigma$. We claim that f is a unique solution of M. To verify this let f_1 be a second solution of M where $f_1(b_\sigma) = g_{\sigma^\frown i}$ for some $i \in \{0, 1\}$. Fix such a σ and i and let $\sigma_0 = \sigma$. Given σ_n let $\sigma_{n+1} = \tau$ where $f_1(b_{\sigma_n}) = g_\tau$. Since f_1 is injective, an easy induction argument shows that σ_{n+1} must always be an extension of σ_n. Hence, $\langle \sigma_n \mid n \in \mathbb{N} \rangle$ forms an infinite path through T, yielding a contradiction. Thus f is unique.

Since M has a unique solution, we can apply item (2) to M and enumerate the boys $\langle b_i \rangle_{i \geq 1}$ so that $|G(b_1, \ldots, b_n)| = n$ for all n. Recursive comprehension proves the existence of translation functions between the two types of subscripting on the boys. Let $r : T \to \mathbb{N}$ be the bijection defined by $r(\sigma) = n$ if and only if $b_n = b_\sigma$.

We claim that each boy appears in the enumeration after all of his proper successors in the tree. Using $\sigma \prec \tau$ to denote that σ is a proper initial segment of τ, our claim

becomes: if $\sigma \prec \tau \in T$, then $r(\sigma) > r(\tau)$. To prove this, suppose by way of contradiction that for some $\sigma \prec \tau \in T$, $r(\sigma) < r(\tau)$. By the Σ^0_0 least element principle (a consequence of Σ^0_1 induction) we can fix a shortest sequence τ such that $r(\sigma) < r(\tau)$ for some $\sigma \prec \tau$. Because τ is shortest, there is no α such that $r(\alpha) > r(\tau)$ and $\sigma \prec \alpha \prec \tau$. Thus we may assume that τ is an immediate successor of σ. Summarizing, we have $r(\sigma) < r(\tau)$ and $\tau = \sigma^\frown i$ for some $i \in \{0, 1\}$. Let $B' = \{b_1, b_2, \ldots, b_{r(\sigma)}\}$. Using the node-based indices for the boys, we can write $B' = \{b_\alpha \mid r(\alpha) \leq r(\sigma)\}$. Note that $r(\tau) > r(\sigma)$, so $b_\tau \notin B'$. By the definition of M, $(b_\sigma, g_\tau) \in R$, so $g_\tau \in G(B')$. Also, for every $b_\alpha \in B'$, $(b_\alpha, g_\alpha) \in R$, so $g_\alpha \in G(B')$. Thus $|G(B')| > |B'|$. However, B' is an initial segment of the enumeration of B provided by the application of (2), so $|G(B')| = |B'|$. This contradiction completes the proof that each boy appears in the enumeration after all of his proper successors in the tree.

The empty sequence $\langle\ \rangle$ is in T, so for some n, $b_{\langle\ \rangle} = b_n$ Since b_n appears after every boy corresponding to a nonempty node of T, we know T is finite, completing the proof of the reversal and the theorem. □

At this time, we have been unable to determine the exact strength of some of the lemmas in the preceding material. For example, although we know that Lemma 6 is provable in ACA_0, we do not know if it can be proved in a weaker subsystem. Consider the following formulation of an infinite version of Lemma 4: If M is a marriage problem in which each boy knows only finitely many girls and M has a unique solution, then some boy knows exactly one girl. Lemma 6 and Lemma 4 give a proof in ACA_0, but the following theorem shows that at most WKL_0 is required.

Theorem 10. (WKL_0) *Suppose M is a marriage problem in which every boy knows at least two girls and at most finitely many girls. If M has a solution, then M has at least two solutions.*

Proof. Assume WKL_0. Let $M = (B, G, R)$ be a marriage problem with solution $f : B \to G$ and suppose that every boy knows at least two girls. Define a function $h_0 : B \to G$ by letting $h_0(b)$ be the first girl other than $f(b)$ that b knows. Formally, $h_0(b) = \mu g((b, g) \in R \wedge f(b) \neq g)$. Define $h_1 : B \to G$ by $h_1(b) = \max\{h_0(b), f(b)\}$ and let $R' = \{(b, g) \mid f(b) = g \vee h_0(b) = g\}$. Recursive comprehension proves the existence of h_0, h_1, and R'. The society $M' = (B, G, R')$ is bounded by h_1 and has f as a solution. Every boy in M' knows exactly two girls. By Theorem 9, if f is a unique solution of M', then some boy in B knows exactly one girl, contradicting the construction of M'. Consequently, M' has at least two solutions. Since every solution of M' is also a solution M, M also has at least two solutions. □

Bibliography

[1] Errett Bishop and Douglas Bridges, *Constructive analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 279, Springer-Verlag, Berlin, 1985. MR804042 (87d:03172)

[2] Gerard J. Chang, *On the number of SDR of a (t, n)-family*, European J. Combin. **10** (1989), no. 3, 231–234. DOI 10.1016/S0195-6698(89)80056-3. MR1029168 (90j:05010)

[3] David S. Dummit and Richard M. Foote, *Abstract algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991. MR1138725 (92k:00007)

[4] A. Fraenkel, *Der Begriff "definit" und die Unabhängigkeit des Auswahlsaxioms*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse (1922), 253–257. Translated in [`?inf:heij`] 284–289.

[5] Harvey Friedman, *Some systems of second order arithmetic and their use*, Proceedings of the International Congress of Mathematicians (Vancouver, B. C., 1974), Canad. Math. Congress, Montreal, Que., 1975, pp. 235–242.

[6] Harvey M. Friedman, *Systems of second order arithmetic with restricted induction, I, II* (abstracts), J. Symbolic Logic **41** (1976), no. 2, 557–559.

[7] Marshall Hall Jr., *Distinct representatives of subsets*, Bull. Amer. Math. Soc. **54** (1948), 922–926. DOI 10.1090/S0002-9904-1948-09098-X. MR0027033 (10,238g)

[8] Philip Hall, *On representatives of subsets*, J. London Math. Soc. **10** (1935), 26–30. DOI 10.1112/jlms/s1-10.37.26.

[9] A. G. Hamilton, *Logic for mathematicians*, 2nd ed., Cambridge University Press, Cambridge, 1988. MR958520 (89e:03002)

[10] David Hilbert and Paul Bernays, *Grundlagen der Mathematik. I*, Die Grundlehren der mathematischen Wissenschaften, vol. 40, Springer-Verlag, Berlin, New York, 1934.

[11] ———, *Grundlagen der Mathematik. II*, Die Grundlehren der mathematischen Wissenschaften, vol. 50, Springer-Verlag, Berlin, New York, 1939.

[12] Denis R. Hirschfeldt and Richard A. Shore, *Combinatorial principles weaker than Ramsey's theorem for pairs*, J. Symbolic Logic **72** (2007), no. 1, 171–206, DOI 10.2178/jsl/1174668391. MR2298478 (2007m:03115)

[13] Jeffry L. Hirst, *Combinatorics in Subsystems of Second Order Arithmetic*, ProQuest LLC, Ann Arbor, MI, 1987. Thesis (Ph.D.)–The Pennsylvania State University. MR2635978

[14] ———, *Marriage theorems and reverse mathematics*, Logic and computation (Pittsburgh, PA, 1987), Contemp. Math., vol. 106, Amer. Math. Soc., Providence, RI, 1990, pp. 181–196. DOI 10.1090/conm/106/1057822. MR1057822 (91k:03141)

[15] Carl G. Jockusch Jr., *Ramsey's theorem and recursion theory*, J. Symbolic Logic **37** (1972), 268–280. MR0376319 (51 #12495)

[16] Jiayi Liu, RT^2_2 *does not imply* WKL_0, J. Symbolic Logic **77** (2012), no. 2, 609–620, DOI 10.2178/jsl/1333566640. MR2963024

[17] David Seetapun and Theodore A. Slaman, *On the strength of Ramsey's theorem*, Notre Dame J. Formal Logic **36** (1995), no. 4, 570–582, DOI 10.1305/ndjfl/1040136917. Special Issue: Models of arithmetic. MR1368468 (96k:03136)

[18] Stephen G. Simpson, *Subsystems of second order arithmetic*, 2nd ed., Perspectives in Logic, Cambridge University Press, Cambridge, 2009. DOI 10.1017/CBO9780511581007. MR2517689 (2010e:03073)

[19] ———, *Which set existence axioms are needed to prove the Cauchy/Peano theorem for ordinary differential equations?*, J. Symbolic Logic **49** (1984), no. 3, 783–802, DOI 10.2307/2274131. MR758929 (86a:03066)

[20] Ernst Specker, *Typical ambiguity*, Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.), Stanford Univ. Press, Stanford, Calif., 1962, pp. 116–124. MR0157901 (28 #1129)

[21] E. Zermelo, *Untersuchungen über die Grundlagen der Mengenlehre I*, Math. Ann. **65** (1908), no. 2, 261–281. Translated in [`?inf:heij`], 199-215.