

INTRODUCTION

CONCRETE MATHEMATICAL INCOMPLETENESS

- 0.1. General Incompleteness.
- 0.2. Some Basic Completeness.
- 0.3. Abstract and Concrete Mathematical Incompleteness.
- 0.4. Reverse Mathematics.
- 0.5. Incompleteness in Exponential Function Arithmetic.
- 0.6. Incompleteness in Primitive Recursive Arithmetic, Single Quantifier Arithmetic, RCA_0 , and WKL_0 .
- 0.7. Incompleteness in Nested Multiply Recursive Arithmetic, and Two Quantifier Arithmetic.
- 0.8. Incompleteness in Peano Arithmetic and ACA_0 .
- 0.9. Incompleteness in Predicative Analysis and ATR_0 .
- 0.10. Incompleteness in Iterated Inductive Definitions and $\Pi_1^1-CA_0$.
- 0.11. Incompleteness in Second Order Arithmetic and $ZFC \setminus P$.
- 0.12. Incompleteness in Russell Type Theory and Zermelo Set Theory.
- 0.13. Incompleteness in ZFC using Borel Functions.
- 0.14. Incompleteness in ZFC using Discrete Structures.
- 0.15. Detailed overview of book contents.
- 0.16. Some Open problems.
- 0.17. Concreteness in the Hilbert Problem List.

This Introduction sets the stage for the new advances in Concrete Mathematical Incompleteness presented in this book.

The remainder of this book can be read without relying on this Introduction. However, we advise the reader to peruse this Introduction in order to gain familiarity with the larger context.

Readers can proceed immediately to the overview of the contents of the book by first reading the brief account in section 0.14C, and then the fully detailed overview in section 0.15. These are self contained and do not rely on the rest of the Introduction.

In this Introduction, we give a general overview of what is known concerning Incompleteness, with particular emphasis on Concrete Mathematical Incompleteness. The emphasis will be on the discussion of examples of concrete mathematical theorems - in the sense discussed in section 0.3 - which can be proved only by using unexpectedly strong axioms.

The incompleteness phenomenon, in the sense understood today, was initiated by Kurt Gödel with his first incompleteness theorem, where he essentially established that there are sentences which cannot be proved or refuted using the usual axioms and rules of inference for mathematics, ZFC (assuming ZFC is free of contradiction). See [Go31], and [Go86-03], volume 1.

Gödel also established in [Go31] that this gap is not repairable, in the sense that if ZFC is extended by finitely many new axioms (or axiom schemes), then the same gap remains (assuming the extended system is free of contradiction).

With his second incompleteness theorem, Gödel gave a critical example of this incompleteness. He showed that the statement

$$\text{Con}(\text{ZFC}) = \text{"ZFC is free of contradiction"}$$

is neither provable nor refutable in ZFC (assuming ZFC is legitimate in the sense that it proves only true statements in the ring of integers). Again, see [Go31], and [Go86-03], volume 1.

Although $\text{Con}(\text{ZFC})$ is a natural statement concerning the axiomatization of abstract set theory, it does not represent a natural statement in the standard subject matter of mathematics.

While it is true that $\text{Con}(\text{ZFC})$ can be stated entirely in terms of finite strings of symbols from a finite alphabet, when stated in this way, it is no longer natural in any mathematical sense.

These considerations led to the informal working distinction between "mathematically natural" and "metamathematically natural".

After the two incompleteness theorems, there remained the crucial question of whether there is a mathematically natural statement which is neither provable nor refutable in ZFC.

This question had a potentially practical consequence. If the answer is no, then there is a clear sense in which mathematicians can forever be content to ignore the incompleteness phenomenon. However, if the answer is yes,

then there is a clear sense in which the incompleteness phenomenon can impact their work.

Gödel addressed this question through his pioneering work on Cantor's Continuum Hypothesis (CH). CH states that every infinite set of real numbers is in one-one correspondence with either the integers or the real numbers.

Gödel proved that ZFC does not suffice to refute CH. See [Go38], and [Go86-03], volume 2. That ZFC does not suffice to prove CH had to wait for the pioneering work of Paul J. Cohen, [Co63,64]. Also see [Je78,06].

Thus by the mid 1960s, a mathematically natural statement - the continuum hypothesis - was shown to be neither provable nor refutable in ZFC. Mathematical Incompleteness from ZFC was born.

Yet mathematicians generally did not feel that CH was relevant to their work. This feeling of irrelevance went much deeper than just their particular research interests.

There is a fundamental alienation of "questions like CH" from mathematical culture. Specifically, CH fundamentally involves a level and kind of generality that is entirely uncharacteristic of important and fruitful mathematical questions.

Mathematicians will normally use general abstract machinery - when convenient - in the course of treating a relatively concrete problem. Witness the extensive use of general abstract machinery in Wiles' proof of Fermat's Last Theorem, and how much of this machinery can be removed (see [Mc10]).

The general abstract machinery will be tamed if it causes its own difficulties or ceases to be convenient for various reasons. But the standards for objects of primary investigation of major interest are quite different.

Sets of real numbers that play a role in mathematics as objects of primary investigation, are constructed in some fashion that is related to clear mathematical purposes. In virtually all cases, sets of real numbers appearing as objects of primary investigation, are Borel measurable (i.e., lie in the σ sigma generated by the open sets), and usually very low in the standard hierarchy of Borel measurable sets.

For Borel measurable sets of real numbers, the continuum hypothesis is a theorem, even in the following strong form:

every infinite Borel measurable set of reals is in one-one correspondence with the integers, or in Borel one-one correspondence with the reals.

See [Al16], [Hau16], and [Ke94], p. 83.

This situation is typical of so many statements involving sets and functions in complete separable metric spaces. The Borel measurable forms are theorems, and have nothing to do with incompleteness.

Furthermore, the great generality present in so many such statements is rather empty from the point of view of mathematical culture: there are virtually no mathematically interesting examples beyond Borel sets.

There have been subsequent examples of ZFC incompleteness of less generality than arbitrary sets of reals. Most notably, involving the projective hierarchy of sets of reals, which is obtained by starting with Borel sets in several dimensions, and applying the operations of projection and complementation.

Yet again, we see that the statements are decided in ZFC for Borel sets, and there are virtually no mathematically interesting examples that come under this generality beyond Borel sets.

We take the view that Concrete Mathematical Incompleteness begins at the level of Borel measurable sets and functions on complete separable metric spaces. In section 0.3, we refine this to

Mathematical statements concerning Borel measurable sets and functions of finite rank in and between complete separable metric spaces.

We take the position that once we are discussing possibly very discontinuous functions between complete separable metric spaces, the Borel sets and functions of finite rank are not overly general - there are sufficient mathematically interesting examples of such reaching out to at least the first few finite levels.

In sections 0.11 - 0.13, incompleteness ranging from fragments of ZFC through ZFC and more are discussed in the setting of finite rank Borel sets and functions. In most cases, the incompleteness already starts kicking in at the first few finite ranks of the Borel hierarchy.

However, Borel measurable sets and functions in complete separable metric spaces - even of low finite rank - is still substantially beyond what is considered normal for significant mathematical questions in the present mathematical culture.

Incompleteness begins to become potentially noticeable when the examples live in discrete structures. Here by discrete structures, we mean finitely generated systems such as the ordered ring of integers, and the ordered field of rationals. We work with sets in and functions between discrete structures.

Examples of incompleteness ranging from fragments of ZFC, to ZFC and beyond, are discussed in sections 0.5 - 0.10, and section 0.14.

Boolean Relation Theory, the subject of this book, involves sets in and functions on the nonnegative integers. There is a brief account in section 0.14, and a detailed account in section 0.15.

Some new developments that push Concrete Mathematical Incompleteness even further into the more immediately accessible and perfectly natural, are presented in section 0.14 without proof. The relevant manuscripts are under preparation.

This Introduction concludes with a discussion of Concreteness in the realm of the Hilbert 1900 Problem List. This illustrates how the usual classification of mathematical statements used in mathematical logic (see the four displayed lists in section 0.3) relates to many contexts in core mathematics.

The reader of this Introduction will see rather explicitly how the use of stronger and stronger fragments of ZFC, all the way through ZFC and extensions thereof by so called large cardinal hypotheses, supports proofs of more and more mathematically natural concrete statements.

In other words, this growing body of results shows rather explicitly what is to be gained by strengthening axiom systems for mathematics.

Of course, there is an even greater loss realized by strengthening a consistent axiom system to an inconsistent one. The issue of why we believe, or why we should believe, that the relevant axiom systems used in this book are consistent - or, more strongly, that they prove only true arithmetic sentences - is an important one, but lies beyond the scope of this book.

Since this Introduction is to be viewed as clarifying background material for the six Chapters, many of the proofs are briefly sketched. We also include folklore, results that can be easily gleaned from the literature, and results, without proof, that we intend to publish elsewhere. We provide an adequate, but by no means complete, list of references.

We close these introductory remarks with a topic for specialists.

We use the system EFA (exponential function arithmetic) as a base theory for most of the arithmetical claims. Sometimes SEFA (superexponential function arithmetic) is needed. EFA and SEFA are already presented and used in section 0.1 for a different purpose.

A typical situation is the conservativity of $I\Sigma_1$ (one quantifier induction) over PRA (primitive recursive arithmetic). Perhaps the simplest proof of this result is by a very natural model theoretic argument (see, e.g., [Si99,09], Theorem IX.3.16). SEFA arises because of the need for cut elimination (to which it is equivalent over EFA). Model theoretic proofs in such contexts are often simpler and well known, but cannot be formalized as given in SEFA, or in even stronger systems. A general method for augmenting the model theoretic arguments with additional ideas to get proofs in SEFA is given in [Fr99c]. Proof theoretic approaches to these results and many other such results are known, and originated much earlier. E.g., see [Min73], [Pa70], and [Tak90]. Careful formalizations of these proof theoretic arguments, here and in many other contexts, can also be made in SEFA.

0.1. General Incompleteness.

General Incompleteness was initiated by Gödel's landmark First and Second Incompleteness Theorems, which apply to very general formal systems. The original reference is [Go31].

Throughout this Introduction, we will use the following setup for logic.

MSL (many sorted logic) is many sorted first order predicate calculus with equality. Here we have countably many sorts, countably infinitely many sorted constant, relation, and function symbols, and equality in each sort.

Let T be a set of formulas in MSL. $L(T)$ is the language of T , which consists of the sorts and symbols that appear in T . In particular, $L(T)$ may not have equality in all of the sorts that appear in T .

We say that φ is provable in T (provable from T , T implies φ), if and only if φ is a formula in $L(T)$ which is provable from (the universal closures of elements of) T using the usual Hilbert style axioms and rules of inference for $L(T)$. By the Gödel Completeness Theorem, this is the same as: T semantically implies φ .

0.1A. Gödel's First Incompleteness Theorem.

0.1B. Two Roles of Gödel's Second Incompleteness Theorem.

0.1C. Sufficiency Property for Formalized Consistency.

0.1D. Gödel's Second Incompleteness Theorem for Arithmetized Consistency.

0.1E. Gödel's Second Incompleteness Theorem for Sequential Consistency.

0.1F. Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability.

0.1G. Gödel's Incompleteness Theorems and Interpretability.

0.1A. Gödel's First Incompleteness Theorem.

The powerful recursion theoretic approach to Gödel's First Incompleteness Theorem first appears in [Ro52] and [TMR53], through the use of the formal system Q .

Q is a set of formulas in one sort and $0, S, +, \cdot, \leq, =$. It consists of the following eight formulas.

1. $Sx \neq 0$.
2. $Sx = Sy \rightarrow x = y$.
3. $x \neq 0 \rightarrow (\exists y)(x = Sy)$.

4. $x + 0 = x$.
5. $x + Sy = S(x + y)$.
6. $x \cdot 0 = 0$.
7. $x \cdot Sy = (x \cdot y) + x$.
8. $x \leq y \leftrightarrow (\exists z)(z + x = y)$.

The last axiom is purely definitional. An alternative is to discard axiom 8 and remove \leq from the language. However, use of \leq facilitates the statement of the following theorem.

A bounded formula in $L(Q)$ is a formula in $L(Q)$ whose quantifiers are bounded, in the following way.

$$(\forall n \leq t)$$

$$(\exists n \leq t)$$

where t is a term in $L(Q)$ in which n does not appear.

A Π_1^0 (Σ_1^0) formula in $L(Q)$ is a formula in $L(Q)$ that begins with zero or more universal (existential) quantifiers, followed by a bounded formula.

The following is well known and easy to prove.

THEOREM 0.1A.1. A Σ_1^0 sentence in $L(Q)$ is true if and only if it is provable in Q . Let T be a consistent extension of Q in MSL. Every Π_1^0 sentence in $L(Q)$ that is provable in T , is true. (Note that the second part follows from the first).

THEOREM 0.1A.2. Let T be a consistent extension of Q in MSL. The set of all Π_1^0 sentences in $L(Q)$ that are i) provable in T , ii) refutable in T , iii) provable or refutable in T , is not recursive.

Proof: This appears in [Ro52] and [TMR53]. It is proved using the construction of recursively inseparable recursively enumerable sets; e.g., $\{n: \varphi_n(n) = 0\}$ and $\{n: \varphi_n(n) = 1\}$. QED

We can obtain the following strong form of Gödel's First Incompleteness Theorem as an immediate corollary.

THEOREM 0.1A.3. Gödel's First Incompleteness Theorem for Extensions of Q (strong Gödel-Rosser form in [Ross36]). Let T be a consistent recursively enumerable extension of Q in MSL. There is a true Π_1^0 sentence in $L(Q)$ that is neither provable nor refutable in T .

Proof: By Theorem 0.1A.1, we can, without loss of generality, remove "true". If this is false, we obtain a decision procedure for the Π_1^0 sentences in $L(Q)$ that are provable in T , by searching for proofs in T . This contradicts Theorem 0.1A.2. QED

We can use the negative solution to Hilbert's Tenth Problem in order to obtain other forms of Gödel's First Incompleteness Theorem that are stronger in certain respects, such as Theorem 0.1A.4.

Hilbert's 10th problem asks for a decision procedure for determining whether a given polynomial with integer coefficients in several integer variables has a zero.

The problem was solved negatively in 1970 by Y. Matiyasevich, building heavily on earlier work of J. Robinson, M. Davis, and H. Putnam. In its strong form, the MRDP theorem (in reverse historical order) asserts that every r.e. subset of N^k is Diophantine, in the sense that it is of the form

$$\{x \in N^k: (\exists y \in N^r) (P(x, y) = 0)\}$$

where r, P depend only on k , and P is a polynomial of $k+r$ variables with integer coefficients. (There are stronger forms of this theorem, where r is an absolute number, and involving only one polynomial P). See [Da73], [Mat93].

The MRDP theorem has been shown to be provable in a certain weak fragment of arithmetic which we call EFA = exponential function arithmetic. See section 0.5 for the axioms of EFA. The proof of MRDP in EFA appears in [DG82].

A Diophantine sentence in $L(Q)$ is a sentence in $L(Q)$ of the form

$$(\forall x_1, \dots, x_n) (s \neq t)$$

where s, t are terms in $L(Q)$. We use the term "Diophantine" because $(\forall x_1, \dots, x_n) (s \neq t)$ expresses the nonexistence in the nonnegative integers of a zero of the polynomial $s-t$.

THEOREM 0.1A.4. Gödel's First Incompleteness Theorem for Diophantine Sentences (using [MRDP], [DG82]). Let T be a consistent recursively enumerable extension of EFA in MSL. There is a Diophantine sentence in $L(Q)$ that is neither

provable nor refutable in T .

Proof: Since EFA proves MRDP, we see that every Π^0_1 sentence in $L(Q)$ is provably equivalent to a Diophantine sentence, over T . Now apply Theorem 0.1A.3. QED

It is not clear whether EFA can be replaced by a weaker system in Theorem 0.1A.4, such as Q . For then the theory T may not prove MRDP.

An important issue is whether there is a "reasonable" Diophantine sentence $(\forall x_1, \dots, x_n)(s \neq t)$ that can be used in Theorem 0.1A.4 for, say, $T = PA$ or $T = ZFC$.

We briefly jump to the use of $PA =$ Peano Arithmetic. The axioms of PA are presented in section 0.5.

Let us call a polynomial P a Gödel polynomial if

- i. P is a polynomial in several variables with integer coefficients.
- ii. The question of whether P has a solution in nonnegative integers is neither provable nor refutable in PA .

We can also use formal systems other than PA here - for example, ZFC . The ZFC axioms are presented in section 0.11.

A truly spectacular possibility is that there might be an "intellectually digestible" Gödel polynomial.

However, we are many many leaps away from being able to address this question. For the present state of the art upper bound on the size of a Gödel polynomial, see [CM07].

One interesting theoretical issue is whether we can establish any relationship between the least "size" of a Gödel polynomial using PA and the least "size" of a Gödel polynomial using ZFC .

0.1B. Two Roles of Gödel's Second Incompleteness Theorem.

Gödel's Second Incompleteness Theorem has played two quite distinct roles in mathematical logic.

Firstly, it is the source of the first intelligible statements that are neither provable nor refutable. E.g., $\text{Con}(PA)$ is neither provable nor refutable in PA , and

$\text{Con}(\text{ZFC})$ is neither provable nor refutable in ZFC. (We use the notation $\text{Con}(T)$ for "T is consistent", or "T is free of contradiction").

Incompleteness from ZFC, involving mathematical statements - in the sense discussed in section 0.3 - came later. Most notably, the continuum hypothesis - a fundamental problem in set theory - was shown to be neither provable nor refutable in ZFC in, respectively, [Co63,64] and [Go38]. The Concrete Mathematical Incompleteness of ZFC came much later - see sections 0.13, 0.14.

Secondly, the Second Incompleteness Theorem is used as a tool for establishing other incompleteness results. In fact, it is used in an essential way here in this book.

Suppose we want to show that ZFC does not prove or refute a statement φ .

i. First we show that φ is provable in an extension T of ZFC that we "trust". In this book, we use an extension of ZFC by a certain large cardinal axiom - strongly Mahlo cardinals of finite order. See section 0.13.

ii. Then we build a model of ZFC using only φ and a fragment K of ZFC. We will assume that K implies EFA, so that K is strong enough to support Gödel's Second Incompleteness Theorem. In this book, we use $K = \text{ACA}'$, a very weak fragment of ZFC, which implies EFA. See Definition 1.4.1.

From i, we have established the consistency of $\text{ZFC} + \varphi$ from the consistency of T.

From ii, we have $\text{ZFC} + \varphi$ proves $\text{Con}(\text{ZFC})$. So if ZFC proves φ , then ZFC proves $\text{Con}(\text{ZFC})$, violating Gödel's Second Incompleteness Theorem (assuming ZFC is consistent).

Note that we have assumed that ZFC is consistent in order to show the unprovability of φ in ZFC. This is necessary, because if ZFC is inconsistent then φ (and every sentence in the language of ZFC) is provable in ZFC.

There is a way of stating the unprovability of φ in a way that does not rely on the consistency of ZFC.

THEOREM 0.1B.1. Let K be a fragment of ZFC, which is strong enough to support the Gödel Second Incompleteness Theorem.

Suppose $K + \varphi$ proves $\text{Con}(\text{ZFC})$. Then φ is unprovable in every consistent fragment of ZFC that proves K .

Proof: To see this, let S be a consistent fragment of ZFC that proves K . We can assume that S is finitely axiomatized. If S proves φ then by the hypotheses, S proves $\text{Con}(\text{ZFC})$. In particular, S proves $\text{Con}(S)$. Since S extends K , S is subject to Gödel's Second Incompleteness Theorem. Hence S is inconsistent. This is a contradiction. QED

We use the following variant of Theorem 0.1B.1 in section 5.9. For the definition of SMAH, see section 0.13.

THEOREM 0.1B.2. Suppose $\text{ACA}' + \varphi$ proves $\text{Con}(\text{SMAH})$. Then φ is unprovable in every consistent fragment of SMAH that logically implies ACA' .

Informal statements of Gödel's Second Incompleteness Theorem are simple and dramatic. However, current fully rigorous statements of the Gödel Second Incompleteness are complicated and awkward. This is because the actual construction of the consistency statement - as a formal sentence in the language of the theory - is rather complicated, and no two scholars would come up with the same sentence.

Although this is a significant issue surrounding the first use of the Gödel Second Incompleteness Theorem as a foundationally meaningful example of incompleteness, this does not affect the applicability of Gödel's Second Incompleteness Theorem for obtaining incompleteness results.

But the fact that we can so confidently use Gödel's Second Incompleteness Theorem without getting bogged down in the construction of actual formalizations of consistency, does strongly suggest that there is a robust formulation of Gödel's Second Incompleteness Theorem.

It is possible to isolate syntactic properties of a formal consistency statement that are sufficient for Gödel's Second Incompleteness Theorem, and which are independent of the construction of any particular formal consistency statement. In this way, we can remove the ad hoc features in a rigorous formulation of Gödel's Second Incompleteness Theorem.

In [Fe60], [Fe82], sufficiency conditions for formalized consistency in predicate calculus are reached by a step by step analysis of the construction of the formalization. However, this leads to a very complicated and lengthy list of conditions. There may be room for future considerable simplification.

Another approach to presenting sufficiency conditions for formalized consistency in predicate calculus is found in the Hilbert Bernays derivability conditions. See [HB34,39], [Fr10]. These are simpler than the conditions that arise from the preceding approach, although they are rather subtle. They also add clarity to the proof of Gödel's Second Incompleteness Theorem.

We present a third kind of sufficiency condition for formalized consistency in predicate calculus. This is through the Gödel Completeness Theorem. The proofs of our results will appear elsewhere in [Fr ∞].

We also refer the reader to [Fr07b] and [Vi09], which are also concerned with novel formulations of Gödel's Second Incompleteness Theorem.

0.1C. Adequacy Conditions for Formalized Consistency.

Here is the key idea:

For Gödel's Second Incompleteness Theorem, it is sufficient that the formalization of consistency used support the Gödel Completeness Theorem.

We will use MSL = many sorted first order predicate calculus with equality. Infinitely many constant, relation, and function symbols are available.

Let S be a set of sentences in MSL, and let σ be a sentence in MSL. We define the notion

φ is an S sufficient formalization of $\text{Con}(\sigma)$.

Here $\text{Con}(\sigma)$ refers to consistency in MSL.

This means that φ is a sentence in $L(S)$ such that there is a structure M in $L(\sigma)$, whose components (domains, constants, relations, and functions) are given by definitions in $L(S)$, such that S proves

$\varphi \rightarrow M$ satisfies σ .

Here the consequent is a sentence of $L(S)$ that is defined straightforwardly by relativization. Note that this definition is quite easy to make fully rigorous - by direct combinatorial construction, or by induction on formulas of MSL. The intensionality issues that plague the usual statements of Gödel's Second Incompleteness Theorem are not present here.

The most natural system of arithmetic to use for S is EFA (see section 0.5). This system corresponds to the $I\Sigma_0(\exp)$ of [HP93]. Note that the notion

the usual formalizations of $\text{Con}(\sigma)$

makes good sense. We can take these to mean those that have been constructed - or are intended - by actual practitioners. Note that such formalizations are rarely given in complete detail, and even more rarely, been thoroughly debugged. EFA is finitely axiomatizable (see [DG82] and [HP93], Theorem 5.6, p. 366).

THEOREM 0.1C.1. Let σ be a sentence in MSL. Every usual formalization of $\text{Con}(\sigma)$ in $L(\text{EFA})$ is an EFA sufficient formalization of $\text{Con}(\sigma)$.

Proof: Let $\text{Con}(\sigma)^*$ be a usual formalization of $\text{Con}(\sigma)$ in $L(\text{EFA})$. We show that $\text{Con}(\sigma)^*$ is a sufficient formalization of $\text{Con}(\sigma)$ in EFA. We adapt a common proof of the Gödel completeness theorem to EFA. We effectively build a labeled 0,1 tree T whose paths define models of a consistent σ . We then show that if T has finitely many vertices, then T can be converted to a proof in MSL of $\neg\sigma$. Otherwise, T has an infinite path, and any infinite path yields a model of σ .

The conversion to a proof in MSL of $\neg\sigma$ goes through in EFA. So assume T has infinitely many vertices. We define the following property $P(v)$ on vertices v in T . $P(v)$ if and only if

- i. There are arbitrarily high vertices extending v .
- ii. There exists n such that the following holds. There are at most n vertices extending any vertex to the strict left of v .

It is clear, in EFA, that

- iii. Any two vertices obeying P are comparable.
- iv. There is no highest vertex obeying P.

If there are arbitrarily high vertices obeying P, then we define a model of σ as usual. Otherwise, we have a "cut" in T. We can use standard cut shortening, if necessary, to form a "cut" in T that can be used to define a model of σ . QED

THEOREM 0.1C.2. Let σ be a sentence in MSL. Every EFA sufficient formalization of $\text{Con}(\sigma)$ implies every usual formalization of $\text{Con}(\sigma)$ in $L(\text{EFA})$, over $\text{EFA} + \text{Con}(\text{EFA})$. (Here $\text{Con}(\text{EFA})$ is any usual formalization of $\text{Con}(\text{EFA})$ in $L(\text{EFA})$.)

Proof: Let φ be an EFA sufficient formalization of $\text{Con}(\sigma)$. Let M witness this assumption. We argue in $\text{EFA} + \text{Con}(\text{EFA}) + \varphi$ that σ is consistent in MSL. Let π be a proof of $\neg\sigma$ in MSL. By relativizing π to M, we obtain a proof in EFA of $\neg\sigma^M$. But we already have a proof in EFA of σ^M . Hence EFA is inconsistent. Therefore π does not exist. Hence σ is consistent. QED

We remind the reader that the usual formalizations of $\text{Con}(\sigma)$ in arithmetic involves arithmetizing finite sequences of nonnegative integers. Accordingly, we define SEFA (super exponential function arithmetic) to be

$\text{EFA} + \text{"for all } n, \text{ there is a sequence of integers of length } n \text{ starting with } 2, \text{ where each non initial term is the base } 2 \text{ exponential of the previous term"}$.

SEFA corresponds to the system $\text{I}\Sigma_0 + \text{Superexp}$ in [HP93], p. 376. It is well known that SEFA proves the cut elimination (see [HP93], Theorem 5.17). From this, it is easy to show that SEFA proves the 1-consistency of EFA.

The following combines Theorems 0.1C.1, 0.1C.2.

THEOREM 0.1C.3. Let σ be a sentence in MSL. The usual formalizations of $\text{Con}(\sigma)$ in $L(\text{EFA})$ are characterized, up to provable equivalence in SEFA, as the weakest EFA sufficient formalizations of $\text{Con}(\sigma)$ (weakest in the sense of SEFA). We can replace SEFA here by $\text{EFA} + \text{Con}(\text{EFA})$. (Here $\text{Con}(\text{EFA})$ is any usual formalization of $\text{Con}(\text{EFA})$ in $L(\text{EFA})$.)

The proofs can be refined to replace EFA, SEFA by PFA, EFA. Here PFA is "polynomial function arithmetic". The more

standard notation is "bounded arithmetic" or $I\Sigma_0$. This extends Q , within the language of Q , by adding the induction scheme for all bounded formulas (i.e., formulas with bounded quantifiers only). See [HP93].

For this purpose, we need to consider $WCon(\sigma)$, or "weak consistency of σ in MSL". This means that there is no cut free proof of σ in MSL. $WCon(\sigma)$ is provably equivalent, over SEFA, to $Con(\sigma)$. However, this is not the case in EFA.

THEOREM 0.1C.4. Let σ be a sentence in MSL. The expert formalizations of $WCon(\sigma)$ in $L(PFA)$ are characterized, up to provable equivalence in EFA, as the weakest PFA sufficient formalizations of $Con(\sigma)$ (weakest in the sense of EFA).

We do not use "usual formalizations of $Con(\sigma)$ in PFA", but instead "expert formalizations of $Con(\sigma)$ in PFA". This is because such formalizations in PFA are normally done only by experts in weak systems of arithmetic, because of the limited facility for finite sequence coding.

We extend sufficiency to sets of sentences in MSL. Let S, T be sets of sentences in MSL. We define

φ is an S sufficient formalization of $Con(T)$

if and only if for every conjunction σ of finitely many sentences in T , φ is an S sufficient formalization of $Con(\sigma)$.

THEOREM 0.1C.5. Let T be a set of sentences in MSL. Every EFA sufficient formalization of $Con(T)$ proves, over SEFA, the usual formalizations of the consistency of each finite fragment of T . If T is recursively enumerable, then the usual formalizations of $Con(T)$ in $L(EFA)$, based on any algorithm for generating T , are EFA sufficient formalizations of $Con(T)$. We can replace SEFA here by $EFA + Con(EFA)$. (Here $Con(EFA)$ is any usual formalization of $Con(EFA)$ in $L(EFA)$.)

THEOREM 0.1C.6. Let T be a set of sentences in MSL. Every PFA sufficient formalization of $Con(T)$ proves, over EFA, the usual formalizations of the weak consistency of each finite fragment of T . If T is recursively enumerable, then the expert formalizations of $Con(T)$ in $L(PFA)$, based on any algorithm for generating T , are PFA sufficient formalizations of $Con(T)$.

We should mention that in many cases, the usual formalizations use "natural" algorithms for generating the elements of T , rather than arbitrary ones. This would be the case for systems axiomatized by finitely many schemes. However, this interesting issue need not concern us here.

0.1D. Gödel's Second Incompleteness Theorem for Arithmetized Consistency.

The following is obtained from Theorem 0.1C.5.

THEOREM 0.1D.1. Gödel's Second Incompleteness Theorem for Consistency Formalized in EFA. Let T be a consistent set of sentences in MSL that implies SEFA. T does not prove any EFA sufficient formalization of $\text{Con}(T)$.

The usual statement of Gödel's Second Incompleteness Theorem for arithmetized consistency, is covered here by taking T to be recursively enumerable, using any usual formalization of $\text{Con}(T)$ in EFA, and applying Theorem 0.1C.5.

The following is obtained from Theorem 0.1C.6.

THEOREM 0.1D.2. Gödel's Second Incompleteness Theorem for Consistency Formalized in PFA. Let T be a consistent set of sentences in MSL that implies EFA. T does not prove any PFA sufficient formalization of $\text{Con}(T)$.

The usual statement of Gödel's Second Incompleteness Theorem for arithmetized consistency (using expert formalizations of consistency), is covered here by taking T to be recursively enumerable, using any expert formalization of $\text{Con}(T)$ in PFA, and applying Theorem 0.1C.6.

0.1E. Gödel's Second Incompleteness Theorem for Sequential Consistency.

Gödel used arithmetized consistency statements. Subsequent developments have revealed that it is more natural and direct to use sequence theoretic consistency statements.

We will use a particularly natural and convenient system for the formalization of syntax of L . We will call it SEQSYN (for sequential syntax).

SEQSYN is a two sorted system with equality for each sort. It is convenient (although not necessary) to use undefined terms. There is a very good and standard way of dealing with logic with undefined terms. This is called free logic, and it is discussed, with references to the literature, in [Fr09], p. 135-138.

In summary, two terms are equal (written =) if and only if they are both defined and have the same value. Two terms are partially equal (written \equiv) if and only if either they are equal or both are undefined. If a term is defined then all of its subterms are defined.

The two sorts in SEQSYN are Z (for integers, including positive and negative integers and 0), and FSEQ (for finite sequences of integers, including the empty sequence). We have variables over Z and variables over FSEQ (we use Greek letters). We use ring operations $0, 1, +, -, \cdot$, and $\leq, =$ between integers. We use lth (for length of a finite sequence, which returns a nonnegative integer), $\text{val}(\alpha, n)$ (for the n -th term of the finite sequence α , which may be undefined), and $=$ between finite sequences. The nonlogical axioms of SEQSYN are

- i. The discrete ordered commutative ring axioms.
- ii. Every α has a largest term.
- iii. $\text{lth}(\alpha) \geq 0$.
- iv. $\text{val}(\alpha, n)$ is defined if and only if $1 \leq n \leq \text{lth}(\alpha)$.
- v. $\alpha = \beta$ if and only if for all n , $(\text{val}(\alpha, n) \equiv \text{val}(\beta, n))$.
- vi. Induction on the nonnegative integers for all bounded formulas.
- vii. Let $n \geq 0$ be given and assume that for all $1 \leq i \leq n$, there is a unique m such that $\varphi(i, m)$. There exists a sequence α of length n such that for all $1 \leq i \leq n$, $\text{val}(\alpha, i) = m \leftrightarrow \varphi(i, m)$. Here φ is a bounded formula in $L(\text{SEQSYN})$ in which α does not appear.

It remains to define the bounded formulas. We require that the integer quantifiers be bounded in this way:

$$(\forall n) (|n| < t \rightarrow \dots)$$

$$(\exists n) (|n| < t \wedge \dots)$$

where t is an integer term in which n does not appear. Here $| \cdot |$ indicates absolute value.

We also require that the sequence quantifiers be bounded in this way:

$$(\forall \alpha) (\text{lth}(\alpha) \leq t \wedge (\forall i) (1 \leq i \leq \text{lth}(\alpha) \rightarrow |\text{val}(\alpha, i)| \leq t) \rightarrow (\exists \alpha) (\text{lth}(\alpha) \leq t \wedge (\forall i) (1 \leq i \leq \text{lth}(\alpha) \rightarrow |\text{val}(\alpha, i)| \leq t) \wedge$$

where t is an integer term in which α does not appear.

Note that SEQSYN does not have exponentiation, yet SEQSYN clearly supports the usual sequence (string) theoretic formalization of consistency.

THEOREM 0.1E.1. SEQSYN is mutually interpretable with Q and with PFA. SEQSYN is interpretable in EFA but not vice versa.

From the above, we see that the **usual** sequence (string) theoretic formalizations of consistency carry a weaker commitment than the **usual** (not the expert) arithmetic formalizations of consistency (which require finite sequence coding in EFA).

We take EXP to be the following sentence in $L(\text{SEQSYN})$.

There exists a sequence α of length $n \geq 1$ whose first term is 2, where every non initial term is twice the previous term.

THEOREM 0.1E.2. Let σ be a sentence in MSL. The usual formalizations of $\text{WCon}(\sigma)$ in $L(\text{SEQSYN})$ are characterized, up to provable equivalence in $\text{SEQSYN} + \text{EXP}$, as the weakest SEQSYN sufficient formalizations of $\text{Con}(\sigma)$ (weakest in the sense of $\text{SEQSYN} + \text{EXP}$).

THEOREM 0.1E.3. Let T be a set of sentences in MSL. Every SEQSYN sufficient formalization of $\text{Con}(T)$ proves, over $\text{SEQSYN} + \text{EXP}$, the usual formalizations of the weak consistency of each finite fragment of T . If T is recursively enumerable, then the usual formalizations of $\text{Con}(T)$ in $L(\text{SEQSYN})$, based on any algorithm for generating T , are SEQSYN sufficient formalizations of $\text{Con}(T)$.

THEOREM 0.1E.3. $\text{SEQSYN} + \text{EXP}$ and EFA are mutually interpretable. They are both finitely axiomatizable.

Proof: As remarked earlier, EFA is finitely axiomatizable (see [DG82] and [HP93], Theorem 5.6, p. 366). Now we cannot conclude from the mutual interpretability that $\text{SEQSYN} + \text{EXP}$ is also finitely axiomatizable. As an instructive example, it is well known that Q and bounded arithmetic are mutually

interpretable ([HP93], Theorem 5.7, p. 367), but it is a well known open problem whether bounded arithmetic is finitely axiomatizable. But in this case, we have a synonymy of the strongest kind, and that preserves finite axiomatizability. QED

THEOREM 0.1E.4. Gödel's Second Incompleteness Theorem for Consistency Formalized in SEQSYN. Let T be a consistent set of sentences in MSL that implies SEQSYN + EXP. T does not prove any SEQSYN sufficient formalization of $\text{Con}(T)$.

0.1F. Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability.

Let T be a finite set of sentences in $\mathcal{E}, =$. By the Set Theoretic Satisfiability of T , we mean the following sentence in set theory ($\mathcal{E}, =$):

there exists D, R , where R is a set of ordered pairs from D , such that (D, R) satisfies each element of T .

Let RST (rudimentary set theory) be the following convenient set theory in $\mathcal{E}, =$.

- a. Extensionality.
- b. Pairing.
- c. Union.
- d. Cartesian product.
- e. Separation for bounded formulas.

It can be shown that RST is finitely axiomatizable.

THEOREM 0.1F.1. Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability. Let T be a consistent finite set of sentences in $\mathcal{E}, =$ which implies RST. T does not prove the Set Theoretic Satisfiability of T .

COROLLARY. Let T be a consistent set of sentences in $\mathcal{E}, =$, which implies RST. Let φ be a sentence in $\mathcal{E}, =$ such that $T + \varphi$ proves the set theoretic satisfiability of each finite subset of T . Then T does not prove φ .

It does not appear that we can obtain Gödel's Second Incompleteness Theorem for PA and fragments, in any reasonable form, readily from Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability.

0.1G. Gödel's Incompleteness Theorems and Interpretability.

The notion of Interpretation between theories is due to Alfred Tarski in [TMR53], and has generated an extensive literature. See [Fr07], lecture 1 for a guide to many highlights. Also see [FVxx].

THEOREM 0.1G.1. Let T be a consistent set of sentences in MSL, in which Q is interpretable. The sets of all sentences in MSL that are i) provable in T , ii) refutable in T , iii) provable or refutable in T , are not recursive.

Proof: Let π be an interpretation of Q in T . Use π to convert the claims to a claim concerning extensions of Q . See Theorem 0.1A.2. This is the approach taken in [TMR53].
QED

We can obtain the following strong form of Gödel's First Incompleteness Theorem as an immediate corollary.

THEOREM 0.1G.2. Let T be a recursively enumerable consistent set of sentences in MSL, in which Q is interpretable. There is a sentence in $L(T)$ that is neither provable nor refutable in T .

Gödel's Second Incompleteness Theorem is used in an essential way to prove the following fundamental fact about interpretations, from [Fe60]. See [Fr07], lecture 1, Theorem 2.4, p. 7.

THEOREM 0.1G.3. For every consistent sentence φ in MSL, there is a consistent sentence ψ in MSL, such that φ is interpretable in ψ , and ψ is not interpretable in φ .

Gödel's Second Incompleteness Theorem also is used in an essential way to prove the following well known fact about PA.

THEOREM 0.1G.4. No consistent extension T of PA in $L(PA)$ is interpretable in any consequence of T .

We can view Theorem 0.1G.4 as a form of Gödel's Second Incompleteness Theorem for extensions of PA, since it immediately implies the following strong form of Gödel's Second Incompleteness Theorem for extensions of PA.

THEOREM 0.1G.5. Let T be a consistent extension of PA in $L(PA)$, and S be a finite fragment of T . No S sufficient formalization of $\text{Con}(T)$ is provable in T .

0.2. Some Basic Completeness.

Note that General Incompleteness depends on being able to interpret a certain amount of arithmetic.

However, there are some significant portions of mathematics, which do not involve any significant amount of arithmetic.

This opens the door to there being recursive axiomatizations for such significant portions of mathematics. This is in sharp contrast to Gödel's First Incompleteness Theorem.

A powerful way to present such completeness theorems is to identify a relational structure M and give what is called an axiomatization of M . For judiciously chosen M , the assertions that hold in M generally form a significant portion of mathematics.

Specifically, an axiomatization of M is a set T of sentences in $L(M)$ (the language of M) such that

$$\begin{array}{l} \text{For any sentence } \varphi \text{ of } L(M), \\ \varphi \text{ is true in } M \text{ if and only if} \\ \varphi \text{ is provable in } T. \end{array}$$

We say that T is a finite (or recursive) axiomatization of M if and only if T is an axiomatization of M , where T is finite (or recursive).

We frequently encounter M which are recursively axiomatizable but not finitely axiomatizable. The important intermediate notion is that of being axiomatizable by finitely many relational schemes.

Axiom schemes arise in many fundamental axiomatizations. Three particularly well known examples are not axiomatizations of structures. These are PA (Peano Arithmetic), Z (Zermelo Set Theory), and ZFC (Zermelo Set Theory with the Axiom of Choice).

We will not give a careful formal treatment of relational schemes here, but be content with the following semiformal description.

To simplify the discussion, it is convenient to work

entirely within the first order predicate calculus with equality, rather than the more general MSL.

Fix a language L' in first order predicate calculus with equality. A scheme is a formula in L' possibly augmented with extra relation symbols called schematic relation symbols. The instances of a relational scheme consists of the result of making any legitimate substitutions of the schematic relation symbols appearing by formulas of L' . One must treat different occurrences of the same schematic symbol in the same way, and put the appropriate restriction on the free variables of the formulas used for substitutions.

Schemes can be generalized to include schematic function symbols. However, we will be using only schematic relation symbols here.

Note that Induction in PA, Comprehension in Z, and both Comprehension and Replacement in ZFC, are schemes. Induction and Comprehension use a single unary schematic relation symbol, whereas Replacement uses a single binary schematic relation symbol. Replacement can also be formalized with a single unary schematic function symbol.

Here we provide axiomatizations by finitely many schemes for each of the 21 basic structures given below.

We use the method of quantifier elimination throughout. The quantifier elimination arguments that we use are well known, and we will not give details.

It is typical in the use of quantifier elimination, that the structures at hand do not admit quantifier elimination themselves, but need to be expanded in order to admit quantifier elimination. Then the quantifier elimination for the expansion is used to derive conclusions about the original structure.

An expansion of a structure is obtained by merely adding new relations, functions, or constants to the structure. A definitional expansion of a structure is an expansion whose new symbols have explicit definitions in the language of the original structure.

We say that M' is the definitional expansion of M via $\pi = \varphi_1, \dots, \varphi_n$ if M' is the expansion of M whose components are given by the definitions in π made in the language of M .

A typical example is the definitional expansion $(\mathbb{N}, <, +)$ of $(\mathbb{N}, +)$ via the definition

$$x < y \leftrightarrow x \neq y \wedge (\exists z)(x+z = y).$$

Sometimes we make a definitional expansion, followed by the introduction of new constants. Specifically, we definitionally expand $(\mathbb{Z}, +)$ to $(\mathbb{Z}, 0, +, -, 2|, 3|, \dots)$, and then introduce the constant 1 to form $(\mathbb{Z}, 0, 1, +, -, 2|, 3|, \dots)$. Note that the constant 1 is not definable in $(\mathbb{Z}, +)$.

The following easy results are quite useful when working with axiomatizations. They were used, essentially, by Tarski.

THEOREM 0.2.1. Let M' be the definitional expansion of M via π , and M'' expand M' with constants new to M' . Let S be a set of sentences that hold in M . Let T be an axiomatization of M'' . Assume that S proves the well definedness of π for the constant and function symbols new in M' . Assume S proves the result of existentially quantifying out the new constants in the conjunction of any given finite subset of T after π is used to replace the new symbols of T in the conjunction. Then S is an axiomatization of M .

Proof: Let M, M', S, T be as given. Let φ hold in M . Then φ holds in M'' , and so φ is provable in T . In any given proof of φ in T , let T' result from conjuncting the axioms of T used, replacing the new symbols of M' by their definitions given by π , and then existentially quantify out the new constants in M'' . Then T' logically implies φ , and also S proves T' . Hence S proves φ . Also by hypothesis, S holds in M . QED

THEOREM 0.2.2. Let M, M', M'' be as given in Theorem 0.2.1, where the language of M'' is finite. M is finitely axiomatizable if and only if all (some) axiomatizations of M are logically equivalent to a finite subset. M is finitely axiomatizable if and only if M' is finitely axiomatizable. If M'' is finitely axiomatizable then M is finitely axiomatizable.

Proof: The first claim (well known), involving only M , is left to the reader.

For the third claim, the process of converting an axiomatization of M' to an axiomatization of M given by Theorem 0.2.1, results in a finite axiomatization of M if the given axiomatization of M' is finite.

For the second claim, it suffices to show that if M is finitely axiomatizable then M' is finitely axiomatizable. The axiomatization of M' consists of the axiomatization of M together with the definitions given by the interpretation of M in M' . QED

There has been considerable work locating basic mathematical structures with recursive - and usually simple and informative - axiomatizations. We believe that there are many striking cases of this that are yet to be discovered across mathematics.

Here is the list of 21 fundamental mathematical structures with recursive axiomatizations.

LINEAR ORDERINGS

$(\mathbb{N}, <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$, $(\mathfrak{R}, <)$.

SEMIGROUPS, GROUPS

$(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathfrak{R}, +)$, $(\mathbb{C}, +)$.

LINEARLY ORDERED SEMIGROUPS/GROUPS

$(\mathbb{N}, <, +)$, $(\mathbb{Z}, <, +)$, $(\mathbb{Q}, <, +)$, $(\mathfrak{R}, <, +)$.

BASE TWO EXPONENTIATION

$(\mathbb{N}, +, 2^x)$.

FIELDS

$(\mathfrak{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\text{RALG}, +, \cdot)$, $(\text{CALG}, +, \cdot)$.

Here RALG is the subfield of real algebraic numbers. CALG is the subfield of complex algebraic numbers.

ORDERED FIELDS

$(\mathfrak{R}, <, +, \cdot)$, $(\text{RALG}, <, +, \cdot)$.

EUCLIDEAN GEOMETRY

(\mathfrak{R}^2, B, E) .

Here B is the three place relation of betweenness. I.e., $B(x, y, z) \leftrightarrow x, y, z$ lie on a line and y is strictly between x and z . Also E is the four place relation of equidistance. I.e., $E(x, y, z, w) \leftrightarrow d(x, y) = d(z, w)$.

Among these 21, $(\mathbb{N}, <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$, $(\mathfrak{R}, <)$ are finitely axiomatizable. The axioms for the remaining 17 are not usually presented as finitely many axiom schemes, and some thought is required in order to put them in this form. Of the 17, all but $(\mathbb{N}, +, 2^x)$ are not finitely axiomatizable. We conjecture that $(\mathbb{N}, +, 2^x)$ is not finitely axiomatizable.

Below, we freely invoke Theorems 0.2.1 and 0.2.2.

THEOREM 0.2.3. $(\mathbb{N}, <)$ is finitely axiomatized by

- i. $<$ is a strict linear ordering.
- ii. There is a $<$ least element.
- iii. Every element has an immediate successor.
- iv. Every element with a predecessor has an immediate predecessor.

Proof: i-iv clearly hold in $(\mathbb{N}, <)$. We use Theorem 0.2.1 with the definitional expansion $(\mathbb{N}, <, 0, S)$ via π , where π defines 0 as "the least element", and π defines S as "the immediate successor". $(\mathbb{N}, <, 0, S)$ has the following well known axiomatization, using elimination of quantifiers. See, e.g., [En72], p. 184.

- a. $<$ is a strict linear ordering.
- b. 0 is $<$ least.
- c. $x \neq 0 \rightarrow (\exists y)(x = S(y))$.
- d. $x < S(y) \leftrightarrow x < y \vee x = y$.

Since π is provably well defined in i-iv, and the results of applying π to a-d are provable in i-iv, we see that i-iv is an axiomatization of $(\mathbb{N}, <)$. QED

THEOREM 0.2.4. $(\mathbb{Z}, <)$ is finitely axiomatized by

- i. $<$ is a strict linear ordering.
- ii. Every element has an immediate predecessor and an immediate successor.

Proof: i-ii clearly hold in $(\mathbb{Z}, <)$. We use Theorem 0.2.1 with the definitional expansion $(\mathbb{Z}, <, S)$ via π , where π defines S as "the immediate successor". $(\mathbb{Z}, <, S)$ has the

following well known axiomatization, using elimination of quantifiers.

- a. $<$ is a strict linear ordering.
- b. $(\exists y)(x = S(y))$.
- c. $x < S(y) \leftrightarrow x < y \vee x = y$.

Since π is provably well defined in i,ii, and the results of applying π to a-c are provable in i,ii, we see that i,ii is an axiomatization of $(\mathbb{N}, <)$. QED

THEOREM 0.2.5. $(\mathbb{Q}, <)$, $(\mathfrak{R}, <)$ are finitely axiomatized by

- i. $<$ is a strict linear ordering.
- ii. There is no least and no greatest element.
- iii. Between any two elements there is a third.

Proof: This is a particularly well known application of elimination of quantifiers, resulting in this axiomatization. No expansion is needed. QED

THEOREM 0.2.6. $(\mathbb{N}, +)$ is axiomatized with a single scheme by

- i. $(x+y)+z = x+(y+z)$, $x+y = x+z \rightarrow y = z$.
 - ii. There are unique $0 \neq 1$ such that $(x+y = 0 \leftrightarrow x, y = 0) \wedge (x+y = 1 \leftrightarrow \{x, y\} = \{0, 1\})$.
 - iii. Every definable set containing 0 and closed under $+1$ is everything.
- $(\mathbb{N}, +)$ is not finitely axiomatizable.

Proof: i-iii clearly hold in $(\mathbb{N}, +)$. We use Theorem 0.2.1 with the definitional expansion $(\mathbb{N}, <, 0, S, +, \equiv_2, \equiv_3, \dots)$ via π , where π defines

- $<$ as $x \neq y \wedge (\exists z)(x+z = y)$.
- 0 as the 0 from ii.
- $S(x) = x+1$, where 1 is from ii.
- $\equiv_d, d \geq 2$, as $x \equiv_d y \leftrightarrow (\exists z)(x = y+dz \vee y = x+dz)$.

Obviously, i-iii proves π is well defined.

We now use the well known elimination of quantifiers for $(\mathbb{N}, <, 0, S, +, \equiv_2, \equiv_3, \dots)$ from [Pr29], [En72], p. 188. Here $\equiv_d, d \geq 2$, is congruence modulo d . This results in the following axiomatization of $(\mathbb{N}, <, 0, S, +, \equiv_2, \equiv_3, \dots)$.

- a. $<$ is a strict linear ordering.
- b. 0 is the least element.
- c. $x \neq 0 \rightarrow (\exists y)(x = S(y))$.
- d. $x < S(y) \leftrightarrow x < y \vee x = y$.

- e. $+$ is commutative, associative.
- f. $x+0 = x$.
- g. $x+S(y) = S(x+y)$.
- h. $x+z < y+z \leftrightarrow x < y$.
- i. $x < y \leftrightarrow (\exists z)(S(x+z) = y)$.
- j. $dx < dy \leftrightarrow x < y$.
- k. $x \equiv_d y \leftrightarrow (\exists z)(x = y + dz \vee y = x + dz)$.
- l. $(\exists y)(x \equiv_d y \wedge y < S^d(0))$.

where $d \geq 2$.

We prove that the results of applying π to a-1 are provable in i-iii.

This is the same as treating $<, 0, S, \equiv_d$ as abbreviations in 1-iii, and verifying a-1 in i-iii. It is convenient to also use the abbreviation $x \leq y \leftrightarrow x < y \vee x = y$, in i-iii.

By ii), $1+1 \neq 0 \wedge 1+1 \neq 1$.

We claim $x+1 \neq 0$. Suppose $x+1 = 0$. Then $x+(1+1) = (x+1)+1 = 0+1 = 1$. By ii), $1+1 \in \{0,1\}$, which is impossible.

We claim $x+0 = x$. Let $E = \{x: x+0 = x\}$. By ii), $0 \in E$. Let $x \in E$. Then $x+0 = x$, and by i), ii), $(x+1)+0 = x+(1+0) = x+1$. Hence E contains 0 and is closed under $+1$. By iii), E is everything.

We claim $x \neq 0 \rightarrow (\exists y)(x = y+1)$. Let $E = \{x: (\exists y)(x = y+1)\} \cup \{0\}$. Then E contains 0 and is closed under $+1$. Hence by iii), E is everything.

We claim $0+x = x$. Let $E = \{x: 0+x = x\}$. Then $0 \in E$. Let $x \in E$. Then $0+(x+1) = (0+x)+1 = x+1$. Apply iii).

We claim $x+y = y+x$. Let $E = \{y: x+y = y+x\}$. By the previous paragraph, $0 \in E$. Let $x \in E$. Then $x+y = y+x$, $x+(y+1) = (x+y)+1 = (y+x)+1 = y+(x+1)$. Apply iii).

We claim $x \leq y \leftrightarrow (\exists z)(x+z = y)$. Suppose $x \leq y$. If $x < y$ then we are done. If $x = y$ then use $z = 0$. Now suppose $x+z = y$. If $z = 0$ then we are done. If $z \neq 0$, write $z = w+1$. Hence $z = S(w)$, and we are done.

Obviously \leq is reflexive. We claim \leq is transitive. Let $x+u = y \wedge y+v = z$. Then $x+u+v = z$, and so $x \leq z$.

We claim $y \leq x \rightarrow y+1 \leq x \vee y = x$. Let $y \leq x$. Write $y+z = x$. If $z = 0$ then $y = x$, and we are done. Assume $z \neq 0$, and write $z = w+1$. Then $y+w+1 = x = y+1+w$, and so $y+1 \leq x$.

We claim $x \leq y \vee y \leq x$. Let $E = \{y: x \leq y \vee y \leq x\}$. Obviously $0 \in E$. We now show that E is closed under $+1$. Suppose $y \in E$. Then $x \leq y \vee y \leq x$. We want $x \leq y+1 \vee y+1 \leq x$.

We are done if $x \leq y$. So assume $y \leq x$. By the previous claim, $y+1 \leq x \vee y = x$. In either case, we are done.

We claim $x \leq y \wedge y \leq x \rightarrow x = y$. Let $x+z = y \wedge y+z = x$. Then $x+z+z = x = x+0$, $z+z = 0$, $z = 0$, $x = y$.

We have established that \leq is a reflexive linear ordering. Hence $<$ is a strict linear ordering.

I.e., we have proved the result of applying π to a) in i-iii.

For b), suppose $x < 0$. Let $x+y = 0$. Then $x, y = 0$, which is impossible.

For c), this has already been proved.

For d), let $x < y+1$. Write $y+1 = x+z+1$. Then $y = x+z$, and so $x \leq y$. Suppose $x < y$. Then $x < y+1$. Suppose $x = y$. Then $x < y+1$.

For e), associativity is from i), and commutativity has been proved.

For f), we have proved $x+0 = x$.

For g), use associativity.

For h), let $x+z < y+z$. Let $x+z+w = y+z$, $w \neq 0$. By cancellation and commutativity, $x+w = y$, and so $x \leq y$. If $x = y$ then $x+z = y+z$, which is impossible. Hence $x < y$. Now let $x < y$. Write $x+w+1 = y$. Then $x+z+w+1 = y+z$, and so $x+z < y+z$.

For i), let $x < y$. Write $y = x+z+1$. Then $S(x+z) = y$. Now let $S(x+z) = y$. Then $y = x+z+1$, and so $x < y$.

For j), let $dx < dy$. We want $x < y$, and so assume $y \leq x$ and write $y+z = x$. Then $d(y+z) < dy$. Hence $dy+dz < dy+0$. By h), $dz < 0$, which is impossible.

For k), this is by definition.

For l), let $E = \{x: (\exists y, z) (x = dy+z \wedge z < S^d(0))\}$. Obviously, $0 \in E$. Suppose $x \in E$. Let $x = dy+z \wedge z < S^d(0)$. Then $x+1 = dy+z+1 \wedge z+1 \leq S^d(0)$. If $z+1 < S^d(0)$ then $x+1 \in E$. Otherwise, $x+1 = dy+S^d(0) = d(y+1)+0 \wedge 0 < S^d(0)$. In either case, $x+1 \in E$. Hence E contains 0 and is closed under $+1$. By iii), E is everything. Hence $(\forall x) (\exists y) (x \equiv_d y \wedge y < S^d(0))$.

To show that $(\mathbb{N}, +)$ is not finitely axiomatizable, by Theorem 0.2.2 it suffices to show that any finite fragment of a-1 has a model not satisfying all of a-1. This is because a-1 is a definitional extension of i-iii.

Let p be any prime. Let D consist of all expressions $nx/m + t$, where $(n, m) = 1$, $n, t \in \mathbb{N}$, $m \in \mathbb{N} \setminus \{0\}$, and p does not divide m . Define the structure $(D, <, 0, S, +)$ in the obvious way, and extend it to $(D, <, 0, S, +, \equiv_2, \equiv_3, \dots)$ via π .

Evidently, a-i hold in $(D, <, 0, S, +, \equiv_2, \equiv_3, \dots)$. Also, l) holds provided $d \geq 2$ is not divisible by p .

But l) fails for $d = p$. This is because we cannot write any of $x, x-1, \dots, x-p+1$ as a multiple of p in this structure.

QED

THEOREM 0.2.7. $(\mathbb{Z}, +)$ is axiomatized with two schemes by

- i. $(\mathbb{Z}, +)$ is an Abelian group.
- ii. Every definable subgroup of $+$ with a definable linear ordering is $\{0\}$.
- iii. R, S be definable binary relations. Suppose for all x , $\{y: R(x, y)\}$ is a subgroup of $+$ containing x , and $\{y: S(x, y)\}$ is a proper subgroup of $+$. Then $(\exists x) ((\forall y) (R(x, y) \wedge \neg S(y, x)))$.

$(\mathbb{Z}, +)$ is not finitely axiomatizable.

Proof: Clearly i) holds in $(\mathbb{Z}, +)$.

For iii), the proper subgroups of $+$ are the multiples of some fixed $d = 0, 2, 3, \dots$. Hence 1 lies outside of all of them. Set $x = 1$.

For ii), we use the definitional expansion $(\mathbb{Z}, 0, +, -, 2|, 3|, \dots)$ of $(\mathbb{Z}, +)$ via π , where 0 is defined as the additive identity, $+$, $-$ as addition and the additive inverse, and $d|x$ as $(\exists y)(dy = x)$, $d \geq 2$.

We use the well known elimination of quantifiers for linear arithmetic adapted to the structure $(\mathbb{Z}, 0, 1, +, -, 2|, 3|, \dots)$.

The quantifier elimination boils down to considering statements of the form

$$(\exists x)(d_1|s_1 \wedge \dots \wedge d_n|s_n \wedge \neg e_1|t_1 \wedge \dots \wedge \neg e_n|t_n \wedge r_1 = 0 \wedge \dots \wedge r_n = 0 \wedge v_1 \neq 0 \wedge \dots \wedge v_n \neq 0)$$

where the d_i, e_i are integers ≥ 2 , and the s_i, t_i, r_i, v_i are terms. We can replace negated divisibilities by disjunctions of divisibilities, and then rewrite the divisibilities as congruences, obtaining the form

$$(\exists x)(a_1x \equiv_{d_1} s_1 \wedge \dots \wedge a_nx \equiv_{d_n} s_n \wedge r_1 = 0 \wedge \dots \wedge r_n = 0 \wedge v_1 \neq 0 \wedge \dots \wedge v_n \neq 0)$$

where the a_i, d_i are integers, $a_i \geq 1$, $d_i \geq 2$, and the s_i, t_i, r_i, v_i are terms, and x does not appear in the s_i . We then consolidate all coefficients on x , obtaining the forms

$$(\exists x)(cx \equiv_{d_1} s_1 \wedge \dots \wedge cx \equiv_{d_n} s_n \wedge cx = r_1 \wedge \dots \wedge cx = r_n \wedge cx \neq v_1 \wedge \dots \wedge cx \neq v_n)$$

$$(\exists x)(x \equiv_{d_1} s_1 \wedge \dots \wedge x \equiv_{d_n} s_n \wedge x = r_1 \wedge \dots \wedge x = r_n \wedge x \neq v_1 \wedge \dots \wedge x \neq v_n)$$

where the d_i are integers ≥ 2 , and the s_i, t_i, r_i, v_i are terms in which x does not appear. We can assume that there are no equations, obtaining the form

$$(\exists x)(x \equiv_{d_1} s_1 \wedge \dots \wedge x \equiv_{d_n} s_n \wedge x \neq v_1 \wedge \dots \wedge x \neq v_n).$$

This is clearly equivalent to

$$(\exists x)(x \equiv_{d_1} s_1 \wedge \dots \wedge x \equiv_{d_n} s_n)$$

and hence has a solution if and only if it has a solution among the nonnegative integers below the product of the d 's. This results in a quantifier free formula.

For ii), first note that every subgroup of $+$ is the set of multiples of some $d \geq 0$. If the multiples of $d > 0$ has a definable linear ordering in $(\mathbb{Z}, +)$, then \mathbb{Z} has a definable linear ordering in $(\mathbb{Z}, +)$, in which case N is definable in $(\mathbb{Z}, +)$. Then N is definable in $(\mathbb{Z}, 0, 1, +, -, |2, |3, \dots)$, and so N is quantifier free definable in $(\mathbb{Z}, 0, 1, +, -, |2, |3, \dots)$. This is impossible (left to the reader).

We now use this quantifier elimination to complete the proof. In order to support the manipulations for this quantifier elimination, it suffices to have

- a. $(\mathbb{Z}, 0, +, -)$ is an Abelian group, with inverse $-$ and identity 0 .
- b. $d|x \leftrightarrow (\exists y)(x = dy)$.
- c. $dx = dy \rightarrow x = y$.
- d. $dx \neq 1$.
- e. $d|x \vee d|x+1 \vee d|x+1+1 \vee \dots \vee d|x+1+\dots+1$ with d disjuncts.

where $d \geq 2$.

We claim that every quantifier free sentence in $0, 1, +, -, |2, |3, \dots$ is provable or refutable in a-e. This is left to the reader.

It now follows that a-e is an axiomatization of $(\mathbb{Z}, 0, 1, +, -, |2, |3, \dots)$.

We now verify the condition in Theorem 0.2.1. Accordingly, fix a positive integer t , let K consist of a) and those instances of b-e based on $2 \leq d \leq t$. Let K' be the result of applying π , and then existentially quantifying out the constant 1 .

We can pull out the conjuncts emanating from a)-c) since they do not mention 1 . We claim that the result of applying π to a-c), is provable in i-iii. This is obvious for a), b).

For c), suppose $dx = dy \wedge x \neq y$. Then $dz = 0$, $z \neq 0$, where $z = x-y$. Let G be the group $\{0, z, 2z, \dots, (d-1)z\}$ under $+$. Obviously G is definable since it has at most d elements. It also has a definable linear ordering since it has at most d elements. By ii), it is $\{0\}$, which is a contradiction. Hence c) has been proved in i-iii.

It remains to prove

$$\#) (\exists x) (\neg 2|x \wedge \dots \wedge \neg t!|x \wedge (\forall y) (t!|y \vee t!|y+x \vee \dots \vee t!|y+(t!-1)x))$$

in i-iii, after applying π . Here $t \geq 2$.

Let $R(x,y)$ be

$$t!|y \vee t!|y+x \vee \dots \vee t!|y+(t!-1)x.$$

and let $S(y,x)$ be

$$(y = 2 \wedge 2|x) \vee \dots \vee (y = t! \wedge t!|x) \vee (y \neq 2 \wedge \dots \wedge y \neq t! \wedge x = 0).$$

Note that i-iii proves $(\forall x) (\{y: R(x,y)\})$ is a group under $+$ containing x , and $(\forall y) (\{x: S(x,y)\})$ is a proper subgroup of $+$. Hence # immediately follows using iii). Therefore i-iii is an axiomatization of $(\mathbb{Z}, +)$.

To show that $(\mathbb{Z}, +)$ is not finitely axiomatizable, we give another axiomatization of $(\mathbb{Z}, +)$, and show that it is not logically equivalent to any finite subset, and invoke Theorem 0.2.2.

i'. $(\mathbb{Z}, +)$ is an Abelian group.

ii'. $dx = dy \rightarrow x = y$.

iii'. $(\exists x) ((\neg 2|x \wedge \dots \wedge \neg d|x) \wedge (\forall y) (d|y \vee d|y+x \vee \dots \vee d|y+(d-1)x))$.

where $d \geq 2$ and $d|x$ is the usual abbreviation. It is clear from the above that the existential closure of every finite subset of a-e is provable in i'-iii'. Therefore i'-iii' is a complete axiomatization of $(\mathbb{Z}, +)$.

Let p be any prime. Let D consist of all expressions $nx/m + t$, where $(n,m) = 1$, $n, t \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$, and p does not divide m . Define the structure $(D, +)$ in the obvious way.

Evidently, i', ii' hold in $(D, +)$ for $2 \leq d < p$. Also iii' holds in $(D, +)$ for $2 \leq d < p$ with $x = 1$.

We claim that iii') fails in $(D, +)$ for $d = p$. To see this, let

$$(\forall y) (p|y \vee p|y+z \vee \dots \vee p|y+(p-1)z).$$

Now suppose $z = nx/m + t$. By setting $y = 1$, we have

$$p|1 \vee p|1+z \vee \dots \vee p|1+(p-1)z).$$

It follows that $p|n \wedge p|t$. Now set $y = x$. Then we obtain

$$p|x \vee p|(n+m)x/m \vee p|(2n+m)x/m \vee \dots \vee p|((p-1)n+m)x/m.$$

Now $(p,m) = 1$, and so the numerators and denominators of the displayed fractions are not divisible by p . Thus we have a contradiction. QED

THEOREM 0.2.8. $(\mathbb{Q}, +)$, $(\mathfrak{R}, +)$, $(\mathbb{C}, +)$ are axiomatized with a single scheme by

- i. $(X, +)$ is an Abelian group with at least two elements.
- ii. Every definable subgroup of $(X, +)$ with at least two elements is $(X, +)$.

$(\mathbb{Q}, +)$, $(\mathfrak{R}, +)$, $(\mathbb{C}, +)$ are not finitely axiomatizable.

Proof: There is a well known quantifier elimination without expansion. This gives the axiomatization

- a. $(X, +)$ is an Abelian group with at least two elements.
- b. $dx = dy \rightarrow x = y$.
- c. $(\exists y)(dy = x)$.

where $d \geq 2$. From this we obtain that the definable subsets in $(X, +)$ are finite or cofinite. Every subgroup of $(X, +)$ is either infinite or $\{0\}$. Hence every subgroup of $(X, +)$ definable in $(X, +)$ is either cofinite or $\{0\}$. But if it is cofinite then it is obviously $(X, +)$. This establishes that i,ii hold in $(X, +)$.

a) is provable in i,ii. For b), suppose $dx = 0$, $x \neq 0$, $d \geq 2$, and form the finite subgroup $\{0, x, \dots, (d-1)x\}$. This contradicts ii).

For c), let $d \geq 2$ and form the subgroup of multiples of d . By a,b, this subgroup has at least two elements. By ii), this subgroup is $(X, +)$. Hence c) holds.

Let p be a prime. Let D be the rationals which, in reduced form, has denominator not divisible by p . Form $(D, +)$. Then a,b hold, and c) holds for $2 \leq d < p$. $d \geq 2$, However, c) fails for $d = p$. Hence $(X, +)$ is not finitely axiomatizable. QED

THEOREM 0.2.9. $(\mathbb{N}, <, +)$ is axiomatized with a single scheme by

- i. $(x+y)+z = x+(y+z)$, $x+y = x+z \rightarrow y = z$.

- ii. There are unique $0 \neq 1$ such that $x+y = 0 \Leftrightarrow x, y = 0$, and $x+y = 1 \Leftrightarrow \{x, y\} = \{0, 1\}$.
 - iii. $x < y \Leftrightarrow x \neq y \wedge (\exists z)(x+z = y)$.
 - iv. Every definable set containing 0 and closed under +1 is everything.
- $(\mathbb{N}, <, +)$ is not finitely axiomatizable.

Proof: Obviously i-iv hold in $(\mathbb{N}, <, +)$. Let φ hold in $(\mathbb{N}, <, +)$. Replace all occurrences of $s < t$ in φ by the definition according to iii). Then the resulting formula φ' holds in $(\mathbb{N}, +)$, and so by Theorem 0.2.6, is provable in the i-iii of Theorem 0.2.6. Hence φ' is provable in the above i-iv. Also $\varphi \Leftrightarrow \varphi'$ is provable in the above i-iv. Hence φ is provable in the above 1-iv. Hence φ is provable in the above i-iv.

$(\mathbb{N}, <, +)$ is not finitely axiomatizable since $(\mathbb{N}, <, +)$ is a definitional extension of $(\mathbb{N}, <)$, and $(\mathbb{N}, <)$ is not finitely axiomatizable by Theorem 0.2.6. QED

THEOREM 0.2.10. $(\mathbb{Z}, <, +)$ is axiomatized with a single scheme by

- i. $(\mathbb{Z}, +)$ is an Abelian group.
 - ii. $<$ is a strict linear ordering.
 - iii. $x+y < x+z \rightarrow y < z$.
 - iv. Every definable set with an element > 0 has a least element > 0 .
- $(\mathbb{Z}, <, +)$ is not finitely axiomatizable.

Proof: i-iv clearly hold in $(\mathbb{Z}, <, +)$. We use Theorem 0.2.1 with the definitional expansion $(\mathbb{Z}, <, 0, 1, +, -, 2|, 3|, \dots)$ via π , where π defines

- 0 as the additive identity.
- 1 as the immediate successor of 0.
- $x-y$ as the additive inverse.
- $d|x \Leftrightarrow (\exists y)(x = dy)$.

where $d \geq 2$. The well known quantifier elimination for $(\mathbb{Z}, <, 0, 1, +, -, 2|, 3|, \dots)$ leads to the complete axiomatization

- a. $(\mathbb{Z}, 0, +, -)$ is an Abelian group, with inverse $-$ and identity 0.
- b. $<$ is a strict linear ordering.
- c. $x+y < x+z \rightarrow y < z$.
- d. $d|x \Leftrightarrow (\exists y)(x = dy)$.
- e. $x+1$ is the immediate successor of x .

f. $x > 0 \rightarrow (\exists y) (0 \leq y < d(1) \wedge d|x-y)$.

where $d \geq 2$. It is easy to see that the result of applying π to a-f is provable in i-iv. Hence i-iv is an axiomatization of $(\mathbb{Z}, <, +)$.

To see that $(\mathbb{Z}, <, +)$ is not finitely axiomatizable, we argue that a-f is not logically equivalent to any finite subset of a-f.

Let p be any prime. Let D consist of all expressions $nx/m + t$, where $(n,m) = 1$, $n, t \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$, and p does not divide m . Define the structure $(D, <, 0, 1, +, -, 2|, 3|, \dots)$ in the obvious way. Then a-e hold. Also f) holds for $2 \leq d < p$. But f) fails for $d = p$. QED

THEOREM 0.2.11. $(\mathbb{Q}, <, +)$, $(\mathfrak{R}, <, +)$ are axiomatized with a single scheme by

- i. $+$ is an Abelian group.
- ii. $<$ is a dense linear ordering without endpoints.
- iii. $x+y < x+z \rightarrow y < z$.
- iv. Every definable subgroup of $(X, +)$ with at least two elements is $(X, +)$.

$(\mathbb{Q}, <, +)$, $(\mathfrak{R}, <, +)$ are not finitely axiomatizable.

Proof: $(X, <, +)$ has a well known quantifier elimination, which yields the following axiomatization.

- a. $+$ is an Abelian group.
- b. $<$ is a dense linear ordering without endpoints.
- c. $x+y < x+z \rightarrow y < z$.
- d. $(\exists y) (dy = x)$.

where $d \geq 2$. It is clear from the quantifier elimination that every set definable in $(X, <, +)$ is a finite union of intervals with endpoints in $X \cup \pm\infty$. Hence i-iv hold in $(X, <, +)$. Also d) is derived from i-iv by forming the subgroup of all multiples of $d \geq 2$, and applying iv). This establishes that i-iv is an axiomatization of $(X, <, +)$.

To see that $(X, <, +)$ is not finitely axiomatizable, argue as in the last paragraph of the proof of Theorem 0.2.8. QED

THEOREM 0.2.12. $(\mathbb{N}, +, 2^x)$ is axiomatized with a single scheme by

- i. $(x+y)+z = x+(y+z)$, $x+y = x+z \rightarrow y = z$.
- ii. There are unique $0 \neq 1$ such that $x+y = 0 \leftrightarrow x, y = 0$, and $x+y = 1 \leftrightarrow \{x, y\} = \{0, 1\}$.

iii. $2^0 = 1, 2^{x+1} = 2^x + 2^x$.

iv. Every definable set containing 0 and closed under +1 is everything.

Proof: Obviously i-iv hold in $(N, +, 2^x)$. We use the definitional expansion of $(N, +, 2^x)$ and its axiomatization given in Appendix B, p. 3. The definitional expansion is $M = (N, +, -, \leq, 0, 1, \div n, 2^x, l_2, \lambda_2)$, $n \geq 0$, where π is as follows.

$x - ' y = 0$ if $y > x$; $x - y$ otherwise.

$x \leq y \leftrightarrow (\exists z)(x+z = y)$.

0 is the 0 of ii).

1 is the 1 of ii).

For $n > 0$, $x+n$ is the unique y such that $ny \leq x < n(y+1)$.

For $n = 0$, $x+n = 0$.

$l_2(x)$ is the unique y such that $2^y \leq x < 2^{y+1}$ if $x > 0$; 0 otherwise.

$\lambda_2(x) = 2^{1-2^{(x)}}$ if $x > 0$; 0 otherwise.

By Theorem 0.2.6, i-iv proves every sentence true in M that has only +. I.e., i-iv contains Presburger Arithmetic. Hence π is provably well defined in i-iv, except possibly for $l_2(x)$ and $\lambda_2(x)$.

Let $E = \{x: (\forall y < x)(2^{y+1} \leq 2^x)\}$. Then $0 \in E$. Let $x \in E$. Since $(\forall y \leq x)(2^{y+1} \leq 2^{x+1})$, we have $x+1 \in E$. We conclude that E is everything. From this, we see that there is at most one y such that $2^y \leq x < 2^{y+1}$.

Let $E = \{x: (\exists y)(2^y \leq x < 2^{y+1})\} \cup \{0\}$. Obviously $0 \in E$. Let $x \in E$, $2^y \leq x < 2^{y+1}$. To see that $x+1 \in E$, note that $2^y \leq x+1 < 2^{y+1}$, holds or $x+1 = 2^{y+1}$. Hence E is everything.

We have established that $l_2(x)$ is well defined.

Appendix B does quantifier elimination for M , with an axiomatization of M on page 3. We briefly sketch why the result of applying π to these axioms is provable in i-iv.

The axiomatization uses the Euler function, $\phi(m) =$ the number of positive integers $\leq m$ that are relatively prime with m . Of course, this function is only used externally.

Appendix B uses the following well known fundamental fact about the Euler totient function. If m is an odd positive integer then $2^{\phi(m)} - 1$ is a multiple of m .

(1) T_{Pres} . Presburger Arithmetic. We have already remarked that by Theorem 0.2.6, the result of applying π to T_{Pres} is provable in 1-iv.

(2) $(\forall x) (\lambda_2(x) \leq x < 2\lambda_2(x))$. Obvious from π at λ_2, l_2 .

(3) $(\forall x, y) (x \geq y \rightarrow l_2(x) \geq l_2(y))$. Obvious from π at l_2 .

(4) $l_2(1) = 0$. Obvious from π at l_2 .

(5) $(\forall x) (x \geq 1 \rightarrow l_2(2x) = l_2(x)+1)$. Obvious from π at l_2 and iii).

(6) $(\forall x) (x \geq 1 \rightarrow 2^{1-2^x} = \lambda_2(x))$. Obvious from π at l_2, λ_2 .

(7) $(\forall x) (l_2(2^x) = x)$. Obvious from π at l_2 .

(8) $(\forall x) (2^{x+1} = 2^x + 2^x)$. By iii).

(9) $(\forall x) (x \geq 1 \rightarrow 2^{x-1} \geq x)$. Let $E = \{x: 2^{x+1} \geq x\} \cup \{0\}$. Obviously $0 \in E$. Suppose $x \in E$. Then $x+1 \in E$. Hence by iv), E is everything.

(10) $(\forall x) (\text{if } x \text{ is a multiple of } \phi(m) \text{ then } 2^x-1 \text{ is a multiple of } m)$, where m is an odd positive integer. It suffices to prove that for all y , $2^{\phi(m)y}-1$ is a multiple of m . We apply iv). Let $E = \{y: 2^{\phi(m)y}-1 \text{ is a multiple of } m\}$. Obviously, $0 \in E$. Let $y \in E$. Then $2^{\phi(m)y}-1$ is a multiple of m . Now if we keep multiplying $2^{\phi(m)y}$ by 2, $\phi(m)$ times, then the exponent raises by m , and so we arrive at $2^{\phi(m)(y+1)}$. Hence $2^{\phi(m)}(2^{\phi(m)y}-1) = 2^{\phi(m)(y+1)}-2^{\phi(m)}$ is a multiple of m . Since $2^{\phi(m)}-1$ is a multiple of m , we see that $2^{\phi(m)(y+1)}-1$ is a multiple of m . Hence $y+1 \in E$. Since we have established that E contains 0 and is closed under $+1$, we apply iv) to obtain that for all y , $2^{\phi(m)y}-1$ is a multiple of m . QED

We conjecture that $(\mathbb{N}, +, 2^x)$ is not finitely axiomatizable.

THEOREM 0.2.13. $(\mathfrak{R}, +, \cdot)$, $(\text{RALG}, +, \cdot)$ are axiomatized with a single scheme by

i. $(X, +, \cdot)$ is a field.

ii. The relation $y-x$ is a nonzero square, is a strict linear ordering of x, y .

iii. Every definable nonempty bounded set has a least upper bound.

$(\mathfrak{R}, +, \cdot)$, $(\text{RALG}, +, \cdot)$ are not finitely axiomatizable.

Proof: It is well known that i-iii hold in $(X, +, \cdot)$. We now use Theorem 0.2.1 and the definitional expansion $(X, <, 0, 1, +, \cdot)$ via π , where $<$ is defined by $x < y \Leftrightarrow y-x$ is a nonzero square, 0 is defined as the unique x with $x+x = x$, 1 is defined as the unique x with $(\forall y)(xy = y)$.

The well known elimination of quantifiers leads to the axiomatization

- a. $(X, 0, 1, +, \cdot)$ is a field.
- b. $<$ is a strict linear ordering.
- c. $x < y \rightarrow x+z < y+z$.
- d. $0 < x \wedge 0 < y \rightarrow 0 < x \cdot y$.
- e. $0 < x \rightarrow (\exists y)(x = y^2)$.
- f. Every polynomial of odd degree ≥ 1 with leading coefficient 1 has a zero.

We claim that the result of applying π to a-f is provable in i-iii. Clearly this holds of a,b.

For c), suppose $y-x$ is a nonzero square. Then $(y+z)-(x+z)$ is a nonzero square.

For d), suppose x, y are nonzero squares. Then $x \cdot y$ is a nonzero square.

For e), suppose x is a nonzero square. Then x is a square.

This also verifies the usual ordered field axioms, formulated with $<$, within i-iii. Hence we can show in i-iii that every monic polynomial of odd degree ≥ 1 is positive for all sufficiently positive x , and negative for all sufficiently negative x .

Let E be the set of all x such that $P(x) < 0$. Then E is obviously nonempty and bounded. Let w be the $<$ least upper bound of E , according to iii. Using the ordered field axioms, we see that $P(w) = 0$.

We have thus proved that i-iii is an axiomatization of $(X, +, \cdot)$.

It is well known that a-f, the theory of ordered real closed fields, is not finitely axiomatizable. Fix an odd prime p . We can build the partial real closure $K[p]$ of the field of rationals, adding square roots of positive elements and roots of odd degree monic polynomials of degree $< p$ only. The p -th root of 2 is missing, but axioms

a-e hold, and axiom f) holds for odd degree $< p$. Hence by Theorem 0.2.2, $(X, +, \cdot)$ is not finitely axiomatizable. QED

We will be using the following combinatorial lemma.

LEMMA 0.2.14. If $(A, <)$ is an uncountable linear ordering, then there exists $a \in A$ such that $(-\infty, a)$ and (a, ∞) are infinite.

Proof: Suppose not. Then for all $a \in A$, $(-\infty, a)$ or (a, ∞) is uncountable.

Define the equivalence relation $a \sim b$ if and only if there are finitely many points between a and b .

Since every equivalence class is countable, there are uncountably many equivalence classes. Let $1 \leq \alpha \leq \omega$ be such that there are uncountably many equivalence classes of cardinality α .

case 1. $\alpha < \omega$. Let $[a, b], [c, d]$ be equivalence classes of cardinality α , $a < b < c < d$. Then b is a limit point from the right, and c is a limit point from the left. Hence $(-\infty, b), (b, \infty)$ are infinite.

case 2. $\alpha = \omega$. Let $I < J < K$ be three equivalence classes of cardinality ω . For all $a \in J$, $(-\infty, a), (a, \infty)$ are infinite. QED

THEOREM 0.2.15. $(C, +, \cdot), (CALG, +, \cdot)$ are axiomatized with two schemes by

- i. $(X, +, \cdot)$ is a field.
 - ii. Every definable subgroup of $(X, +)$ with at least two elements is $(X, +)$.
 - iii. Let $f: X^2 \rightarrow X$ be definable. Let $(A, <)$ be a definable strict linear ordering, $A \subseteq X$. Assume that for all $z \in A$, $f_z: X \rightarrow X$ is either constant, or the identity, or the sum or product of two $f_w: X \rightarrow X$ with $w < z$. Then for all $z \in A$, $f_z: X \rightarrow X$ is constant or onto.
- $(C, +, \cdot)$ and $(CALG, +, \cdot)$ are not finitely axiomatizable.

Proof: We use Theorem 0.2.1 and the definitional expansion $(X, +, \cdot, 0, 1)$ by π , where 0 is the unique z with $(\forall w)(z+w = w)$ and 1 is the unique $z \neq 0$ with $(\forall w)(z \cdot w = w)$.

$(X, +, \cdot, 0, 1)$ has a very well known quantifier elimination leading to the very well known axiomatization

- a. $(X, +, \cdot, 0, 1)$ is a field.
- b. $dz = dw \rightarrow z = w$.
- c. Every polynomial of degree ≥ 1 has a zero.

where $d \geq 2$. Using the quantifier elimination, we easily obtain the well known crucial property that every set definable in $(X, +, \cdot)$ is finite or cofinite. We also see that X has no strict linear ordering.

Obviously i) holds in $(X, +, \cdot)$. For ii), let G be a definable subgroup with at least two elements. Obviously G is infinite. But G is finite or cofinite. Hence G is cofinite. Therefore $G = X$.

For iii), we first show that in $(C, +, \cdot)$, every definable linear ordering on a definable subset of C is finite. To see this, we have A is finite or cofinite. Suppose A is cofinite. By Lemma 0.2.14, there exists $a \in A$, such that $\{x: x < a\}$ and $\{x: x > a\}$ are infinite. This is impossible.

It then follows by the well known elementary equivalence of $(C, +, \cdot)$ and $(\text{CALG}, +, \cdot)$, that in $(\text{CALG}, +, \cdot)$, every definable linear ordering on a definable subset of CALG is finite.

To complete the verification of iii), let $f, A, <$ be as given. By the above, A is finite. It is clear by finite induction that every f_z is a polynomial. Polynomials in $(X, +, \cdot)$ are constant or onto because $(X, +, \cdot)$ is algebraically closed.

The result of applying π to a) is obviously provable in i-iii. For b), assume $dz = 0$, $z \neq 0$, and form the group $\{0, z, \dots, (d-1)z\}$. This group is definable in $(X, +, \cdot)$, and so by ii), it is $(X, +)$. This is a contradiction.

For c), let P be a polynomial of degree ≥ 1 with leading coefficient 1. Let Q_1, \dots, Q_n be polynomials, where each Q_i is either constant, the identity, or the sum or product of two Q_j , $j < i$, and where $Q_n = P$. Use $A = \{1, \dots, n\} \subseteq X$ with the usual $<$ to apply iii). Use $f: X^2 \rightarrow X$, where

$$f(z, w) = Q_z(w) \text{ if } z \in \{1, \dots, n\}; 0 \text{ otherwise.}$$

By iii), $Q_n = P$ is constant or onto. It remains to prove in i-iii that P is not constant.

Every model of i-iii is a field of characteristic zero. From algebra, in every field of characteristic zero, every

polynomial of degree ≥ 1 is not constant. By the Gödel completeness theorem, i-iii proves that P is not constant.

We have established that i-iii is an axiomatization of $(X, +, \cdot)$.

To see that $(X, <, \cdot)$ is not finitely axiomatizable, let p be a prime, and let F be the algebraically closed field of characteristic p . Then a-c hold in F . Also b) holds for $2 \leq d < p$. But b) fails for $d = p$. QED

THEOREM 0.2.16. $(\mathfrak{R}, <, +, \cdot)$, $(\text{RALG}, <, +, \cdot)$ are axiomatized with a single scheme by

- i. $(X, +, \cdot)$ is a field.
- ii. $<$ is a strict linear ordering.
- iii. $x < y \leftrightarrow y-x$ is a nonzero square.
- iv. Every definable nonempty set with an upper bound has a least upper bound.

$(\mathfrak{R}, +, \cdot)$, $(\text{RALG}, +, \cdot)$ are not finitely axiomatizable.

Proof: Clearly i-iv hold in $(\mathfrak{R}, <, +, \cdot)$, $(\text{RALG}, <, +, \cdot)$. Also $(\mathfrak{R}, <, +, \cdot)$, $(\text{RALG}, <, +, \cdot)$ are respective definitional extensions of $(\mathfrak{R}, +, \cdot)$, $(\text{RALG}, +, \cdot)$ by the interpretation π that defines

$x < y$ if and only if $y-x$ is a nonzero square.

So an axiomatization consists of the above definition of $<$, together with the axioms i-iii from Theorem 0.2.13. This axiomatization is equivalent to the present i-iv.

By Theorems 0.2.2, 0.2.13, $(\mathfrak{R}, +, \cdot)$, $(\text{RALG}, +, \cdot)$ are not finitely axiomatizable. QED

THEOREM 0.2.17. (\mathfrak{R}^2, B, E) is axiomatized with a single scheme. (\mathfrak{R}^2, B, E) is not finitely axiomatizable.

Proof: Tarski's axiomatization of Euclidean geometry uses B = betweenness, and E = equidistance, equality, and points, as the primitives. It has finitely many axioms together with an axiom scheme of continuity. See [Ta51], [TG99].

(\mathfrak{R}^2, B, E) is well known to be not finitely axiomatizable, using the $(K[p]^2, B, E)$, where $K[p]$ is as defined in the last paragraph of the proof of Theorem 0.2.13. By the axiomatization of real closed fields a-f there, we see that any finite set of sentences true in (\mathfrak{R}^2, B, E) is true in some $(K[p]^2, B, E)$. Furthermore, the existence of a p -th root

of 2 in \mathfrak{R} corresponds to a true statement in (\mathfrak{R}^2, B, E) that fails in $(K[p], B, E)$. Hence there cannot be a finite axiomatization of (\mathfrak{R}^2, B, E) . QED

We shall briefly mention three additional fundamental structures that have been investigated intensively.

The first is $(\mathfrak{R}, +, \cdot, e^x)$. It has been proved that every subset of \mathfrak{R} definable in $(\mathfrak{R}, +, \cdot, e^x)$ is a finite union of intervals with endpoints in $\mathfrak{R} \cup \{\pm\infty\}$. It is not known if $(\mathfrak{R}, +, \cdot, e^x)$ is recursively axiomatizable. However, it has been shown that if a famous conjecture in transcendental number theory, called the Schanuel Conjecture, is true, then $(\mathfrak{R}, +, \cdot, e^x)$ is recursively axiomatizable. See [MW96], [Wi96], [Wi99].

The second is the field $(\mathbb{Q}_p, +, \cdot)$ of all p-adic numbers and its finite algebraic extensions, where p is any given prime. See [AK65], [AK65a], [AK66], [Co69], [Eg98].

The third is the structure S2S. This is a two sorted structure $(\{0,1\}^*, \emptyset(\{0,1\}^*), \in, S_0, S_1)$, where S_0 and S_1 are the two successor functions on the set $\{0,1\}^*$ of finite bit strings defined by $S_0(x) = x0$, $S_1(x) = x1$. It is more common to present S2S, equivalently, either $(\{0,1\}^*, S_0, S_1)$, or $(T, <)$, where second order logic is used instead of the customary first order logic. Here T is the full binary tree viewed abstractly, with its usual partial order $<$.

A recursive axiomatization of S2S was first given using automata, in [Rab68]. For a modern treatment using game theory, see [BGG01], section 7.1.

It is often said that in "tame" contexts such as the ordered group of integers, or the ordered field of reals, we avoid the Gödel Incompleteness Phenomena.

However, the Gödel Incompleteness Phenomena simply shifts to the computational complexity context, where the results are based on diagonal constructions pioneered by Kurt Gödel. Even in these "tame" structures, one has the same kind of no algorithm results. One also has Gödelian type results involving lengths of proofs. We conjecture that there is a rich theory of Concrete Mathematical Incompleteness, involving lengths of proofs, in such "tame" contexts. See, e.g., [FR74], [Rab77], and [FeR79].

0.3. Abstract and Concrete Mathematical Incompleteness.

The focus of this book is on Concrete Mathematical Incompleteness. We use the following working definition of the Mathematically Concrete:

Mathematical statements concerning Borel measurable sets and functions of finite rank in and between complete separable metric spaces.

We take the Mathematically Abstract to begin with the transfinite levels of the Borel hierarchy, and continue in earnest with the low levels of the projective hierarchy of subsets of functions between complete metric spaces, starting with the analytic sets, followed by the higher levels of the projective hierarchy. Here there are still only continuumly many such subsets and functions.

Yet higher abstract levels include arbitrary subsets of and functions between complete separable metric spaces. Here there are more than continuumly many such subsets and functions. At still higher levels, the objects are no longer subsets or functions between complete separable metric spaces.

The overwhelming majority of mathematicians work within the Mathematically Concrete as defined above. In fact, the overwhelming majority work considerably below this level.

An indication of the special status of the functions and sets highlighted here is afforded by the following result, which is proved by standard techniques, and is part of the folklore of descriptive set theory.

THEOREM 0.3.1. Let X be a complete separable metric space. The following classes of functions from X into X are the same.

- i. The Borel measurable functions of finite rank from X to X .
- ii. The closure under composition of the pointwise limits of sequences of continuous functions from X to X .
- iii. The bold faced arithmetic functions from X into X in the sense of recursion theory.

This equivalence also holds for functions of several variables, using generalized composition in ii).

Clause ii) shows that we get to finite rank Borel by means of composition, and a family of reasonable discontinuous functions. Pointwise limits of continuous functions occur

in classical mathematics, particularly in connection with power series and Fourier series. Often these are not everywhere convergent, and we can use a default value where the limit does not exist. This is a variant of ii), for which Theorem 0.3.1 obviously still holds. One also sees functions defined as the sup of an infinite sequence of continuous functions, where we have uniform boundedness, or a point at infinity, so that the sups exist everywhere. This clearly falls under ii).

It would be very interesting to understand the closure under composition of special classes of functions, or the closure under composition of continuous functions with various specific simply presented discontinuous functions.

The highlight of this section is a discussion of various aspects of Concreteness in core mathematics, including levels of Concreteness. Many interesting issues arise, including a rather systematic program.

This systematic program, which we call Mathematical Statement Theory, is spelled out more carefully and applied to the Hilbert Problem List of 1900 in section 0.17.

A somewhat different, but well established program, which we founded in the late 1960's to mid 1970's, is Reverse Mathematics, and is discussed in detail in section 0.4.

We close this section with a brief history of Incompleteness, in which Abstract Mathematics plays a central role.

In order to proceed informatively and robustly, we will make free use of the standard analysis from logic of the quantifier complexity of formal sentences. The relevant standard robust categories of sentences from logic based on quantifier complexity are

$$\begin{array}{l} \Pi^0_0, \Pi^0_1, \dots . \\ \Sigma^0_0, \Sigma^0_1, \dots . \\ \Pi^1_0, \Pi^1_1, \dots . \\ \Sigma^1_0, \Sigma^1_1, \dots . \end{array}$$

Here Π^0_n (Σ^0_n) refers to sentences starting with n quantifiers ranging over \mathbb{N} , the first of which is universal (existential), followed by formulas using only bounded numerical quantifiers, connectives, and equations and

inequalities involving multivariate primitive recursive functions from N into N .

Also Π_n^1 (Σ_n^1) refers to sentences starting with n quantifiers ranging over subsets of N , the first of which is universal (existential), followed by a formula using only numerical quantifiers, connectives, equations and inequalities involving multivariate primitive recursive functions from N into N , and membership in subsets of N .

In practice, one normally encounters blocks of like quantifiers. It is a standard fact from mathematical logic that blocks of like quantifiers, in our context, behave like a single quantifier.

Since the languages on which these quantifier complexity classes are based are streamlined for logical simplicity, we make free use of the so called coding techniques from logic in order to actually gauge the strength of real mathematical statements. The appropriate robustness of the method of coding for such purposes is well established.

Another approach is to base the quantifier complexity classes on rich languages. This is less standard, and we will not take that approach here. The results obtained using this alternate approach would be essentially the same.

We do not use superscripts higher than 1 because any Mathematically Concrete assertion can be viewed as a Π_n^1 sentence, for some $n \geq 1$.

In fact, actual Mathematically Concrete assertions are often Π_3^0 or simpler. The quantifier complexity classes Π_1^0 , Π_2^0 , and Π_3^0 play very special roles at the concrete end of the spectrum.

The $\Pi_0^0 = \Sigma_0^0$ sentences have the special property that we can prove or refute them by running a computer - at least in principle. The computer resources needed may or may not be practical. A particularly interesting example of this is the proof of the Four Color Conjecture. The statement

existence of an unavoidable
finite set of reducible configurations

is a Σ_1^0 sentence because unavoidability and reducibility are local properties (unavoidability only involves graphs

of size related to the set). This Σ^0_1 sentence immediately implies the Four Color Conjecture. Appel and Haken gave an explicit instantiation of the outermost existential quantifier, and then proceeded to prove the resulting Π^0_0 sentence with the help of a computer.

The Π^0_1 sentences have the special property that if they are false, then we can find a counterexample and verify that it is a counterexample by computer - at least this can be done in principal. Obviously, any counterexample may be so huge that verifying it directly is impractical. Of course, the use of theory may make it practical even if the actual counterexample is so huge - by greatly reducing the actual computer resources.

A particularly well known example of a Π^0_1 sentence refuted by counterexample is Euler's Quartic Conjecture, which states that no fourth power of a positive integer is the sum of three fourth powers of positive integers. It was refuted in [El88] with

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Of course, here verifying that this is a counterexample barely requires a computer. Roger Frye subsequently found the counterexample

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

by a computer search using techniques suggested by Elkies, and demonstrated that this is the counterexample in fourth powers with smallest right hand side. Apparently, some theory is needed to obtain minimality. See [Gu94], p. 140. Note that Frye's minimality result is a $\Pi^0_0 = \Sigma^0_0$ sentence.

The category $\Pi^0_\infty = \cup_n \Pi^0_n$ also has special significance. This is the category of "arithmetic sentences". Many scholars feel that the integers and associated finite objects have a kind of objective existence that is not shared by arbitrary infinite objects such as an infinite sequence of integers. They often believe that statements involving only such finite objects - no matter how much quantification over all such finite objects are present - have a matter of factness that protects them from foundational issues in a way that statements involving infinite objects do not.

Some scholars have this kind of attitude towards only, say, Π^0_1 sentences. Others have varying degrees of cautiousness

about the matter of factness of even $\Pi^0_0 = \Sigma^0_0$ sentences, which can involve integers far too large for computer processing. For example, the number $A_{7198}(158,386)$, which arises in Theorem 0.7.11, or even an exponential stack of 100 2's.

We have the following noteworthy representatives.

Π^0_1 . Fermat's Last Theorem (Wiles' Theorem), Goldbach's Conjecture, the Riemann Hypothesis.

Π^0_2 . Collatz Conjecture.

Π^0_3 . Falting's Theorem (Mordell's Conjecture), Thue-Siegel-Roth Theorem.

Note that some of these statements are conjectures and some of these statements are theorems. There are a number of interesting issues related to these classifications above.

Consider the known FLT. It could be argued that FLT is in fact Π^0_0 , since it is known to be equivalent to $0 = 0$. However, that equivalence depends on some substantial portion of the new ideas in its proof. In fact, that equivalence relies on all of the new ideas in its proof!

So in this classification scheme applied to theorems, we must only use equivalence proofs that are orthogonal to the proof of the theorem. Perhaps surprisingly, in practice this requirement is sufficiently robust to support our classification scheme.

In section 0.17, we formulate Mathematical Statement Theory, where we are sensitive to such issues, so that this classification theory meaningfully applies to actual theorems.

FLT and Goldbach's Conjecture are obviously, on the face of it, Π^0_1 . One need go no further than consider their utterly standard formulations.

However, RH is quite a different matter. Looking at the standard formulation, we only obtain Π^1_1 , because of the quantification over all real numbers. This is hugely higher than any Π^0_n .

But there are well known concrete equivalences of RH. We present one of many well known Π^0_1 equivalences in section

0.17, when we discuss H8 = Hilbert's Eighth Problem. There is also a Π^0_1 equivalence of RH in [Mat93], Chapter 7. Hence RH is what we call essentially Π^0_1 .

The Collatz Conjecture is stated as follows. Define $f:Z^+ \rightarrow Z^+$ by $f(n) = n/2$ if n is even; $3n+1$ if n is odd. For all $n \in Z^+$, if we keep iterating f starting at n , then we eventually arrive at 1.

Note that the Collatz Conjecture takes the form

$$(\forall n \in Z^+) (\exists \text{ a finite sequence ending in 1, which starts with } n \text{ and continues by applying } f).$$

This can be put in Π^0_2 form using standard coding techniques from logic that rely on the fact that a finite sequence form Z^+ is a finite object of a basic kind.

Π^0_2 sentences practically beg to become Π^0_1 sentences through the use of an upper bound. Thus, if we could show, e.g., that

#) $(\forall n \in Z^+) (\exists \text{ a finite sequence ending in 1, which starts with } n \text{ and continues by applying } f, \text{ where all terms are at most } (8n)!!)$

without using ideas in the proof of Collatz Conjecture (at the moment we are not even close to being able to do this), then we would say that the Collatz Conjecture is essentially Π^0_1 .

Another possibility is that after we prove the Collatz Conjecture, we actually prove a stronger theorem that is Π^0_1 - such as #). In this case, we won't say that the Collatz Conjecture is, or is essentially, Π^0_1 , since we are relying on the proof of the Collatz Conjecture. But we would certainly want to note that

The Collatz Conjecture is implied by a Π^0_1 theorem.

Of course, another possibility is that we are able to prove the equivalence of the Collatz Conjecture with, say, #), without using ideas in the proof of the Collatz Conjecture - but in fact, historically, we only saw this after we proved the Collatz Conjecture. In this case, we would say that the Collatz Conjecture is essentially Π^0_1 .

Of course, independently of the discussion above, if we were to prove the equivalence of the Collatz Conjecture with #), we would have made a major contribution that would be readily recognized.

We now come to Falting's Theorem. This asserts that there are finitely many solutions to an effectively recognizable class of Diophantine problems over \mathbb{Q} . This takes the form

$$(\forall n) (\text{there are finitely many } m \text{ such that } P(n,m))$$

where P is an appropriate (primitive recursive) binary relation. Because of standard coding techniques, we can collapse several integers to a single integer for our purposes.

This in turn takes the form

$$(\forall n) (\exists r) (\forall m) (P(n,m) \rightarrow m < r)$$

which is obviously Π^0_3 . Note how this is significantly higher - i.e., less concrete - than Π^0_2 (Collatz Conjecture).

Π^0_3 sentences also practically beg to become Π^0_1 sentences through the use of an upper bound - just like Π^0_2 sentences.

Suppose we could show, e.g., that Mordell's Conjecture is equivalent to

$$\#\#) (\forall n) (\forall m) (P(n,m) \rightarrow m < (8n)!!)$$

without using ideas in the proof of Mordell's Conjecture (Falting's Theorem), then we would say that Mordell's Conjecture is essentially Π^0_1 .

Of course, independently of the discussion above, if we prove $\#\#)$ then we would have made a major contribution that would be readily recognized.

A situation quite analogous to Falting's Theorem, in this sense, is the Thue-Siegel-Roth Theorem. It states that if α is an irrational algebraic number, and $\varepsilon > 0$, the inequality

$$|\alpha - p/q| < 1/q^{2+\varepsilon}$$

has finitely many solutions in integers p and q . This is also in Π^0_3 for the same reason - and also begs to graduate to Π^0_1 .

We now jump to the upper reaches of the quantifier complexity classes that we are using. These most commonly appear as Π^1_1 , Π^1_2 , Σ^1_1 , Σ^1_2 .

This level of quantifier complexity has special significance for our purposes.

THEOREM 0.3.2. Let φ be a Π^1_2 or Σ^1_2 sentence. The main methods of set theory - inner models and forcing - cannot establish that φ is unprovable in ZFC. In particular, any two transitive models of ZFC with the same ordinals agree on the truth value of φ .

Theorem 0.3.2 essentially tells us that if a sentence is Π^1_2 or Σ^1_2 , then establishing its unprovability in ZFC requires something quite different than standard techniques from set theory. The only techniques available for establishing the unprovability in ZFC of mathematical sentences in these complexity classes are essentially those used for sections 0.13, 0.14, and laid out in detail in Chapters 4,5 of this book.

Furthermore, we claim that mathematics has, for many decades, been focused on problems that are well within the Π^1_2 and Σ^1_2 classes. This seems to be increasingly the case in recent years, particularly with the steady increase in the power of computation. The question "can you compute this" and "how efficiently can you compute this" have become more attractive now that many answers to the second question are actually implemented. This has inevitably affected the interest in the Concrete, even if one is still far removed from implementability.

It is still the case that you will see abstract mathematical statements from time to time considered by core mathematicians. The usual situation in which this arises is where the great generality is not causing its own inherent difficulties.

But if difficulties arise, traced to the generality and abstraction - not to the intended mathematical purposes - then interest wanes in the abstract formulation, and attention shifts to more concrete formulations where these "foreign" difficulties are absent.

This basically amounts to a kind of separation of the "set theoretic difficulties" from the "fundamental mathematical difficulties".

For instance, we still teach that every field has a unique (in the appropriate sense) algebraic closure. This is a highly abstract assertion, because the field is completely arbitrary. However, the set theoretic difficulties, which are not negligible, are highly manageable through Zorn's Lemma.

On the other hand, the highly abstract continuum hypothesis (discussed below under H1) is now well known to cause major difficulties disconnected from the normal issues in analysis.

Borel measurable sets and functions in separable metric spaces, lie at the outer cusp of what mathematicians generally accept as appropriate for the formulation of problems of genuine mathematical interest.

Thus the "Borel Continuum Hypothesis" arises, and is a rather basic and striking classical result in descriptive set theory. See [Ke95] and the discussion below in H1 of section 0.17.

Sometimes a highly abstract statement not only causes no logical difficulties, but it even is obviously equivalent to a much more concrete statement. See the discussion below in H14 of section 0.17.

These points are elaborated in some detail, as we discuss the levels of Concreteness associated with Hilbert's famous list of 23 problems, 1900, in section 0.17.

It appears that exactly one of the Hilbert problems lies outside Concrete Mathematics, according to our working definition above. This is H1, the first one in the list.

We conjecture that all of the other problems on this list, and all closely related problems, are

- i. Essentially Π^1_2 or essentially Σ^1_2 ; or
- ii. Will get proved or refuted in ZFC, and stronger statements will emerge from those proofs that are essentially Π^1_2 or essentially Σ^1_2 (and in most cases, much lower).

Two other problem lists, created one hundred years later, are the 18 Smale problems, 1998, and the 7 Clay Millennium Prize Problems, 2000. See [Sm00] and [<http://www.claymath.org/millennium/>].

We also conjecture that all of the problems on these other two lists, and all closely related problems, have properties i,ii above.

So what are we to make of this adequacy of the usual foundations of mathematics through ZFC with regard to these problem lists?

This matter is addressed in some detail in the Preface. Specifically, the development of mathematics is still extremely primitive on evolutionary - let alone cosmological - time scales. Although the scope of deep mathematical activity represented by these three lists of problems and the efforts leading up to them may look incredibly impressive to us, they are certain to look mundane in a few centuries (or even earlier), let alone in thousands (or millions!) of years.

We maintain that Boolean Relation Theory is just one of many subjects of gigantic scope (see section 1.2) that are yet to be discovered or developed, but which are entirely inevitable given their internal coherence, motivating themes, and simplicity of concept.

We believe that Concrete Mathematical Incompleteness - where large cardinals are shown to be sufficient, and weaker large cardinals are shown to be insufficient - will ultimately become commonplace.

What is much less clear is whether mathematicians will ultimately decide to accept large cardinal hypotheses, even under such utility. A major drawback of the large cardinal hypotheses in this regard is that they postulate objects that are radically foreign to mathematical practice.

It would seem more palatable to have forms of the large cardinal hypotheses involving objects that are least familiar to mathematicians, if not used generally in mathematical practice.

This is not possible in terms of literal equivalence. However, for applications of large cardinals such as the

ones in this book (the Exotic case), as well as any Π_2^0 consequence, an alternative is to use only the 1-consistency of the large cardinal hypotheses, and not the actual existence of the large cardinal. This opens the door to reformulations of large cardinal hypotheses in terms of familiar, or at least more familiar, objects.

One radical possibility along these lines is through the axiomatization of concepts that are entirely foreign to mathematics, but are, instead, a part of common everyday thinking. Plausible, or perhaps compelling, principles might be identified involving such concepts. Formal systems based on such principles may emerge, and imply the 1-consistency of the relevant large cardinal hypotheses. See [Fr06] and [Fr11] for work along these lines.

Another possibility is to directly analyze the mental pictures that are used to process large cardinals. Mental pictures are normally a crucial component in sophisticated mathematical reasoning, whether or not large cardinals are involved. They are a crucial component in the widespread acceptance of the usual ZFC axioms.

Moreover, mental movies are a particularly powerful component in mathematical reasoning, in the sense of short coherent sequences of mental pictures.

Mental pictures, and the more powerful mental movies, are combinatorial objects of very limited finite size.

The idea is to develop a combinatorial analysis of such finite movies, and discover some fundamental principles about them that imply the consistency or the 1-consistency of a range of large cardinal hypotheses.

We now close with a brief history of Incompleteness in which Abstract Mathematics plays a central role.

Let us review the initial stages of work on Incompleteness.

We can view Gödel's First Incompleteness Theorem as an existence theorem only, or we can view it as proving the independence of an arithmetization of the Liar's paradox. In either case, one cannot view it as providing an intelligible instance of mathematical incompleteness.

Gödel's Second Incompleteness Theorem does provide an important and intelligible example - e.g., $\text{Con}(\text{ZFC})$.

However, the intelligibility of $\text{Con}(\text{ZFC})$ depends on an understanding of "formalizations of abstract set theory".

One can object to this comment on the grounds that $\text{Con}(\text{ZFC})$ can be stated purely in terms of the ring of integers, or the hereditarily finite sets - using the standard coding devices. This "removes" the reference to abstract set theory and to formalizations.

However, when one removes the references to formalizations of abstract set theory, the presentation of $\text{Con}(\text{ZFC})$ becomes unintelligible - in particular, unintelligibly complex. This is a crucially important point, even though we do not have (yet) any kind of surrounding rigorous theory that formally supports important distinctions of this kind.

We are beginning to get a sense of definite criteria for judging the intelligibility or naturalness of mathematical statements. We believe that there are ways of judging intelligibility or mathematical naturalness that are independent of particular mathematical research interests or the sociology of mathematics. This topic lies well beyond the scope of this book.

The next big development in Incompleteness involved two obviously important problems in abstract set theory - the first implicitly used by Cantor, and the second emphasized by Cantor. These were the axiom of choice, and the continuum hypothesis. The consistency of $\text{ZFC} + \text{CH}$ relative to ZF was established in [Go38]. The consistency of $\text{ZF} + \neg\text{AxC}$, and $\text{ZFC} + \neg\text{CH}$, relative to ZF , was later established in [Co63,64].

Note that here there is no reference to formalizations of abstract set theory. AxC and CH are problems directly in abstract set theory.

However, AxC and CH are not concrete - in anything like the way that $\text{Con}(\text{ZFC})$ is.

$\text{Con}(\text{ZFC})$ is formulated in terms of finite objects only. It asserts the nonexistence of a finite configuration. Its intelligibility depends on some understanding of abstract set theory. But nevertheless, with the help of coding, it asserts the nonexistence of a finite configuration.

In contrast, AxC and CH cannot be formulated in this way,

regardless of coding devices. These statements live inherently in the abstract set theoretic universe.

Subsequent developments in Incompleteness initially centered around analyzing a large backlog of problems from abstract set theory, mostly with the help of Cohen's method of forcing introduced in [Co63,64]. Some of the problems in this backlog were well known from the set theoretic parts of analysis, group theory, and other subjects. Early pioneers in this extensive development include Donald Martin, Saharon Shelah, Robert Solovay, and others. See [Je78,06] for a comprehensive treatment.

A notably different method of attack on Abstract Incompleteness arose from Ronald Jensen's work on Gödel's constructible universe, which provides tools for establishing that various statements hold in L (Gödel's constructible universe). This establishes relative consistency with ZFC, where the independence is normally established by forcing. E.g., see [Jen72], [De84].

These applications of forcing and constructible sets established that ZFC neither proved nor refuted many problems in Abstract Mathematics, but generally did not determine or even shed light on their truth or falsity, from the abstract set theoretic point of view.

Work on the projective hierarchy of sets of reals took hold, forming an entry point for large cardinals in Incompleteness.

The projective hierarchy begins with Borel and analytic sets (analytic sets are projections of Borel sets), and forms a hierarchy indexed by the natural numbers.

Classical analysts from the first half of the twentieth century sought to extend their impressive understanding of the structure of Borel and analytic sets to the more general projective sets.

During the 1960s and 1970s, it was discovered that projective determinacy implies all of these sought after generalizations to projective.

Large cardinal hypotheses were shown to imply projective determinacy in [MSt89]. Specifically, Martin and Steel proved in ZFC that if there are infinitely many Woodin cardinals then projective determinacy holds. In addition,

projective determinacy establishes all of the generalizations

Woodin has proved in ZFC that if there are infinitely many Woodin cardinals below a measurable cardinal, then $L(\mathfrak{R})$ determinacy holds, extending the work of Martin and Steel. See [St09], [Lar04]. These results are shown to be roughly optimal. For a detailed account, see [KW10]. (Here $L(\mathfrak{R})$ is the constructible closure of \mathfrak{R} , and $L(\mathfrak{R})$ determinacy asserts that in all infinite length games with integer moves and winning set in the constructible closure of \mathfrak{R} , one player has a winning strategy).

For a much more detailed picture of set theoretic incompleteness, see [Je78,06].

We close with a brief account of an important development initiated by Richard Laver, taken from [DJ97].

In [La92], properties of the free left-distributive algebra on one generator are proved using an extremely large cardinal - a nontrivial elementary embedding from some $V(\lambda)$ into $V(\lambda)$. These consequences included the recursive solvability of the word problem for this algebra.

These algebraic results were later proved in [Deh94], [Deh00] using completely different methods based on braid groups and generalizations thereof. The new proofs use only very weak fragments of ZFC, and in fact weak fragments of PA.

But some further algebraic results were obtained using the large cardinal. [La95] produces a sequence of finite left-distributive algebras A_n , which can be constructed in simple combinatorial terms without the large cardinal. [La95] proves that A_∞ is also free.

" A_∞ is free" can be rephrased in purely algebraic form, as a Π^0_2 sentence asserting that certain equations do not imply certain other equations under the left distributive law.

In [DJ97a], it is shown that " A_∞ is free" is not provable in PRA (primitive recursive arithmetic). At present, the only proof of " A_∞ is free" uses the extremely large cardinal.

Even if (as many expect) the large cardinal is subsequently removed, this does show how large cardinals can provide insights into Concrete Mathematics.

But here we give an application of large cardinals to combinatorics that is proved in Chapter 4 from large cardinals, and shown to be necessary (unremoveable) in Chapter 5.

In fact, we believe that in the future, large cardinals will be systematically used for a wide variety of Concrete Mathematics in an essential, unremoveable, way.

0.4. Reverse Mathematics.

The ZFC axioms (Zermelo Frankel with the axiom of choice) have served for nearly a century as the de facto standard by which we judge whether a mathematical theorem has been proved.

Early on, it was clear that ZFC serves as convenient overkill for this purpose. Mathematical results generally require use of only a "small part" of the power of the ZFC axioms.

Interest naturally developed in determining which fragments of ZFC are sufficient to prove which specific theorems.

In order to systematize this work in an informative way, a collection of standard fragments of ZFC are needed. This turns out to be rather awkward given the way the axioms of ZFC are laid out.

The advantages of working with the pair of primitives, natural numbers and sets of natural numbers (or natural numbers, and the closely related alternative choice of functions from natural numbers into natural numbers), became apparent, both for proof theory and for the logical analysis of mathematical theorems. See [Kre68], [Fe64], [Fe70].

Thus Feferman, Kreisel, and others, began to use the system Z_2 and its fragments for the purpose of identifying logical principles sufficient to prove various mathematical theorems.

Reverse Mathematics (RM) is an open ended project in which a wide range of mathematical theorems are systematically classified in terms of the "minimum" logical principles sufficient to prove them.

After RM was founded through [Fr74], [Fr75-76], and [Fr76], S. Simpson focused on the area, made important advances in RM, supervised many Ph.D. students in RM, and wrote the authoritative book [Si99,09] covering RM.

But how can we identify the "minimum" logical principles sufficient to prove a given mathematical theorem?

Our key insight goes back to at least 1969 (cited in [Fr75-76]), and culminated in the polished formulations of [Fr74], [Fr76].

We first identify a weak "base theory" T of core fundamental principles, in the form of a subsystem of Z_2 .

We then realize through experimentation with examples, that the base theory is strong enough so that the equivalence relation

base theory T proves A is equivalent to B

on basic mathematical theorems, has relatively few equivalence classes.

These insights already supported a robust theory of "logical strength" of mathematical theorems, although the phrase "logical strength" now has a more focused meaning. See the DEEP UNEXPLAINED OBSERVED FACT below.

We went further and identified natural preferred logical systems associated with the various equivalence classes of mathematical theorems that arise.

We identified a group of natural fragments of Z_2 such that many mathematical theorems correspond exactly to one of these fragments in the sense that

base theory T proves that theorem A is
equivalent to the formal system S

so that theorem A is calibrated by the system S .

Note that under this conception, we have both the usual

proving of mathematical theorems from formal systems

and the unusual

proving of formal systems from mathematical theorems
(over the base theory).

Hence we introduced the name "reverse mathematics" for this classification project.

Our choice of base theory for RM underwent some evolution, culminating with RCA in [Fr74] and the improved, weaker, finitely axiomatized RCA_0 in [Fr76]. The choice of RCA_0 has remained the working standard for RM since that time.

In [Fr75-76], one of our earliest results is cited in these terms:

"1. In 1969 I discovered that a certain subsystem of second order arithmetic based on a mathematical statement (that every perfect [sic] tree that does not have at most countably many paths, has a perfect subtree) was provably equivalent to a logical principle (the weak Π^1_1 axiom of choice) modulo a weak base theory (comprehension for arithmetic formulae)."

The use of the first "perfect" here was an apparent typographical error, and should be struck out here [sic].

Already in [Fr74], [Fr76], we used the system ATR_0 for that level instead of the weak Π^1_1 axiom of choice.

But note that our use of arithmetic comprehension as the base theory, at least for this early reversal from 1969. This is what appears as ACA in [Fr74] - but not as the base theory.

Our choice of base theory in [Fr74] is the much weaker RCA = recursive comprehension axiom scheme, which has full induction in its language (the language of Z_2). We subsequently sharply weakened the induction axiom to what is really essential, resulting in the base theory RCA_0 of [Fr76].

The most commonly occurring systems of RM were first introduced as a group (with some additional systems) in [Fr74]. These are

RCA, WKL, ACA, ATR, Π^1_1 -CA

and were later weakened, in [Fr76], to the finitely axiomatized systems

$$\text{RCA}_0, \text{WKL}_0, \text{ACA}_0, \text{ATR}_0, \Pi^1_1\text{-CA}_0$$

by limiting the induction axioms to what is essential. Many reversals of some basic mathematical theorems are also presented in [Fr74] and [Fr76].

Two additional levels are also introduced in [Fr74] and [Fr76]. These levels had figured prominently in earlier investigations of fragments of Z_2 . These are the closely related

$$\text{HCA}, \text{HAC}, \text{HDC}, \text{and } \text{HCA}_0, \text{HAC}_0, \text{HDC}_0$$

of hyperarithmetical comprehension, choice, dependent choice, better known as

$$\Delta^1_1\text{-CA}, \Sigma^1_1\text{-AC}, \Sigma^1_1\text{-DC}, \Delta^1_1\text{-CA}_0, \Sigma^1_1\text{-AC}_0, \Sigma^1_1\text{-DC}_0$$

and the system TI of transfinite induction, better known as BI (bar induction of lowest type).

All of these systems above, starting with RCA, that are based on full induction (i.e., without the naught), figured prominently in earlier work on fragments of Z_2 by S. Feferman and G. Kreisel and others. Their main motivation was proof theoretic. The development of the naught systems with restricted induction serves the particular needs of Reverse Mathematics.

The hyperarithmetical systems above have not played an important role in RM until recently. But now see [Mo06], [Mo ∞], [Ne09], [Ne ∞ 1], [Ne ∞ 2].

TI, or at least significant fragments of TI, have figured importantly in the metamathematics of Kruskal's theorem. For example,

$$\text{RCA}_0 + \text{Kruskal's theorem for wqo labels} \\ \text{with bounded valence;}$$

and

$$\text{the theory } \Pi^1_2\text{-TI}_0$$

prove the same Π^1_1 sentences. See [RW93] and [Fr84].

In the development of RM, many systems have arisen beyond

the most frequently occurring ones discussed above. In the main Chapters of this book alone, which is not focused on RM, the systems ACA' and ACA⁺ arise (Definitions 1.4.1, 6.2.1). In [Si99,09], we find, additionally, Σ^1_1 -IND, Π^1_1 -TR₀, Σ^1_1 -TI₀, and WWKL₀.

Incomparability under provability does naturally arise in Reverse Mathematics. A particularly clear example, that involves only modest amounts of coding, is as follows. Consider

- i. Every ideal in the polynomial ring in n variables over any finite field is finitely generated.
- ii. Every infinite tree of finite sequences of 0's and 1's has an infinite path.

In [Si88], it is shown that i) above is provably equivalent to " ω^ω is well ordered" over RCA₀. WKL₀ is RCA₀ + ii).

Now RCA₀ + " ω^ω is well ordered" does not imply WKL₀ since the former has the ω model consisting of the recursive subsets of ω , whereas this does not form a model of WKL₀.

Also, WKL₀ does not imply RCA₀ + " ω^ω is well ordered" since the ordinal, in the sense of proof theory, of WKL₀ is ω^ω , whereas the ordinal of the former is considerably higher. See [Si99,09], p. 391.

The systems that arise above form a hierarchy - but not in the sense of being linearly ordered under provability. Instead, we have linearity under interpretability. Moreover, we expect that as the range of systems used in RM expands from the analysis more and more mathematical theorems, we will maintain this linearity under interpretability.

We summarize this observed phenomena as follows.

DEEP UNEXPLAINED OBSERVED FACT. For any two naturally occurring mathematical theorems A, B, naturally formulated in the language of RM, either RCA₀ + A is interpretable in RCA₀ + B, or RCA₀ + B is interpretable in RCA₀ + A.

This phenomenon also holds in wide ranging contexts, including in set theories, provided a suitable base theory is chosen.

This phenomenon begs for an explanation. At present, there isn't any. Theoretically, lots of incomparability arise under interpretability. See [Fr07], Lecture 1.

In light of this observed comparability, the phrase "logical strength" for formal systems has come to mean "interpretation power". Sometimes it also means "consistency strength". We have shown that interpretation power and consistency strength are equivalent, in a certain precise sense. See [Fr80a], [Smo84], [Vi90], [Vi92], [Vi09], [FVxx].

The principal theme of [Fr75-76] is actually a criticism of the use of fragments of Z_2 for RM. Our idea was that the language of Z_2 is far too impoverished to adequately represent mathematical statements. We categorically rejected the use of coding, which is generally required for formalization within Z_2 .

Nevertheless, we quickly came to realize that there were just too many unresolved issues involved in setting up a coding free RM. We chose not to publish the approach of [Fr75-76] (although we circulated those manuscripts widely), but rather focus initially on the more straightforward approach of [Fr74], [Fr76], initiating the Reverse Mathematics program.

The setup in [Fr76] is a compromise. It uses variables over \mathbb{N} and variables over unary, binary, and ternary functions from ω into ω , with the numerical constant 0 and a unary function constant for successor.

The system ETF - elementary theory of functions - is then formulated in this language, which is equivalent to the now standard RCA_0 (adapted in the obvious way to the language of ETF). Note that ETF avoids any use of axiom schemes, or reliance in any way on formulas with bounded quantifiers.

As we expected, these subtle issues were put aside by the community, and the much more manageable version of RM using RCA_0 was pursued using the standard coding apparatus used for many years in recursion theory.

In particular, the normal presentation of RCA_0 is simply the axioms for RCA that we gave in [Fr74], with the Induction Axiom Scheme replaced by the weaker Σ^0_1 Induction Axiom Scheme. E.g., see [Si99,09], Definition II.1.5. We preferred the equivalent formulation of ETF.

Our deep interest in coding free RM was, in retrospect, premature. Any reasonably stated equivalent form of RCA_0 was adequate to drive the subsequent development of RM.

Recently, we have come back to the development of coding free RM under the banner of SRM = Strict Reverse Mathematics. Our initial publication on SRM has appeared in [Fr09]. Also see the abstract [Fr09a].

This initial development of SRM is focused on arithmetic (integers and finite sets and finite sequences of integers), and provides strictly mathematical assertions that generate the bounded induction scheme. Integer exponentiation is also investigated in this context, both as an additional principle, and as a derived construction (geometric progressions).

Thus SRM can suitably operate with robustness at a level considerably lower than RCA_0 . This promises to refine the reverse mathematics idea to analyze the considerable range of interesting mathematics that is already provable in RCA_0 when suitably formalized.

An intermediate approach is to weaken the base theory RCA_0 to RCA_0^* . Here we drop Σ^0_1 induction in favor of the weaker Σ^0_0 induction. See [Si99,09], p. 410-411.

We believe that SRM (strict reverse mathematics), which aims to remove coding entirely, is the appropriate vehicle for greatly expanding the scope of RM.

For the convenience of the reader, we now present the axioms of our now standard RM systems RCA_0 , WKL_0 , ACA_0 , ATR_0 , and Π^1_1 - CA_0 . Of course, these are entirely unsuitable for our new SRM.

The language is two sorted, with variables over natural numbers and variables over subsets of N . We use $0, S, +, \cdot, <, =$ on sort N , and \in between natural numbers and sets of natural numbers.

A formula is Σ^0_1 (Π^0_1) if it begins with an existential (universal) numerical quantifier, and is followed by a formula with only bounded quantifiers (using $<$).

A formula is Π^1_1 if it begins with a universal set quantifier, followed by a formula with no set quantifiers.

The axioms of RCA_0 are

- i. Basics. $\neg S(n) = 0$, $S(n) = S(m) \rightarrow n = m$, $n + 0 = n$, $n + S(m) = S(n + m)$, $n \cdot 0 = 0$, $n \cdot S(m) = (n \cdot m) + n$. $n < m \leftrightarrow (\exists r)(n + S(r) = m)$.
- ii. Σ^0_1 induction. $\varphi[n/0] \wedge (\forall n)(\varphi \rightarrow \varphi[n/S(n)]) \rightarrow \varphi$, where φ is Σ^0_1 .
- iii. Δ^0_1 comprehension. $(\forall n)(\varphi \leftrightarrow \psi) \rightarrow (\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ is Σ^0_1 , ψ is Π^0_1 , and A is not free in φ .

The axioms of WKL_0 are RCA_0 together with "every infinite tree of finite sequences of 0's and 1's has an infinite path" suitably coded in RCA_0 .

The axioms of ACA_0 are

- i. Basics. See RCA_0 .
- ii. Set induction. $0 \in A \wedge (\forall n)(n \in A \rightarrow S(n) \in A) \rightarrow n \in A$.
- iii. Arithmetic comprehension. $(\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ has no set quantifiers, and A is not in φ .

The axioms of ATR_0 are ACA_0 together with "transfinite recursion can be performed along any well ordering using any arithmetic formula" suitably coded in ACA_0 .

The axioms of Π^1_1 - CA_0 are

- i. Basics. See RCA_0 .
- ii. Set induction. See ACA_0 .
- iii. Π^1_1 comprehension. $(\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ is Π^1_1 , and A is not free in φ .

0.5. Incompleteness in Exponential Function Arithmetic.

Exponential Function Arithmetic, or EFA, is a fragment of Peano Arithmetic (PA) that we explicitly named, identified, and used, in [Fr78], p. 2, and continue to use in [Fr78], p. 23, [Fr79], p. 6, [Fr80a], p. 2, to this day.

The language of PA consists of $0, S, +, \cdot, =$. The axioms of PA are

1. $\neg Sx = 0$, $Sx = Sy \rightarrow x = y$.
2. $x + 0 = x$, $x + Sy = S(x + y)$.
3. $x \cdot 0 = 0$, $x \cdot Sy = (x \cdot y) + x$.
4. Induction for all formulas in the language of PA.

The language of EFA consists of $0, S, +, \cdot, 2^{\wedge}, \leq, =$. The axioms of EFA are

1. The axioms of Q . (See section 0.1A).
2. $2^{\wedge}0 = 1$, $2^{\wedge}Sy = 2^{\wedge}y + 2^{\wedge}y$.
3. Induction for all bounded formulas in the language of EFA.

In bounded formulas, all quantifiers must be bounded (\leq) to terms not mentioning the variable being bounded.

Technically speaking, EFA is not a fragment of PA since its language is not even a fragment of the language of PA. However, PA is a definitional extension of EFA whose symbols of PA are unmodified.

We focused on EFA long ago because it is the most obvious natural weak fragment of PA for which finite sequence coding provably behaves as expected.

EFA is called EA, or elementary arithmetic, in [Av03], where a major conjecture of mine is discussed in great detail. He writes

"From the point of view of finitary number theory and combinatorics, EA turns out to be surprisingly robust. So much so that Harvey Friedman has made the following Grand conjecture: Every theorem published in the Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., what logicians call an arithmetical statement) can be proved in elementary arithmetic."

A special case of this conjecture is that Fermat's Last Theorem is provable in EFA. However, we are a long way from establishing this, although there is an attack on showing that FLT is provable in PA (see [Mac11]). However, [Mac11] explicitly denies confidence that FLT is provable in EFA. Also see [Mc10].

EFA is essentially identical to what is now called $I\Sigma_0(\text{exp})$ (see [HP93]). It is synonymous with $I\Sigma_0 + \text{exp}$. EFA is more convenient than $I\Sigma_0 + \text{exp}$, in the sense that in order to formulate the latter, we need a suitable formalization of exp in $I\Sigma_0$ - which is cumbersome.

EFA is known to be finitely axiomatizable. This is credited

to J. Paris (see [HP93], p. 366).

We are unaware of any presentation of EFA earlier than our [Fr78]. The system $I\Sigma_0 = I\Delta_0$ = bounded arithmetic (which we like to call PFA for polynomial function arithmetic), was introduced much earlier in [Pa71]. Here PFA is Q is extended with the Δ_0 induction scheme. It is open whether PFA is finitely axiomatizable. This question has been seen to be related to issues in computational complexity theory (see [HP93]).

Here is the key property of EFA that is behind the incompleteness from EFA that we discuss.

We write $2^{[y]}(x)$ for $2^{\dots^2^x}$, where there are y 2's. We take $2^{[0]}(x) = x$.

THEOREM 0.5.1. Suppose EFA proves a sentence of the form $(\forall x_1, \dots, x_n)(\exists y_1, \dots, y_m)(\varphi)$, where φ is bounded. There exists r such that $(\forall x_1, \dots, x_n)(\exists y_1, \dots, y_m < 2^{[r]}(\max(x_1, \dots, x_n)))(\varphi)$. Furthermore, there exists r such that EFA proves $(\forall x_1, \dots, x_n)(\exists y_1, \dots, y_m < 2^{[r]}(\max(x_1, \dots, x_n)))(\varphi)$.

This is an instance of what is known as Parikh's theorem. See [HP93], Theorem 1.4, p. 272.

The best known example of a finite theorem that is not provable in EFA but is provable just beyond EFA, is the ordinary finite Ramsey theorem. We give two standard forms of this theorem.

FINITE RAMSEY THEOREM 1. For all $k, p, r \geq 1$ there exists n so large that the following holds. In any coloring of the unordered k tuples from $\{1, \dots, n\}$ using p colors, there is an r element subset of $\{1, \dots, n\}$ whose unordered k tuples have the same color.

FINITE RAMSEY THEOREM 2. For all $k, p, r \geq 1$ there exists n so large that the following holds. For all $f: \{1, \dots, n\}^k \rightarrow \{1, \dots, p\}$, there exists $S \subseteq \{1, \dots, n\}$ of cardinality r , such that for any $x, y \in S^k$ of the same order type, $f(x) = f(y)$.

These two formulations are easily proved to be equivalent in EFA.

There has been considerable work on upper and lower bounds

for these statements. For our purposes, we need only the following.

Let $R_k(l)$ be the least n such that the following holds. In any coloring of the unordered k tuples from $\{1, \dots, n\}$ using 2 colors, there is an l element subset of $\{1, \dots, n\}$ whose unordered k tuples have the same color.

THEOREM 0.5.2. For all $k \geq 4$, there is a constant c_k , such that the following holds. For all $l \geq 1$, $R_k(l) \geq 2^{\lfloor k-2 \rfloor (c_k l^2)}$.

For a proof of Theorem 0.5.2, see [GRS80], p. 91-93.

There is ongoing work on sharper estimates of such higher Ramsey numbers of various kinds. For example, see [CFS10].

By Theorems 0.5.1 and 0.5.2, we obtain

COROLLARY 0.5.3. The Finite Ramsey Theorem, even for 2 colors, is not provable in EFA.

The status of the Finite Ramsey Theorem over EFA is completely known. It is given by a so called reversal (as in reverse mathematics).

Consider the statement

$$(\forall n) (2^{[n]} \text{ exists}).$$

This can be formalized in EFA as follows. For all n , there is a (coded) finite sequence with n terms, starting with 1, where each term is the base 2 exponential of the previous term. It is immediate from Theorem 0.5.1 that this sentence is not provable in EFA.

We also consider the following obvious generalization.

$$(\forall n, m) (n^{[m]} \text{ exists}).$$

THEOREM 0.5.4. EFA proves the equivalence of the following.

- i. Finite Ramsey Theorem.
- ii. Finite Ramsey Theorem for $p = 2$.
- iii. $(\forall n) (2^{[n]} \text{ exists})$.
- iv. $(\forall n, m) (n^{[m]} \text{ exists})$.

$n^{[m]}$ is often referred to as the superexponential. Accordingly, we can define the system SEFA =

superexponential function arithmetic, as follows.

The language of SEFA consists of $0, S, +, \cdot, 2^{\wedge}, 2^{\wedge\wedge}, \leq$. The axioms of SEFA are

1. The axioms of EFA.
2. $2^{\wedge\wedge 0} = 1, 2^{\wedge\wedge S y} = 2^{\wedge}(2^{\wedge\wedge y})$.
3. Induction for all bounded formulas in the language of SEFA.

SEFA has the finite sequence coding of EFA. This can be used to treat the obvious generalization, $n^{\wedge m}$.

THEOREM 0.5.5. SEFA proves the Finite Ramsey Theorem. SEFA and EFA + $(\forall n) (2^{[n]} \text{ exists})$ prove the same sentences from $L(\text{EFA})$.

There is a very attractive weakening of the Finite Ramsey Theorem, which we call the Adjacent Ramsey Theorem.

THEOREM 0.5.6. Adjacent Ramsey Theorem. For all $k, p \geq 1$ there exists t so large that the following holds. For all $f: \{1, \dots, t\}^k \rightarrow \{1, \dots, p\}$, there exist $1 \leq x_1 < \dots < x_{k+1} \leq t$ such that $f(x_1, \dots, x_k) = f(x_2, \dots, x_{k+1})$.

We have shown that this behaves like the Finite Ramsey Theorem. We have also shown that for $p = 2$, we can set $t = 2k+1$. [Fr08], [Fr10a].

THEOREM 0.5.7. EFA proves the equivalence of the following.

- i. Adjacent Ramsey Theorem.
- ii. $(\forall n) (2^{[n]} \text{ exists})$.
- iii. $(\forall n, m) (n^{[m]} \text{ exists})$.

We became aware of work that is pretty close to the Adjacent Ramsey Theorem, again with iterated exponential lower bounds - that predates our work. See [DLR95].

A sketch of our work appears in [Fr99b], [Fr10a]. A full self contained manuscript will appear elsewhere.

0.6. Incompleteness in Primitive Recursive Arithmetic, Single Quantifier Arithmetic, RCA_0 , and WKL_0 .

This level of incompleteness is unusually rich, and we organize the discussion as follows.

0.6A. Preliminaries.

- 0.6B. Sequences of Vectors.
- 0.6C. Walks in N^k .
- 0.6D. Hilbert's Basis Theorem.
- 0.6E. Sequences of Algebraic Sets.
- 0.6F. Relatively Large Ramsey Theorem for Pairs.

0.6A. Preliminaries.

PRA (primitive recursive arithmetic), $I\Sigma_1$ (single quantifier arithmetic), RCA_0 (our base theory for Reverse Mathematics), and WKL_0 (another of our theories for Reverse Mathematics), are well known systems that represent the same "level", in a sense made explicit below.

PA = Peano arithmetic, is most commonly formulated in the language $0, S, +, \cdot, =$, with the following axioms.

1. $\neg Sx = 0$.
2. $Sx = Sy \rightarrow x = y$.
3. $x+0 = x$, $x+Sy = S(x+y)$.
4. $x \cdot 0 = 0$, $x \cdot Sy = x \cdot y + x$.
5. Induction for all formulas in $L(PA)$.

The Σ_n (Π_n) formulas are the formulas which begin with an existential (universal) quantifier, followed by at most $n-1$ quantifiers, followed by a bounded formula.

$I\Sigma_n$ ($I\Pi_n$) denotes the fragment of PA based on induction for Σ_n (Π_n) formulas.

There is a fair amount of robustness here. For instance, we can allow blocks of like quantifiers in the definition of Σ_n , (Π_n) and we get the same fragments of PA.

It is well known that for $n \geq 1$, $I\Sigma_n$ and $I\Pi_n$ are equivalent. See [HP93], p. 63.

By single quantifier arithmetic, we will mean $I\Sigma_1 \cup I\Pi_1$, which is equivalent to $I\Sigma_1$.

Another important system is PRA = primitive recursive arithmetic. The language of PRA includes $0, S$, and symbols for every primitive recursive function (the primitive recursive function symbols). The axioms of PRA are as follows.

1. $\neg Sx = 0$.
2. $Sx = Sy \rightarrow x = y$.

3. The primitive recursive defining equations.
4. Induction for all quantifier free formulas of PRA.

Some authors work with a quantifier free version of PRA. See, e.g., [Min73].

The systems RCA_0 and WKL_0 are from Reverse Mathematics. See [Fr74], [Fr76], [Si99,09], and the end of section 0.4.

We will use the following proof theoretic information about the systems PRA, $I\Sigma_1$, RCA_0 , and WKL_0 .

THEOREM 0.6A.1. PRA proves induction for all bounded formulas of PRA. WKL_0 proves RCA_0 proves $I\Sigma_1$ proves PRA. The implications are strict. $I\Sigma_1$, RCA_0 , WKL_0 prove the same arithmetic sentences. $I\Sigma_1$, PRA prove the same Π^0_2 sentences. $I\Sigma_1$ and RCA_0 prove the same arithmetic sentences. RCA_0 and WKL_0 prove the same Π^1_1 sentences. These results are provable in SEFA. If we remove the second "PRA", then these results are provable in EFA.

For proofs, see [Si99,09], Corollary IX.1.11, Corollary IX.2.7, and Theorem IX.3.16. The proof of the fifth claim, involving $I\Sigma_1$ and PRA, is model theoretic, not formalizable in weak fragments of arithmetic. However, it has been proved in SEFA. See the last paragraph before section 0.1.

Recall that bounded quantifiers are allowed after the unbounded existential quantifier in Π^0_2 formulas. In Π^1_1 sentences, we start with one universal set quantifier, followed by an arithmetic formula.

We also need the following relationship between RCA_0 , WKL_0 , and the ordinal ω^ω .

THEOREM 0.6A.2. Let T be a primitive recursively given finite sequence tree. If RCA_0 proves that T is well founded, then there exists $n \in \mathbb{N}$ and a primitive recursive function h such that RCA_0 proves that h is a map from vertices of T into notations $< \omega^n$, such that if v' extends v in T , then $h(v') < h(v)$. The same holds for WKL_0 . These results are provable in SEFA.

Proof: This can be established through the use of $I\Sigma_1(F)$, which is $I\Sigma_1$ extended by a single unary function symbol F . The induction allows use of F . This system has a natural proof theoretic analysis. The last claim follows from the

fact that WKL_0 and RCA_0 prove the same Π^1_1 sentences, due to L. Harrington. See [Si99,09], p. 372. QED

We note that the h in Theorem 0.6A.2 can be chosen to be elementary recursive by an observation in [Ara98].

We define the strict Π^1_1 sentences to be sentences asserting the well foundedness of a particular primitive recursively given finite sequence tree.

We obtain the following from Theorem 0.6A.2.

THEOREM 0.6A.3. The following are provably equivalent in RCA_0 .

- i. Every strict Π^1_1 sentence provable in RCA_0 is true.
- ii. Every strict Π^1_1 sentence provable in WKL_0 is true.
- iii. ω^ω is well ordered.

THEOREM 0.6A.4. Suppose PRA proves a sentence $(\forall x_1, \dots, x_n)(\exists y_1, \dots, y_m)(\varphi)$, where φ is bounded. There is a primitive recursive function f such that $(\forall x_1, \dots, x_n)(\exists y_1, \dots, y_m < f(x_1, \dots, x_n))(\varphi)$. Furthermore, there are primitive recursive function symbols F_1, \dots, F_m such that PRA proves $\varphi(x_1, \dots, x_n, F_1(x_1, \dots, x_n), \dots, F_m(x_1, \dots, x_n))$. The same is true of $I\Sigma_1$, RCA_0 , and WKL_0 . These results are provable in SEFA.

Proof: Since PRA has a universal axiomatization, we can obtain this using Herbrand's theorem (in a sharper form, with $<$ replaced by $=$). Or we can apply Parikh's theorem to each finite fragment of PRA. See [HP93], Theorem 1.4, p. 272, and [Sie91]. QED

Note that Theorems 0.6A.1 and 0.6A.4 are closely related. They are used in the same way. Thus, if a Π^0_2 sentence has an associated growth rate higher than all primitive recursive functions, then we know that it is not provable in PRA, or even WKL_0 , by Theorem 0.6A.4.

0.6B. Sequences of Vectors.

We now consider termination of lexicographic descent in the natural numbers.

For $k \geq 1$, $x, y \in \mathbb{N}^k$, write $x <_{\text{lex}} y$ if and only if at the first coordinate at which x, y differ, x is less than y .

THEOREM 0.6B.1. Every sequence from \mathbb{N}^k that is decreasing in

the lex ordering terminates.

Note that Theorem 0.6B.1 is a strict Π^1_1 sentence. Its status is well known over the base theory, RCA_0 , of reverse mathematics.

THEOREM 0.6B.2. For each fixed k , Theorem 0.6B.1 is provable in RCA_0 . The following are provably equivalent in RCA_0 .

- i. Theorem 0.6B.1.
- ii. ω^ω is well ordered.

Theorem 0.6B.2 follows from the identification of each ω^k with the lexicographic ordering on \mathbb{N}^k . Use the straightforward provability in RCA_0 of $(\forall k)(\omega^k \text{ is well ordered} \rightarrow \omega^{k+1} \text{ is well ordered})$.

There is an important sharper form of Theorem 0.6B.1. For $x, y \in \mathbb{N}^k$, write $x \leq_c y$ if and only if for all i , $x_i \leq y_i$. Here "c" means "coordinatewise".

THEOREM 0.6B.3. Every infinite sequence from \mathbb{N}^k has a finite initial segment such that every term is \geq_c some term in that finite initial segment.

The equivalence of Theorem 0.6B.3 with ω^ω is well ordered is more delicate.

THEOREM 0.6B.4. For each fixed k , Theorems 0.6B.1 and 0.6B.3 are provable in RCA_0 . The following are provably equivalent in RCA_0 .

- i. Theorem 0.6B.1.
 - ii. Theorem 0.6B.3.
 - iii. ω^ω is well ordered.
- The first claim is provable in SEFA.

Proof: We have already seen that for each fixed k , Theorem 0.6B.1 is provable in RCA_0 . It is obvious that Theorem 0.6B.3 implies Theorem 0.6B.1 in RCA_0 .

We first show that for each k , RCA_0 proves that every infinite sequence from \mathbb{N}^k has an infinite increasing (\leq_c) subsequence. This is proved by induction on k . The case $k = 1$ asserts that every infinite sequence from \mathbb{N} has an infinite increasing (\leq) subsequence. If the sequence is bounded, then it has a constant infinite subsequence. Otherwise, use primitive recursion.

Suppose RCA_0 proves this for k . Now let $x_1, x_2, \dots \in \mathbb{N}^{k+1}$. Consider the infinite sequence of first terms, take an infinite increasing (\leq) subsequence, and then chop the first terms off, forming $y_1, y_2, \dots \in \mathbb{N}^k$. By the induction hypothesis, we can prove that the y 's have an infinite increasing (\leq_c) subsequence, which immediately gives rise to an infinite increasing (\leq_c) subsequence of the x 's.

We claim that $\text{RCA}_0 + \omega^\omega$ is well ordered proves

for all k , for every x_1, x_2, \dots from \mathbb{N}^k ,
there exists $i < j$ such that $x_i \leq_c x_j$

because for each fixed k , the above is strict Π^1_1 , and we can apply Theorem 0.6A.3. (The RCA_0 proofs for each k are a primitive recursive function of k).

Now the above proves Theorem 0.6B.3 by the following argument.

Let $x_1, x_2, \dots \in \mathbb{N}^k$ be such that for all n there exists x_m that is not \geq_c any of x_1, \dots, x_n . By primitive recursion, build an infinite subsequence y_1, y_2, \dots of the x 's such that no y_i is \geq_c any of y_1, \dots, y_{i-1} . Choose $i < j$ such that $y_i \leq_c y_j$. This is a contradiction.

Hence $\text{iii} \rightarrow \text{ii} \rightarrow \text{i}$. We have already seen that $\text{i} \rightarrow \text{iii}$. QED

Theorem 0.6B.4 was first proved in [Si88] using combinatorial methods. Note that here we have avoiding the combinatorial argument in favor of proof theory.

We now discuss finite forms of Theorems 0.6B.1 and (a weak form of) 0.6B.3. These are Π^0_2 sentences, thus falling within the scope of PRA and $\text{I}\Sigma_1$.

THEOREM 0.6B.5. For all $k \geq 1$ there is a longest sequence $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \dots >_{\text{lex}} x_n$ from \mathbb{N}^k such that each $\max(x_i) \leq i$.

THEOREM 0.6B.6. For all k there exists n such that the following holds. For all x_1, \dots, x_n from \mathbb{N}^k such that each $\max(x_b) \leq b$, there exists $1 \leq i < j \leq n$ such that $x_i \leq_c x_j$.

It is also natural to add a parameter as follows.

THEOREM 0.6B.7. For all $k \geq 1$ and $p \geq 0$, there is a longest sequence $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \dots >_{\text{lex}} x_n$ from \mathbb{N}^k such that each $\max(x_i) \leq i+p$.

THEOREM 0.6B.8. For all $k \geq 1$ and $p \geq 0$, there exists n such that the following holds. For all x_1, \dots, x_n from N^k such that each $\max(x_b) \leq b+p$, there exists $1 \leq i < j \leq n$ such that $x_i \leq_c x_j$.

THEOREM 0.6B.10. EFA proves $0.6B.8 \leftrightarrow 0.6B.6 \rightarrow 0.6B.7 \leftrightarrow 0.6B.5$.

Proof: This is easily seen by raising the dimension. E.g., to derive Theorem 0.6B.8, apply Theorem 0.6B.6 in N^{k+p} to $(0, \dots, 0; 1, \dots, 0), (0, \dots, 0; 0, 1, \dots, 0), \dots, (0, \dots, 0; 0, \dots, 1), (x_1; 0, \dots, 0), (x_2; 0, \dots, 0), \dots, (x_n; 0, \dots, 0)$. QED

We show below that \rightarrow can be replaced by \leftrightarrow .

THEOREM 0.6B.11. For each fixed $k \geq 1$, Theorem 0.6B.8 is provable in WKL_0 , and hence in PRA. For fixed $k \geq 1$, Theorem 0.6B.8 has a primitive recursive witness function (of p). This applies to Theorems 0.6B.5 - 0.6B.7. The first claim is provable in SEFA.

Proof: We argue in WKL_0 . Fix k, p , and form the appropriate finitely branching tree. By Theorem 0.6B.3, there is no infinite path through this tree. Hence this tree is finite. QED

To pin down the status of Theorems 0.6B.5 - 0.6B.8, we need the analog of Theorem 0.6A.3 for Π^0_2 sentences. This is given through a formalization of the primitive recursive functions in EFA.

Now EFA cannot treat an arbitrary primitive recursive function, because they grow too fast - see Theorem 0.5.1. So the primitive recursive functions are instead treated in EFA as partial recursive functions given by specific algorithms.

We work in EFA. We assume that each primitive recursive function symbol comes with an associated primitive recursive derivation, using terms rather than projection functions and composition introduction.

We let PRCT be the class of closed terms in this language. We define the all important reduction function $RF: PRCT \rightarrow PRCT$ as follows. Let $t \in PRCT$. Let s be the leftmost subterm of t which has exactly one occurrence of a primitive recursive function symbol F other than S . Replace

s by its expansion given by the derivation associated with F . If there is no such subterm of t , set $RF(t) = t$.

Let F be a primitive recursive function symbol. We associate the following algorithm $ALG(F)$. Given $p_1, \dots, p_k \geq 0$, apply RF successively starting at $F(p_1^*, \dots, p_k^*)$. Stop when we arrive at a fixed point of RF , say q^* . Output q .

From the point of view of EFA, $ALG(F)$ defines a k -ary partial recursive function, where the arity of F is k .

We can now state the analog of Theorem 0.6A.3.

THEOREM 0.6B.12. The following are provably equivalent in SEFA.

- i. 1-Con(PRA).
- ii. 1-Con(WKL₀).
- iii. Every primitive recursive definition defines a total function (i.e., each $ALG(F)$ computes a total function).

Proof: Here $i \leftrightarrow ii$ is by Theorem 0.6A.1. It is straightforward in EFA to construct, for each primitive recursive function symbol F , a proof in WKL₀ that $ALG(F)$ is total. It is easiest to make use of Σ^0_1 induction in WKL₀. Hence $ii \rightarrow iii$. Using iii , first obtain super exponentiation, and hence cut elimination. Then use the primitive recursive semantics of cut free proofs in PRA to obtain i . QED

THEOREM 0.6B.13. SEFA proves that for each fixed k , Theorems 0.6B.5 - 0.6B.8 are provable in PRA. The following are provably equivalent in SEFA.

- i. Any of Theorems 0.6B.5 - 0.6B.8.
- ii. Every primitive recursive definition defines a total function.
- iii. 1-Con(PRA).

Proof: For the first claim, fix k . Prove Theorem 0.6B.8 by assuming that it is false, constructing an associated finitely branching tree, taking an infinite path, and applying Theorem 0.6A.7 to get a contradiction. This proves the first claim with PRA replaced by WKL₀. Now apply Theorem 0.6A.1. From the first claim, we obtain $iii \rightarrow i$. For $ii \rightarrow iii$, see Theorem 0.6B.12.

For $i \rightarrow ii$, we argue in EFA. We have to be careful to avoid use of Σ^0_1 induction. Assume first that Theorem 0.6B.7 holds.

We need to handle the reduction process $\text{RFCT:PRCT} \rightarrow \text{PRCT}$ in EFA.

For any $t \in \text{PRCT}$, we can use a numerical measure $\#(t)$ computed as follows. Let r be the largest depth of the primitive recursive function symbols appearing in t , other than S . Form the length r sequence, where the i -th term, $1 \leq i \leq r$, is the number of occurrences in t of primitive recursive function symbols whose derivation has depth $r-i+1$.

It is clear that if t is not a fixed point of RFCT, then $\#(t) >_{\text{lex}} \#(\text{RF}(t))$. We can almost use Theorem 0.6B.7 to show that iteration of RFCT comes to a fixed point. However, the growth in the max's of the #'s is greater than 1. Nevertheless, the growth is at most a constant, for each $\text{ALG}(F)$, that depends only on the derivation of F . Hence we can Theorem 0.6B.7, by raising the dimension, and using dummy variables.

Also by raising the dimension, it is easily seen that Theorem 0.6B.6 implies Theorem 0.6B.7. Thus we obtain $ii \rightarrow i$. QED

0.6C. Walks in N^k .

A walk in N^k is a finite or infinite sequence in N^k such that each successive vector is "close" to the preceding vector.

There are several interesting notions of "close" that we can use. We restrict attention to only these four:

1. The Euclidean distance $|x-y|_2$ is at most 1.
2. The Euclidean distance $|x-y|_2$ is at most 1.5.
3. The Euclidean distance $|x-y|_2$ is at most 2.
4. The sup norm distance $|x-y|_\infty$ is at most 1.

These all have combinatorial equivalents that are easier to think about for our purposes.

1. At most one coordinate is changed, and it is changed by 1.
2. At most two coordinates are changed, and they are changed by 1.
3. Either no change, or one coordinate is changed by 1 or 2, or two coordinates are each changed by 1.
4. All coordinates are changed by at most 1.

Recall the definition of \leq_c in N^k . We can think of $x \leq_c y$ as "x points outward to y".

Let W_1, W_2, \dots be a walk in N^k . We look for $i < j$ such that $W_i \leq_c W_j$.

THEOREM 0.6C.1. For all $x \in N^k$, in every sufficiently long walk W in N^k starting with x , there exists $i < j$ such that $W_i \leq_c W_j$. Here we can use any of 1-4. If we use 1), then a walk of length $|x|_1 + k + 1$ is sufficient.

Proof: This is proved the same way that Theorem 0.6B.8 was proved using Theorem 0.6B.3. For the final claim, note that we cannot keep going down for that long. Hence there exists $i < j$ such that the i -th and $(i+1)$ -st terms are the same, or the former goes up to the latter, according to 1. QED

Note that the weakest of 1-4, except for the trivial 1), is 2). Hence we now focus on 2).

We now develop lower bounds for the functions $f_1, f_2, \dots: Z^+ \rightarrow Z^+$ given by

$f_k(n)$ = the of terms in the longest walk $(n, 0, \dots, 0) = x_1, x_2, \dots, x_r \in N^k$, such that for no $i < j$ is $x_i \leq_c x_j$. (Here we take the length of a walk as the number of terms, r).

This particular definition of $f_k(n)$ is used for convenience. Note that any longest such walk must have $x_r = (0, \dots, 0)$.

First consider the case $k = 2$. Clearly for all $n \geq 1$, $f_2(n) \geq 2n$, by looking at the walk

$(n, 0)$
 \dots
 $(0, n)$
 $(0, n-1)$
 \dots
 $(0, 0)$

We now develop a lower bound on $f_{k+2}(n)$ in terms of f_k .
 $f_{k+2}(1) \geq 2$.

Now consider the following walk in N^{k+2} , which is divided into n blocks. In the i -th block, $f_k f_k \dots f_k(1)$ appears, where there are i f_k 's.

$(n, 0, \dots, 0)$
 $(n-1, 1, 1, \dots, 0)$
 \dots
 $(n-1, f_k(1), 0, \dots, 0)$
 $(n-2, f_k(1), 0, \dots, 1)$
 \dots
 $(n-2, 0, \dots, 0, f_k f_k(1))$
 $(n-3, 1, \dots, 0, f_k f_k(1))$
 \dots
 $(n-3, f_k f_k f_k(1), 0, \dots, 0)$
 \dots
 $(0, \dots, 0, f_k f_k \dots f_k(1)),$ or $(0, f_k f_k \dots f_k(1), 0, \dots, 0)$
 \dots
 $(0, \dots, 0)$

where there are n f_k 's in the second to last displayed tuple.

The first block starts with $(n-1, 1, 1, \dots, 0)$. It walks from $(1, 0, \dots, 0)$ to $(0, \dots, 0)$ in dimension k , for $f_k(1)$ steps, using coordinates 3 through $k+2$. Meanwhile, the first term stays unchanged at $n-1$, and the second term counts from 1 to $f_k(1)$.

We continue in this way, creating n blocks.

In this walk, no x_i is \leq_c any later x_j . Hence $f_{k+2}(n) \geq f_k f_k \dots f_k(1)$, where $k, n \geq 1$, and there are n f_k 's.

Note that

$$f_2(n) \geq 2n, \quad f_{k+2}(1) \geq 2, \quad f_{k+2}(n) \geq f_k f_k \dots f_k(1).$$

It now follows immediately that $f_{2k}(n) \geq A_k(n)$, $k, n \geq 1$. See the definition of the A_k , $k \geq 1$, just before Theorem 0.7.10.

From these considerations, and from Theorem 06B.13, we obtain the following.

THEOREM 0.6C.2. For each fixed k , Theorem 0.6C.1 is provable in PRA. EFA + 1-Con(PRA) proves Theorem 0.6C.1.

THEOREM 0.6C.5. SEFA proves that for each fixed k , Theorem 0.6C.2 is provable in PRA. The following are provably equivalent in SEFA.

- i. Theorem 0.6C.1.
- ii. Theorem 0.6C.2.

iii. Every primitive recursive definition defines a total function.

iv. $1\text{-Con}(\text{PRA})$.

Here $1\text{-Con}(T)$ means T is 1-consistent; i.e., every Σ_1^0 sentence provable in T is true.

0.6D. Hilbert's Basis Theorem.

We now come to a discussion of concrete formulations of the Hilbert basis theorem for polynomial rings in several variables over fields.

THEOREM 0.6D.1. HBT (Hilbert's Basis Theorem). Let P_1, P_2, \dots be an infinite sequence of polynomials from the polynomial ring in k variables over a countable field. There exists n such that each P_i is in the ideal generated by P_1, P_2, \dots, P_n .

Here a countable field in RCA_0 consists of operations $0, 1, +, -, \cdot, ^{-1}$ obeying the field axioms, on a domain which is a subset of ω .

Let us review a proof of the above concrete strict Π_1^1 form of HBT.

Order the monomials in k variables lexicographically. First let Q_1, Q_2, \dots enumerate all polynomials in the ideal generated by the P 's. For each i , look at the leading monomial M_i of Q_i .

Apply Theorem 0.6B.3 to the sequence M_1, M_2, \dots , obtaining n such that all M 's are multiples of at least one of M_1, \dots, M_n . This gives us n such that the leading coefficient of every Q_i is a multiple of the leading coefficient of at least one of Q_1, \dots, Q_n . Then every Q_i is ideal generated by Q_1, \dots, Q_n , using iterated division with remainder.

From this sketch, and by looking at monomial ideals, we see the following.

LEMMA 0.6D.2. RCA_0 proves $0.6B.3 \rightarrow \text{HBT} \rightarrow 0.6B.1$. In fact, this implication works for HBT over the two element field. We write this special case as $\text{HBT}(2)$.

THEOREM 0.6D.3. HBT is provable in RCA_0 for each fixed k . RCA_0 proves the equivalence of

- i. HBT.
- ii. $\text{HBT}(2)$.

ii. ω^ω is well ordered.

This is obtained immediately from Theorem 0.6B.2 and Lemma 0.6D.2.

Theorem 0.6D.3 was proved in [Si88].

We also have the following finite form of HBT.

THEOREM 0.6D.4. FHBT (Finite Hilbert's Basis Theorem). For each $k \geq 1$ there exists n so large that the following holds. Let F be a countable field. Let P_1, P_2, \dots, P_n be polynomials in k variables with coefficients from F . Assume that the degree of each P_i is at most i . There exists $1 \leq i \leq n$ such that P_i is in the ideal generated by P_1, \dots, P_{i-1} .

The above result is stronger than expected, in that it has a strong uniformity - the integer n depends only on k , and not on the field. It is true for all fields F , but we want to stay within countable objects.

We also have the form with an additional numerical parameter.

THEOREM 0.6D.5. FHBT' (Finite Hilbert's Basis Theorem'). For each $k \geq 1$ and $p \geq 0$, there exists n so large that the following holds. Let F be a countable field. Let P_1, P_2, \dots, P_n be polynomials in k variables with coefficients from F . Assume that the degree of each P_i is at most $i+p$. There exists $1 \leq i \leq n$ such that P_i is in the ideal generated by P_1, \dots, P_{i-1} .

We sketch a proof of FHBT' in $WKL_0 + HBT$. Fix k, r, p , and assume FHBT' is false. Write down the countable field axioms, and the infinitely many axioms with infinitely many constants asserting that we have polynomials P_1, P_2, P_3, \dots . The number of constants used for each P_i is dictated by the bound $\deg(P_i) \leq i+p$. For each i , assert that P_i is not in the ideal generated by P_1, \dots, P_{i-1} using infinitely many universal axioms. Call this theory T , and let $T_0 \subseteq T$ be finite. Using the counterexample F, P_1, P_2, \dots , we see that T_0 is consistent (with the help of cut elimination in WKL_0). Hence T is consistent, and has a model. A model of T violates HBT.

The statement of FHBT' is not in explicitly Π^0_2 form. If F is a finite field or the field of rationals, then FHBT and FHBT' are in Π^0_2 form.

THEOREM 0.6D.6. SEFA proves that for each $k \geq 1$, FHBT and FHBT' for finite fields and the field of rationals is provable in PRA. The following are provably equivalent in SEFA.

- i. FHBT on any finite field or the rationals.
- ii. FHBT' on any finite field or the rationals.
- iii. Every primitive recursive definition defines a total function.

We can put FHBT' in Π^0_2 form using the uniform algorithm and bounds for ideal membership in polynomial rings over fields, from [He26]. For a modern treatment of ideal membership, see [As04].

Alternatively, note that for fixed k, p , the conclusion quantifying over countable fields F is equivalent, over WKL_0 , to a Σ^0_1 sentence, using the formalized completeness theorem. This gives us a Π^0_2 sentence which appropriately strengthens FHBT from the point of view of WKL_0 .

Using either argument, and applying Theorem 0.6B.11, and using monomials, we obtain the following.

THEOREM 0.6D.7. In FHBT', for each $k \geq 1$, there is a primitive recursive upper bound on n as a function of p . There is no universal primitive recursive bound for FHBT or FHBT'. The following are provably equivalent in RCA_0 .

- i. FHBT.
- ii. FHBT'.
- iii. Every primitive recursive definition defines a total function.

A proof of the first two claims of Theorem 0.6D.7 has appeared in [Soc92].

0.6E. Sequences of Algebraic Sets.

We now consider the following well known consequence of HBT: every decreasing chain of algebraic sets is eventually constant. We will formulate this directly in terms of polynomials.

THEOREM 0.6E.1. Let P_1, P_2, \dots be an infinite sequence of polynomials from the polynomial ring in k variables over a countable field. There exists n such that every simultaneous zero of P_1, \dots, P_n is a zero of all P 's.

It is somewhat tricky to show that Theorem 0.6E.1 implies ω^0 is well ordered. We cannot just use monomials. Also, this cannot be done if the P 's represent irreducible algebraic sets, by Krull's theorem for chains of prime ideals. So we must consider reducible algebraic sets.

Fix the dimension k and an infinite field F . Let T be a finite tree with at least one vertex, where every path has at most k vertices (excluding the root), and where the vertices other than the root are labeled with different elements of the field F . We call these k -good trees.

The algebraic meaning of a vertex at the i -th level above the root with label c is the equation $x_i = c$ (the root is at the 0-th level). The algebraic meaning of a path is the conjunction of the algebraic meaning of the vertices along that path other than the root. The algebraic meaning of the tree T is the disjunction of the algebraic meanings of the paths of T . Take $[T]$ to be this union of intersections. Rewrite this as an intersection of unions. Each union is the zero set of a polynomial obtained by multiplying the relevant $x_i - c$. $[T]$ becomes an algebraic subset of F^k , given by polynomials of degree $\leq \#T =$ the number of terminal vertices of T .

We need to have a sufficient criterion for $[T]$ to properly contain $[T']$.

LEMMA 0.6E.2. Let T, T' be k -good trees. Suppose T' is obtained from T by adding one or more children to a terminal vertex. Or suppose T' is obtained from T by deleting one of the children of a vertex that has at least two children (and of course all vertices above the one deleted). Then $[T]$ properly contains $[T']$.

Now all we have to do is to deal with the combinatorics of these two tree operations.

There is a nice way of assigning ordinals $< \omega^k$ to k -good trees. For each terminal node x of height $1 \leq i \leq k$, assign the ordinal ω^{i-1} . Now take the sum of the ordinals assigned to the terminal nodes, in decreasing (\geq) order. This is $\text{ord}(T)$.

The two tree operations lower ordinals. Also, $\text{ord}(T)$ is onto the ordinals $< \omega^k$. Even more is true and useful. Given $\alpha < \text{ord}(T)$, there exists T' obtained from T by successive

applications of the two tree operations in some combination, such that $\text{ord}(T') = \alpha$.

We have just provided a way of assigning an algebraic set to ordinals $< \omega^k$ so that if the algebraic set decreases then the ordinal lowers. We do require that the field be infinite.

THEOREM 0.6E.3. The following are provably equivalent in RCA_0 .

- i. HBT.
- ii. HBT(2).
- iii. Theorem 0.6E.1.
- iv. Theorem 0.6E.1 for the field of rationals.
- v. ω^ω is well ordered.

We can also develop a finite form for Theorem 0.6E.1 that is analogous to the finite forms discussed above for HBT.

THEOREM 0.6E.4. Let $k \geq 1$ and F be a field. There is a bound on the length of chains of algebraic sets $A_1 \supseteq \dots \supseteq A_n$ in F^k , where each A_i is of presentation degree $\leq i$.

Furthermore, the bound can be taken to depend on k only, and not on F .

We can show that the witness function for Theorem 0.6E.4 is (roughly) at least the witness function for our finite form of lex descent using the above way of assigning algebraic sets to ordinals (see Theorems 0.6B.5, 0.6B.7). In fact, the analog of Theorem 0.6D.7 holds here.

0.6F. Relatively Large Ramsey Theorem for Pairs.

We discuss the Relatively Large Ramsey Theorem in section 0.8C. [EM81] considers this theorem for pairs.

THEOREM 0.6F.1. Relative Large Ramsey Theorem for Pairs. For all p, r there exists n so large that the following holds. In any coloring of the unordered pairs from $\{1, \dots, n\}$ using p colors, there is a relatively large subset of $\{1, \dots, n\}$ with at least r elements whose unordered pairs have the same color.

The following is proved in [EM81].

THEOREM 0.6F.2. For each p , consider the function f_p of r that outputs the least n that makes Theorem 0.6F.1 true. Then each f_p is primitive recursive, and each primitive

recursive function is dominated by some f_p .

0.7. Incompleteness in Nested Multiply Recursive Arithmetic, and Two Quantifier Arithmetic.

The material in this section is taken from [Fr01c], until the last four paragraphs.

The well known proof theoretic analysis of $I\Sigma_n$, $n \geq 1$, is based on the ordinal $\omega[n+1] = \omega^{\dots^{\omega}}$, a tower of $n+1$ ω 's. In particular, the proof theory of $I\Sigma_2$ is based on the ordinal $\omega^{\omega^{\omega}}$.

Nested multiple recursion on the nonnegative integers is given by the scheme

$$f(x_1, \dots, x_k, y_1, \dots, y_m) = t(f_{\langle x_1, \dots, x_k \rangle}(y_1, \dots, y_m))$$

where

i) $f_{\langle x_1, \dots, x_k \rangle}$ is the function given by

$$f_{\langle x_1, \dots, x_k \rangle}(z_1, \dots, z_k, y_1, \dots, y_m) = f(z_1, \dots, z_k, y_1, \dots, y_m) \text{ if } (z_1, \dots, z_k) <_{lex} (x_1, \dots, x_k); 0 \text{ otherwise};$$

ii) t is any term involving $f_{\langle x_1, \dots, x_k \rangle}$, variables $x_1, \dots, x_k, y_1, \dots, y_m$, the successor function, constants for integers, previously defined functions, and IF THEN ELSE based on $<, =$.

The functions generated in this way are called the nested multiply recursive functions (on the integers). This is a rather robust collection of functions on the integers, whose definition does not involve ordinal notations. It coincides with the $<\omega^{\omega^{\omega}}$ recursive functions, and the $<\omega^{\omega}$ nested recursive functions; see [Ros84], pages 93,94, going back to [Tai61]. For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

Combining this with the proof theory of $I\Sigma_2$ based on $\omega^{\omega^{\omega}}$, gives the following.

THEOREM 0.7.1. The provably recursive functions of $I\Sigma_2$ are the $<\omega^{\omega^{\omega}}$ recursive functions (via descent recursion, [FSh95]), and the nested multiply recursive functions. Every Π_2^0 sentence provable in $I\Sigma_2$ has a nested multiply

recursive witness function. The first result is provable in SEFA.

NMRA (nested multiply recursive arithmetic) is the analog of PRA (primitive recursive arithmetic). It extends the usual axioms for successor by the defining equations for the nested multiply recursive functions, and the induction scheme for quantifier free formulas in its language.

THEOREM 0.7.2. $I\Sigma_2$ and NMRA prove the same Π_2^0 sentences. The following are provably equivalent over SEFA.

- i. $1\text{-Con}(I\Sigma_2)$.
- ii. $1\text{-Con}(\text{NMRA})$.
- iii. Every primitive recursive (elementary recursive, polynomial time computable) sequence from ω^{ω^ω} stops descending.

These are provable in $I\Sigma_3$ but not in $I\Sigma_2$.

Let us start with the following simple problem.

THEOREM 0.7.3. There is a longest finite sequence x_1, x_2, \dots, x_n from $\{1, 2\}$ in which no consecutive block x_i, \dots, x_{2i} is a subsequence of any later consecutive block x_j, \dots, x_{2j} .

Let us call this property of finite sequences property $*$.

One can easily show that the maximal length of a sequence from $\{1, 2\}$ with property $*$ is 11, and that the only examples are 12221111111 and 21112222222.

THEOREM 0.7.4. There is a longest finite sequence from $\{1, 2, 3\}$ with property $*$.

Since the above is a Σ_1 statement, it is provable in extremely weak fragments of arithmetic. However, such a proof is not of reasonable size.

The simplest known proof of reasonable size is truly exotic compared with the statement; this proof is conducted in $\Pi_1^1\text{-CA}_0$ (see section 0.4). With some considerable trouble, it can be replaced with a considerably less exotic proof, of reasonable size, that is formalizable in $I\Sigma_2$. Of course, this is still rather exotic compared to the statement.

We sketch the simplest known proof, which uses the Nash Williams minimal bad sequence argument, from [NW65], in this context. First we shift context to infinite sequences

of finite sequences.

THEOREM 0.7.5. Let $k \geq 1$ and x_1, x_2, \dots be an infinite sequence of finite sequences from $\{1, \dots, k\}$. There exists $i < j$ such that x_i is a subsequence of x_j .

Proof: Suppose this is false. Call an infinite sequence bad if it is a counterexample. Let x_1 be of least length so that it starts an infinite bad sequence. Let x_2 be of least length

so that x_1, x_2 starts a bad sequence. Continue in this way, getting a "minimal" bad sequence x_1, x_2, \dots . There is an infinite subsequence x_{i_1}, x_{i_2}, \dots , all of which start with the

same number. Note that $x_{i_1}', x_{i_2}', \dots$ is bad, where the primes mean "chop off the first term" (no x can be empty). Hence $x_1, \dots, x_{i_1-1}, x_{i_1}', x_{i_2}', \dots$ is also bad. But x_{i_1}' is shorter than x_{i_1} , contradicting the choice of x_{i_1} . QED

Proof of Theorem 0.7.4: Suppose there are arbitrarily long such. Build the finitely branching tree of such. Let x_1, x_2, \dots be an infinite branch, which therefore has property *. Consider the infinite sequence

x_1, x_2
 x_2, x_3, x_4
 x_3, x_4, x_5, x_6
 \dots

By Theorem 0.7.5, one is a subsequence of a later one. This contradicts property *. QED

Obviously we did not use that there are only three letters.

THEOREM 0.7.6. The Block Subsequence Theorem. For all $k \geq 1$, there is a longest finite sequence x_1, \dots, x_n in k letters in which no consecutive block x_i, \dots, x_{2i} is a subsequence of a later consecutive block x_j, \dots, x_{2j} .

THEOREM 0.7.7. For each fixed k , the Block Subsequence Theorem is provable in $I\Sigma_2$ and NMRA. This is provable in EFA.

Proof: In order to tame the proof of The Block Subsequence Theorem, we need to tame Theorem 0.7.5. I.e., we need to replace the minimal bad sequence argument with something more concrete.

The sharpest way to do this is to effectively assign (names for) ordinals $< \omega^{\omega^k}$ to finite bad sequences in the partial order of finite sequences from $\{1, \dots, k+1\}$ under subsequence, where if one is extended to another, then the corresponding ordinal decreases. This is for each fixed $k \geq 1$. This construction appears in [Si88]. Also see [Has94].

For fixed k , we now build the tree T of bad finite sequences in the sense of the Block Subsequence Theorem for $\{1, \dots, k+1\}$. Each bad finite sequence here gives rise to a bad sequence in the partial order of finite sequences from $\{1, \dots, k+1\}$. Therefore we can assign ordinals $< \omega^{\omega^k}$ to vertices in T according to the preceding paragraph.

For each level n of the tree T , we have finitely many vertices of that level, whose assigned ordinals are $\alpha_1, \dots, \alpha_p < \omega^{\omega^k}$, where $p \geq 0$. We define β_n to be the ordinal $\omega^{\alpha_1} + \dots + \omega^{\alpha_p}$, where $\alpha_1, \dots, \alpha_p$ is $\alpha_1, \dots, \alpha_p$ put in decreasing order.

It is obvious that if $\beta_n > 0$ then $\beta_{n+1} < \beta_n$. Hence for some n , $\beta_n = 0$. Therefore T is finite, and the Block Sequence Theorem is proved.

Note that this proof is carried out in just EFA, together with the fact that there is no double exponential time computable infinite descending sequence through ω^{ω^k} . However, the latter is well known to be provable in $\text{I}\Sigma_2$ and in NMRA. Or we can prove the latter in $\text{I}\Sigma_2$ and appeal to Theorem 0.7.2. If we follow that route, we need SEFA and not just EFA. QED

THEOREM 0.7.8. The Block Subsequence Theorem is provable in $\text{I}\Sigma_3$.

Proof: We argue in $\text{I}\Sigma_3$. By Theorem 0.7.7, we see that for each k , The Block Subsequence Theorem for k is provable in $\text{I}\Sigma_2$. Note that for each k , the Block Subsequence Theorem is a Σ_1^0 sentence. It is well known that $\text{I}\Sigma_3$ proves 1-Con($\text{I}\Sigma_2$). E.g., see [HP93], Corollary 4.34, p. 108. Hence we have The Block Subsequence Theorem. QED

In [Fr01c], it is shown how to reverse this process in order to show how descent recursion through ω^{ω^ω} can be suitably handled in EFA + the block subsequence theorem. Hence from Theorems 0.7.1, 0.7.2, we obtain the following.

THEOREM 0.7.9. The Block Subsequence Theorem is provable in

$I\Sigma_3$ but not in NMRA and $I\Sigma_2$. The witness function for The Block Subsequence Theorem dominates all multiply recursive functions. The following are provably equivalent in SEFA.

i. The Block Subsequence Theorem.

ii. $1\text{-Con}(I\Sigma_2)$.

iii. $1\text{-Con}(\text{NMRA})$.

To prove this, use Theorems 0.7.1, 0.7.8.

We now return to the block subsequence theorem with 3 letters. The exotic lower bounds are obtained in [Fr01c].

The construction is rather intricate, and uses a seed that we constructed by hand. This seed is a particular sequence of length 216 with property *. This sequence α is displayed on p. 126 of [Fr01c]. (Actually, its blocks $\alpha[i], \dots, \alpha[2i]$, $1 \leq i \leq 108$, are displayed). It is important that α has the following two additional properties from [Fr01c], p. 122.

i. α is of the form $u13^{108}$.

ii. For all $i \leq 108$, $\alpha[i], \dots, \alpha[2i]$ has at least one 1.

In [Fr01c], we use a convenient version of the Ackermann hierarchy of functions. We define functions A_1, A_2, \dots from Z^+ into Z^+ as follows. A_1 is doubling. $A_{k+1}(n) = A_k \dots A_k(1)$, where there are n A_k 's.

It is worth noting that $A_k(1) = 2$, $A_k(2) = 4$, and $A_k(3)$ goes to ∞ as k goes to ∞ .

We take the Ackermann function to be given by $A(k) = A_k(k)$.

It is easy to see that all primitive recursive functions are eventually dominated by some A_k . In fact, all primitive recursive functions are dominated by some A_k at all arguments ≥ 3 .

In [Fr01c], this seed is extended to a sequence of length $> A_7(184)$, thus obtaining the following.

THEOREM 0.7.10. The longest length of a sequence from $\{1, 2, 3\}$ with * is $> A_7(184)$.

Randall Dougherty wrote some software that looks for sequences from $\{1, 2, 3\}$ with * obeying i, ii above, 108 replaced by much higher even integers. He was able to find such a seed with length 187,196; i.e., 108 replaced by 93,598. Using this seed, we obtain the following in

[Fr01c].

THEOREM 0.7.11. The longest length of a sequence from $\{1,2,3\}$ with $*$ is $> A_{7198}(158,386)$.

As for an upper bound, we haven't worked this out, but are confident that $A(A(5))$ is a crude upper bound.

If we consider 4 letters, then the numbers grow considerably more exotic. The maximal length is greater than $AA\dots A(1)$, where there are $A(5)$ A 's.

Let $J(k)$ be the maximal length of a sequence in k letters with property $*$. By Theorem 0.7.9, J grows faster than all multiply recursive functions. By comparison, the Ackermann function $A_k(k)$ is a puny little doubly recursive function.

The ordinal $\omega^{\omega^{\omega}}$ is also used in [Si88] in connection with the Robson basis theorem, involving polynomial rings based on noncommuting indeterminates (see [Robs78a], [Robs78b]). It is shown there that RBT is provably equivalent to " $\omega^{\omega^{\omega}}$ is well ordered" over RCA_0 .

We close with a brief discussion of braids. The following is obtained from [CDW10].

Artin's braid groups are algebraic structures of substantial importance in core mathematics. There has emerged a standard ordering on braids, called the Dehornoy order.

It is known that the restriction of this standard ordering to B_n^+ , which consists of the Garside positive braids, is a well ordering of type $\omega^{\omega^{n-2}}$. This allows for the development of combinatorial theorems based on this restricted ordering, that are provable in $I\Sigma_3$ but not in $I\Sigma_2$, and whose associated functions are just beyond being multiply recursive. This has been accomplished in [CDW10].

0.8. Incompleteness in Peano Arithmetic and ACA_0 .

This level of incompleteness is unusually rich. We will not try to be exhaustive.

We will organize the discussion as follows.

0.8A. Preliminaries.

0.8B. Goodstein Sequences.

- 0.8C. Relatively Large Ramsey Theorem.
- 0.8D. Regressive Ramsey Theorem.
- 0.8E. Hercules Hydra Game and Worms.
- 0.8F. Regressive Counting Theorems.
- 0.8G. The Shift Inequality.
- 0.8H. Tree Embedding Theorems.

0.8A. Preliminaries.

The earliest mathematical example of incompleteness in Peano Arithmetic (PA) appeared in [Goo44], although it wasn't known until [KP82] that the result was not provable in PA. The result is the termination of Goodstein sequences.

This was followed by an entirely different example in [PH77], that is closely related to well known existing mathematical developments - i.e., Ramsey theory. This was the Paris-Harrington Ramsey theorem.

0.8E is a direct spin-off of 0.8B. 0.8D is a direct spin-off of 0.8C. 0.8F, 0.8G, and 0.8H break new ground, and represent the current state of the art with regard to incompleteness at the level of Peano Arithmetic.

0.8H is particularly flexible, and is a specialization to the binary case of incompleteness results from far stronger systems than PA. These are discussed in sections 0.9 and 0.10.

The relevant proof theoretic information about PA, ACA_0 , ACA' is as follows. For the definition of ACA' , see Definition 1.4.1.

THEOREM 0.8A.1. ACA_0 is a conservative extension of PA. The provably recursive functions of ACA_0 and PA are the $< \epsilon_0$ recursive functions. ACA_0 proves WKL_0 . The following are provably equivalent in RCA_0 .

- i. Π^1_1 reflection on ACA_0 .
- ii. ϵ_0 is well ordered.

These are provable in ACA' but not in ACA_0 .

The first claim is provable in SEFA.

For a general treatment of $< \lambda$ recursive functions via descent recursion, see [FSh95]).

THEOREM 0.8A.2. The following are provably equivalent in SEFA.

- i. $1\text{-Con}(\text{ACA}_0)$.
- ii. $1\text{-Con}(\text{PA})$.
- iii. Every primitive recursive (elementary recursive, polynomial time) sequence from \in_0 stops descending.

0.8B. Goodstein Sequences.

Let $b \geq 2$. We can write any $n \geq 0$ uniquely in base b , where we think of the exponents as nonnegative integers. Then we can write these exponents in base b , again creating perhaps more exponents. Of course, numbers $< b$ do not get rewritten. This process must end, and we obtain a fully base b representation of n . It has the structure of a finite tree, and the only integers appearing are b 's and numbers from $[1, b)$.

Let $n \geq 0$. We define the Goodstein sequence starting at n as follows.

Firstly, write n completely in base 2.

Next raise the base to 3, evaluate the number, and subtract 1.

Secondly, write this completely in base 3.

Next raise the base to 4, evaluate the number, and subtract 1.

Thirdly, write this completely in base 4.

...

This process is terminated once 0 is reached. E.g., the Goodstein sequence starting at 0 is of length 1.

THEOREM 0.8B.1. Goodstein's Theorem. The Goodstein sequence starting at any $n \geq 0$ eventually terminates.

This was proved in [Goo44]. The idea is that if we change the base to the infinite ordinal ω in all of the complete representations that occur starting at n , then the ordinals so represented form a strictly decreasing sequence. Hence we must have termination.

Let $G(n)$ be the length of the Goodstein sequence starting at n .

THEOREM 0.8B.2. Goodstein's Theorem can be proved in ACA' but not in PA . It is provably equivalent to $1\text{-Con}(\text{PA})$ over EFA . The function G is \in_0 recursive but eventually dominates every $<\in_0$ recursive function.

This was proved in [KP82]. Also see [Ci83] and [BW87].

0.8C. Relatively Large Ramsey Theorem.

Here is the original infinite Ramsey theorem.

THEOREM 0.8C.1. Infinite Ramsey Theorem. In any coloring of the unordered k tuples from the positive integers using p colors, there is an infinite set of positive integers whose unordered k tuples have the same color.

This is proved in [Ra30], and applied there to a fundamental decision problem in predicate calculus.

A set of positive integers is said to be relatively large if and only if its cardinality is at least its minimum element.

THEOREM 0.8C.2. Infinite Relatively Large Ramsey Theorem. In any coloring of the unordered k tuples from any infinite set of positive integers using p colors, there is a relatively large finite set of positive integers with at least r elements whose unordered k tuples have the same color.

Proof: This is an immediate consequence of the Infinite Ramsey Theorem, as observed in [PH77]. QED

THEOREM 0.8C.3. Relatively Large Ramsey Theorem. For all k, p, r there exists n so large that the following holds. In any coloring of the unordered k tuples from $\{1, \dots, n\}$ using p colors, there is a relatively large subset of $\{1, \dots, n\}$ with at least r elements whose unordered k tuples have the same color.

Proof: This is proved in [PH77] from Theorem 0.8C.2, using a finitely branching infinite tree argument. QED

This should be compared with the Finite Ramsey Theorem 1 of section 0.5.

Let $\text{PH}(k, p, r)$ be the least n in Theorem 0.8C.3.

THEOREM 0.8C.4. The Relatively Large Ramsey Theorem can be proved in ACA' but not in PA . It is provably equivalent to $1\text{-Con}(\text{PA})$ over EFA . The function PH is ϵ_0 recursive, but the unary function $\text{PH}(k, k, k)$ eventually dominates every $<\epsilon_0$ recursive function.

Proof: See [PH77]. QED

Theorem 0.8C.4 has been proved even if we fix $p = 2$ (i.e., for 2 colors). See [LN92], p. 824.

0.8D. Regressive Ramsey Theorem.

The Regressive Ramsey Theorem and its independence from PA can be gleaned from [PH77], as it was used as a kind of unadvertised intermediate step. The statement is also essentially present in [Sc74], but without any discussion or results, except to note that it follows from the usual infinite Ramsey theorem. However, The Regressive Ramsey Theorem was first focused on and perfected in [KM87].

Let N be the set of all nonnegative integers. We write $[A]^k$ for the set of all unordered k element subsets of $A \subseteq N$. Also, write $[n]^k$ for the set of all unordered k element subsets of $\{0, \dots, n-1\}$.

We say that $f: [N]^k \rightarrow N$ is regressive if and only if for all $x \in [N]^k$, if $\min(x) > 0$ then $f(x) < \min(x)$.

We say that f is min homogenous on $A \subseteq N$ if and only if for all $x, y \in [A]^k$, $\min(x) = \min(y) \rightarrow f(x) = f(y)$.

THEOREM 0.8D.1. Infinite Regressive Ramsey Theorem. Any regressive $f: [N]^k \rightarrow N$ is min homogenous on some infinite $A \subseteq N$.

It is well known that RCA_0 proves the equivalence of the Infinite Ramsey Theorem and the Infinite Regressive Ramsey Theorem. They are both equivalent, over RCA_0 , to ACA' . See Definition 1.4.1.

THEOREM 0.8D.2. Finite Regressive Ramsey Theorem. For all k, r there exists n so large that the following holds. Every regressive $f: [n]^k \rightarrow [n]$ is min homogenous on some r element $A \subseteq [n]$.

This is obtained from the Infinite version by a finitely branching infinite tree argument, in [KM87]. Also, in [KM87], the equivalence of Theorems 0.8C.3 and 0.8D.2 is established. Thus we have the following result from [KM87].

Let $KM(k, r)$ be the least n in Theorem 0.8D.2.

THEOREM 0.8D.3. The Finite Regressive Ramsey Theorem can be proved in ACA' but not in PA . It is provably equivalent to $1-Con(PA)$ over EFA . The function KM is ϵ_0 recursive, but $KM(k,k)$ eventually dominates every $<\epsilon_0$ recursive function.

0.8E. Hercules Hydra Game and Worms.

In [KP82], Goodstein's Theorem (Theorem 0.8B.1) is analyzed, and also the closely related Hercules Hydra games are introduced and analyzed.

Let T be a hydra, which is simply a finite rooted tree. We draw trees with the root at the bottom, and $v < v'$ means that v is a parent of v' (equivalently, v' is a child of v).

Hercules goes to battle with $T_1 = T$. Hercules first removes a leaf, and the hydra reacts by growing new vertices in the manner below, creating T_2 . Then Hercules removes a leaf from T_2 , and the hydra grows new vertices as below, thus creating T_3 . This continues as long as the tree has at least two vertices.

Suppose Hercules removes the leaf, x , from T_n , creating the temporary tree T_n' . Since we are assuming that T_n has at least two vertices, let y be the parent of x . If y is the root of T_n' , then set $T_{n+1} = T_n'$. Otherwise, let z be the parent of y . Let $T_n'|_{\geq y}$ be the subtree of T_n' with root y . The hydra grafts n copies of $T_n'|_{\geq y}$ on top of z , so that the roots of these copies become children of z . This results in the tree T_{n+1} .

By assigning ordinals to trees, [KP82] proves the following.

THEOREM 0.8E.1. Every strategy for Hercules in the Hercules hydra game is a winning strategy. I.e., the hydra is eventually cut down to a single vertex.

[KP82] also proves the following.

THEOREM 0.8E.2. Theorem 0.8E.1 can be proved in ACA' but not in PA . It is provably equivalent to $1-Con(PA)$ over EFA .

In [Bek06], a Worm Principle is introduced and investigated. It is a flattened and deterministic version of the Hercules Hydra game, and metamathematical properties

corresponding to those of the Hercules Hydra game are established.

0.8F. Regressive Counting Theorems.

Our Counting Theorems appear in section 1 of [Fr98].

THEOREM 0.8F.1. Let $k, r, p > 0$ and $F: N^k \rightarrow N^r$ obey the inequality $\max(F(x)) \leq \min(x)$. There exists $E \subseteq N$, $|E| = p$, such that $|F[E^k]| \leq (k^k)p$.

We now turn this around so that it asserts a combinatorial property of any function $F: N^k \rightarrow N^r$.

Let $A, B \subseteq N^k$, and $F: A \rightarrow N^r$. We say that y is a regressive value of F on B if and only if there exists $x \in B$ such that $F(x) = y$ and $\max(y) < \min(x)$.

THEOREM 0.8F.2. Let $k, r, p > 0$ and $F: N^k \rightarrow N^r$. F has $\leq (k^k)p$ regressive values on some $E^k \subseteq N^k$, $|E| = p$.

We now state the obvious finite forms of Theorems 0.8F.1 and 0.8F.2.

THEOREM 0.8F.3. For all $k, r, p > 0$ there exists n so large that the following holds. Let $F: \{0, \dots, n-1\}^k \rightarrow \{0, \dots, n-1\}^r$ obey the inequality $\max(F(x)) \leq \min(x)$. There exists $E \subseteq \{0, \dots, n-1\}$, $|E| = p$, such that $|F[E^k]| \leq (k^k)p$.

THEOREM 0.8F.4. For all $k, r, p > 0$ there exists n so large that the following holds. Let $F: \{0, \dots, n-1\}^k \rightarrow \{0, \dots, n-1\}^r$. F has $\leq (k^k)p$ regressive values on some $E^k \subseteq \{0, \dots, n-1\}^k$, $|E| = p$.

In [Fr98], equivalences are established between these Theorems and the Regressive Ramsey Theorems. We obtain the following.

THEOREM 0.8F.5. Theorems 0.8F.1 and 0.8F.2 are provable in ACA' but not in ACA_0 . They are provably equivalent to " ϵ_0 is well ordered" over RCA_0 . These results hold even if we fix $r = 2$ and merely state the existence of constants c_k depending only on k .

THEOREM 0.8F.6. Theorems 0.7.3 and 0.7.4 are provable in ACA' but not in PA . They are provably equivalent to $1-Con(PA)$ over PRA . These results hold even if we fix $r = 2$

and merely state the existence of constants c_k depending only on k .

0.8G. The Shift Inequality.

Recall that Adjacent Ramsey Theory studies the shift equation

$$F(x_1, \dots, x_k) = F(x_2, \dots, x_{k+1})$$

over N . See the Adjacent Ramsey Theorem (Theorem 0.5.6). We saw that Adjacent Ramsey Theory corresponds to EFA in the same way that Finite Ramsey Theory does.

We have intensively studied the inequality

$$F(x_1, \dots, x_k) \leq F(x_2, \dots, x_{k+1})$$

over the nonnegative integers, N . This is far more exotic than the Adjacent Ramsey Theory, in that it corresponds, not to EFA, but to PA.

These results are from [Fr08], [Fr10a].

For $x, y \in N^k$, we write $x \leq_c y$ if and only if for all $1 \leq i \leq k$, $x_i \leq y_i$.

THEOREM 0.8G.1. For all $k \geq 1$ and $f: N^k \rightarrow N^2$, there exist distinct x_1, \dots, x_{k+1} such that $f(x_1, \dots, x_k) \leq_c f(x_2, \dots, x_{k+1})$.

THEOREM 0.8G.2. For all $k \geq 1$ and $f: N^k \rightarrow N$, there exist distinct x_1, \dots, x_{k+3} such that $f(x_1, \dots, x_k) \leq f(x_2, \dots, x_{k+1}) \leq f(x_3, \dots, x_{k+2})$.

THEOREM 0.8G.3. For all $k \geq 1$ and $f: N^k \rightarrow N$, there exist distinct x_1, \dots, x_{k+1} such that $f(x_2, \dots, x_{k+1}) - f(x_1, \dots, x_k) \in 2N$.

THEOREM 0.8G.4. For all $k, r \geq 1$ and $f: N^k \rightarrow N^r$, there exist distinct x_1, \dots, x_{k+1} such that $f(x_1, \dots, x_k) \leq_c f(x_2, \dots, x_{k+1})$.

THEOREM 0.8G.5. For all $k, r, t \geq 1$ and $f: N^k \rightarrow N^r$, there exist distinct x_1, \dots, x_{k+t-1} such that $f(x_1, \dots, x_k) \leq_c \dots \leq_c f(x_t, \dots, x_{t+k-1})$.

THEOREM 0.8G.6. For all $k, r, t \geq 1$ and $f: N^k \rightarrow N^r$, there exist distinct x_1, \dots, x_{k+1} such that $f(x_2, \dots, x_{k+1}) - f(x_1, \dots, x_k) \in tN^r$.

THEOREM 0.8G.7. Theorems 0.8G.1 - 0.8G.6 are provable in ACA' but not in ACA₀. They are provably equivalent to " ϵ_0 is well ordered" over RCA₀.

We can weaken these Theorems by restricting to complexity classes. These restrictions are obviously arithmetic sentences.

THEOREM 0.8G.8. Theorems 0.8G.1 - 0.8G.6 hold for recursive f . These are explicitly Π^0_3 sentences.

THEOREM 0.8G.9. Theorems 0.8G.1 - 0.8G.6 hold for primitive recursive (elementary recursive, polynomial time in base 2 representations) f . These are explicitly Π^0_2 sentences.

For $p \geq 0$, we define p -Con(T) to be the sentence "every Σ^0_p sentence provable in T is true".

THEOREM 0.8G.10. Theorem 0.8G.8 (all forms) is provably equivalent to 2-Con(PA) over EFA. Theorem 0.8G.9 (all forms) is provably equivalent to 1-Con(PA) over EFA.

We say that $f: N^k \rightarrow N^r$ is limited if and only if for all $x \in N^k$, $\max(f(x)) \leq \max(x)$.

THEOREM 0.8G.11. Theorems 0.8G.1 - 0.8G.6 hold for limited functions.

THEOREM 0.8G.12. Theorem 0.8G.9 (all forms) is provably equivalent to 1-Con(PA) over RCA₀.

THEOREM 0.8G.13. Theorems 0.8G.1 - 0.8G.6 hold for limited functions defined on some $[0, n]^k$, n depending on the given numerical parameters.

Note that Theorem 0.8G.13 (all forms) is explicitly Π^0_2 .

THEOREM 0.8G.14. Theorem 0.8G.13 (all forms) is provably equivalent to 1-Con(PA) over EFA. The associated witness function (all forms) is ϵ_0 recursive but eventually dominates all $<\epsilon_0$ recursive functions.

We have applied the shift inequality to polynomials with integer coefficients, and to the tangent function.

Let $n_1, \dots, n_k \in \mathbb{Z}$. The translates of (n_1, \dots, n_k) in coordinate $1 \leq i \leq k$ are the vectors obtained by adding an integer to the i -th coordinate.

THEOREM 0.8G.15. The Polynomial Shift Translation Theorem. For all polynomials $P: \mathbb{Z}^k \rightarrow \mathbb{Z}^k$, there exist distinct positive integers n_1, \dots, n_{k+1} such that, in each coordinate, the number of translates of (n_1, \dots, n_k) which are values of P is at most the number of translates of (n_2, \dots, n_{k+1}) which are values of P .

THEOREM 0.8G.16. Theorem 0.8G.15 is provable in ACA' but not in Peano Arithmetic. It implies 2-Con(PA) over EFA.

A **block** is a subsequence that does not skip over terms. A k -block is a block of length k .

Tangent here means the trigonometric \tan function. We exploit the periodic and surjective properties of \tan . There have been earlier results of ours and others concerning sine. See [Bo07].

THEOREM 0.8G.17. Let $k \geq 1$. Every infinite sequence of integers contains an infinite subsequence, where the tangents of the products of its k -blocks lie within 1 of each other, or go to $+\infty$.

We make Theorem 0.8G.17 successively more concrete as follows.

THEOREM 0.8G.18. Let $k, n \geq 1$. Every infinite sequence of integers contains a subsequence of length n , where the tangents of the products of its k -blocks lie within 1 of each other, or are strictly increasing and positive, or are strictly decreasing and negative.

THEOREM 0.8G.19. Let $k \geq 1$. Every infinite sequence of integers contains a subsequence of length $k+2$, where the tangents of the products of its k -blocks lie within 1 of each other, or are strictly increasing and positive, or are strictly decreasing and negative.

THEOREM 0.8G.20. For $k \geq 1$ there exists n such that the following holds. Every finite sequence of integers of length n obeying $|x[i]| \leq i$, $i \geq 1$, contains a subsequence of length $k+2$, where the tangents of the products of its k -blocks lie within 1 of each other, or are strictly increasing and positive, or are strictly decreasing and

negative.

THEOREM 0.8G.21. Theorems 0.8G.17 - 0.8G.20 are provable in ACA' but not in ACA₀. Theorems 0.8G.17 - 0.8G.19 are provably equivalent to " ϵ_0 is well ordered" over RCA₀. Theorem 0.8G.20 is provably equivalent to 1-Con(PA) over EFA. The witness function associated with Theorem 0.8G.20 is ϵ_0 recursive but grows faster than all $<\epsilon_0$ recursive functions.

0.8H. Tree Embedding Theorems.

We will postpone a full discussion of Kruskal's Tree Theorem until section 0.9B. We refer the reader to section 0.9B for definitions not given here.

We will consider three immediate consequences of Kruskal's Theorem here. We know that these are equivalent. Various natural variants can also be seen to be equivalent.

EBTE. Exactly Binary Tree Embedding Theorem.

TE. Tree Embedding Theorem.

STE. Structured Tree Embedding Theorem.

These are presented below. STE \rightarrow TE \rightarrow EBTE is immediate.

Kruskal's Theorem involves inf preserving embeddings. Here we will use only embeddings. Here is the reason behind this.

THEOREM 0.8H.1. The following is provable in EFA. If there is an embedding from a finite binary tree S into a finite binary tree T, then there is an inf preserving embedding from S into T. If there is a structure preserving embedding from a finite structured binary tree S into a finite structured binary tree T, then there is a structure and inf preserving embedding from S into T.

Proof: This is well known. Use induction on the sum of the number of vertices in S and T. QED

An exactly binary tree is a tree all of whose vertices have valence 0 or 2.

In reading the next theorem (and later), note that according to the definitions in section 0.9, embeddings between finite structured trees are required to preserve

structure. However, inf preservation must be explicitly stated.

THEOREM 0.8H.2. i. Exactly Binary Tree Embedding Theorem (EBTE). In any infinite sequence of exactly binary trees, some tree is embeddable into a later tree.
 ii. Tree Embedding Theorem (TE). In any infinite sequence of finite trees, some tree is embeddable into a later tree.
 iii. Structured Tree Embedding Theorem (STE). In any infinite sequence of finite structured trees, some tree is embeddable into a later tree.

Proof: These are very special cases of Kruskal's Theorem [Kr60]. EBTE is also a very special case of Higman's Wqo Theorem from [Hig52]. QED

THEOREM 0.8H.3. The following are provably equivalent in RCA_0 .

- i. EBTE.
 - ii. TE.
 - iii. STE.
 - iv. ϵ_0 is well ordered.
- i-iv are provable in ACA' but not in ACA_0 .

Proof: $i \rightarrow iv$ is due to [VV05] and A. Weiermann (advisor), and will appear in [FWa], together with a different proof of ours. These proofs yield very effective ordinal assignments f to binary trees onto ϵ_0 , where if S is embeddable into T then $f(S) \leq f(T)$.

That iv) implies structured EBTE is in [Fr84]. Specifically, In [Fr84], calculations are made of the ordinals of the trees of bad sequences for various restricted forms of Kruskal's Theorem, including structured EBTE. In general, these calculations used a theory of ordinals - i.e., ATR_0 . However, in this case, the proof shows that for each starting exactly binary structured tree, ACA_0 proves that there are no infinite bad sequences extending it. Hence structured EBTE can be proved using Π^1_1 reflection on ACA_0 . Now apply Theorem 0.8A.1.

We have recently proved that structured EBTE implies STE as follows. We inductively define a very effective map h from finite structured trees into finite exactly binary structured trees, so that if $h(S)$ is structure preserving embeddable into $h(T)$ then S is structure preserving embeddable into T . This will appear in [FWa]. This establishes that structured EBTE implies STE.

By combining the last two paragraphs, we have $iv \rightarrow iii$. Note that $iii \rightarrow ii \rightarrow i$ is trivial. QED

The following two Theorems are immediate consequences of EBTE, TE, STE, respectively.

THEOREM 0.8H.4. Subrecursive EBTE, TE, STE. In any infinite primitive recursive (elementary recursive, polynomial time computable) sequence of finite exactly binary trees (trees, structured trees), one tree is embeddable in a later tree.

THEOREM 0.8H.5. Recursive EBTE, TE, STE. In any infinite recursive sequence of finite exactly binary trees (trees, structured trees), one tree is embeddable in a later tree.

THEOREM 0.8H.6. Finite EBTE, TE, STE. For all $c \geq 0$ there exists n such that the following holds. Let T_1, \dots, T_n be exactly binary trees (trees, structured trees), where each T_i has at most $i+c$ vertices. There exist $i < j$ such that T_i is embeddable in T_j .

Proof: The argument is in [Fr81a]. Also see [Si85]. Let $c \geq 0$ be given and assume this is false. Build a finitely branching tree of counterexamples. By STE, the tree has no infinite paths, and therefore is finite. QED

The following Theorem provides the required link between these effective and finite forms of EBTE, TE, STE, and proof theory.

THEOREM 0.8H.7. The following are provably equivalent in EFA.

- i. Every primitive recursive sequence from ϵ_0 stops descending.
- ii. Every elementary recursive sequence from ϵ_0 stops descending.
- iii. Every polynomial time computable sequence from ϵ_0 stops descending.
- iv. $1\text{-Con}(\text{PA})$.

Proof: This is well known from standard proof theory - except for iii. Here we follow the usual practice in computational complexity theory, where the base 2 representation is used for nonnegative integers - not only for representing the indexation of the infinite sequences, but also for the coefficients in notations below ϵ_0 . It is

straightforward to check that the required manipulations can be done in polynomial time. QED

An interesting question is how small a subclass of poly time can be used for iii above. At very low computational levels, we expect that some interesting detailed issues should naturally arise.

THEOREM 0.8H.8. The following are provably equivalent in EFA.

- i. Every recursive sequence from ϵ_0 stops descending.
- ii. $2\text{-Con}(\text{PA})$.

Proof: Assume ii. Fix $k \geq 1$. Let M be a TM set up to compute a partial recursive function from N into $\omega^{[k]}$. Obviously PA proves

if M computes a total recursive function from N into $\omega^{[k]}$, then that function is not everywhere descending.

The above sentence is obviously Σ_2^0 . Hence we have

for all $k \geq 1$, if M is a TM set up to compute a partial recursive function from N into $\omega^{[k]}$, and if M computes a total recursive function from N into $\omega^{[k]}$, then that function is not everywhere descending.

for all $k \geq 1$, every recursive function from N into $\omega^{[k]}$ stops descending.

every recursive function from N into ϵ_0 stops descending.

This establishes $\text{ii} \rightarrow \text{i}$.

For $\text{i} \rightarrow \text{ii}$, we argue in EFA. Assume i. In particular, every polynomial time computable sequence from ϵ_0 stops descending. Hence by Theorem 0.8H.7, we have $1\text{-Con}(\text{PA})$. Therefore we have access to all of the $< \epsilon_0$ recursive functions.

We now use the standard Schütte infinitary proof theory for PA. See [Sch77] and [Bu91].

We start with a proof in PA of a Σ_2^0 sentence. We use primitive recursive function symbols, and so the Σ_2^0 sentence φ takes the form $(\exists n)(\forall m)(F(n,m) = 0)$.

By effective infinitary cut elimination, we obtain an infinitary cut free proof, tagged with ordinals $< \epsilon_0$, that is $< \epsilon_0$ recursive. We now examine this infinitary proof.

We go up the proof tree (backwards in the proof), starting at the root, through vertices of valence 1 only. By 1-Con(PA), we see that this process must stop. It is clear that it must stop at a vertex of valence > 1 . This must be a vertex which is the result of \forall introduction. But then we must have introduced $F(t(n), 0) = 0$, $F(t(n), 1) = 0$, and so on. Here $t(n)$ is a term which may or may not mention the variable n . By 1-Con(PA), these equations can only be introduced here if they are true. Hence we obtain $(\forall m) (F(t(n), m) = 0)$. Therefore $(\exists n) (\forall m) (F(n, m) = 0)$. QED

THEOREM 0.8H.9. The following are provably equivalent in EFA.

- i. Subrecursive EBTE.
- ii. Subrecursive TE.
- iii. Subrecursive STE.
- iv. 1-Con(PA).

Proof: Assume i. Using the very effective surjective assignment of ordinals $< \epsilon_0$ to exactly binary trees referred to in the proof of Theorem 0.8H.3, we obtain i in Theorem 0.8H.7. Hence 1-Con(PA).

Assume 1-Con(PA). Fix a primitive recursive sequence f of finite exactly binary structured trees. Let T be the first tree in the sequence. The proof from [Fr84] discussed in the proof of Theorem 0.8H.3, shows how to prove in PA that for some $i < j$, $f(i) \leq f(j)$. Hence i holds, for exactly binary structured trees.

We then have iii by applying the very effective map from finite structured trees to finite exactly binary structured trees, referred to in the proof of Theorem 0.8H.3.

Thus we have shown $i \rightarrow iv \rightarrow iii$. Obviously $iii \rightarrow ii \rightarrow i$. QED

THEOREM 0.8H.10. The following are provably equivalent in EFA.

- i. Recursive EBTE.
- ii. Recursive TE.
- iii. Recursive STE.
- iv. 2-Con(PA).

Proof: Assume i. Using the very effective surjective assignment of ordinals $< \epsilon_0$ to exactly binary trees referred to in the proof of Theorem 0.8H.3, we obtain i) in Theorem 0.8H.8. Hence $2\text{-Con}(\text{PA})$.

Assume $2\text{-Con}(\text{PA})$. We argue similarly to the proof of $ii \rightarrow i$ in Theorem 0.8H.8. Fix a finite exactly binary structured tree T . Let TM be set up to compute a partial recursive function from N into finite exact binary trees. From [Fr84], as discussed in the proof of Theorem 0.8H.3, PA proves

if TM computes a total recursive function f from N into finite exactly binary trees, starting with T , then there exist $i < j$ such that $f(i) \leq f(j)$.

The above sentence is obviously Σ_2^0 . Hence we have

for all finite exactly binary structured T , if a TM is set up to compute a partial recursive function from N into finite exactly binary structured trees, starting with T , and if that TM computes a total recursive function from N into finite exactly binary structured trees, then there exist $i < j$ such that $f(i) \leq f(j)$.

for all finite exactly binary structured trees T , for every recursive function f from N into finite exactly binary structured trees, starting with T , there exist $i < j$ such that $f(i) \leq f(j)$.

for all recursive functions f from N into finite exactly binary structured trees, there exist $i < j$ such that $f(i) \leq f(j)$.

This establishes $iv \rightarrow i$ for exactly binary structured trees.

We then have iii by applying the very effective map from finite structured trees to finite exactly binary structured trees, referred to in the proof of Theorem 0.8H.3.

Thus we have shown $i \rightarrow iv \rightarrow iii$. Obviously $iii \rightarrow ii \rightarrow i$. QED

THEOREM 0.8H.11. The following are provably equivalent in EFA.

- i. Finite EBTE.
- ii. Finite TE.

- iii. Finite STE.
- iv. 1-Con(PA).

Proof: Assume i. Using the very effective surjective assignment of ordinals $< \epsilon_0$ referred to in the proof of Theorem 0.8H.3, we obtain the "slow well foundedness of ϵ_0 " or CWF = "combinatorial well foundedness of ϵ_0 ", in the sense of [Fr81a] and [Fr01c], p. 71. This is bootstrapped up (as in [Fr81a] and [Fr01c]) to obtain the elementary recursive or even primitive recursive well foundedness of ϵ_0 . By the proof theory of PA, 1-Con(PA) follows.

Assume 1-Con(PA). Fix $c \geq 0$. We can obtain a proof in PA of i for finite exactly binary structured trees, for this fixed c , very effectively in c , as follows. Assume that i for this fixed c is false, using structured binary trees. Now form the tree T of appropriately bad sequences, and hypothesize in PA that T is infinite. Then there is an arithmetically defined infinite bad sequence. Now there are only finitely many first terms that this infinite bad sequence can have. For each of these terms, we argue from [Fr84] as in the proof of Theorem 0.8H.3, to obtain a contradiction. Therefore T is finite.

Since the statement of i with structure, for fixed c is Σ_1^0 , we see that the statement must be true for any c , by 1-Con(PA). This establishes $\text{iv} \rightarrow \text{i}$ for exactly binary structured trees. We can obviously use, say, a double exponential growth rate in the formulation of i for exactly binary structured trees, and the same argument will apply. I.e., we will obtain that also from 1-Con(PA). But this modification of i for exactly binary structured trees obviously implies iii using the very effective map from finite structured trees into finite exactly binary structured trees, referred to in the proof of Theorem 0.8H.3. This establishes $\text{iv} \rightarrow \text{iii}$. Note that $\text{iii} \rightarrow \text{ii} \rightarrow \text{i}$ is immediate. QED

In section 0.10, my Extended Kruskal Theorem is discussed, in which we impose a gap condition on the inf preserving embeddings. It is provable in $\Pi_1^1\text{-CA}$ but not in $\Pi_1^1\text{-CA}_0$ (see Theorems 0.10A.4 and 0.10A.5).

In [SS85], the Extended Kruskal Theorem is specialized to valence 1, which is just for finite sequences. The resulting statement is much weaker, and is shown to correspond to ϵ_0 .

In [Gor89], the Extended Kruskal Theorem for valence 1 is generalized allowing ordinal labels (with a suitable natural weakening of the gap condition), still at valence 1. The logical strength for α corresponds roughly to the Turing jump hierarchy on α .

0.9. Incompleteness in Predicative Analysis and ATR_0 .

0.9A. Predicative analysis, Γ_0 , and ATR_0 .

0.9B. Kruskal's Theorem.

0.9C. Comparability.

0.9A. Predicative analysis, Γ_0 , and ATR_0 .

The philosophy of mathematics known as predicativity focuses on the legitimacy of forming a subset of N via the construction $\{n: \varphi(n)\}$.

H. Poincaré, in [Po06], argued that this is not legitimate if the condition φ refers to all subsets of N . He argued that φ must only refer to subsets of N that have already been constructed, thus implicitly introducing a notion of abstract time. Note that this criterion is easily met if φ is arithmetical, even if it has parameters for subsets of N . Poincaré referred to this as the Vicious Circle Principle.

His ideas were taken up by Weyl, in [Wey18,87], and others. Russell articulated the basic idea earlier than Poincaré, but in the context of the paradoxes. Russell in effect abandoned the Vicious Circle Principle through his adoption of his highly impredicative Theory of Types, [Ru08,67].

S. Feferman and K. Schütte, independently sought to analyze predicative analysis formally. The initial analyses appeared in [Fe64] and [Sch65]. Subsequently, Feferman refined his analysis in many papers, culminating with [Fe05].

What is constant throughout all of these formal analyses is that

i. The provably recursive functions of predicative analysis consists of the $< \Gamma_0$ recursive functions.

ii. The finite sequence trees, presented arithmetically, that are provably well founded within predicative analysis, have ordinals up to, but not including, Γ_0 .

iii. The subsets of N present in the first Γ_0 levels of the hyperarithmetical hierarchy form (the subset of N part of) a model of predicative analysis.

For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

These analyses have been generally accepted as reasonably representing predicative analysis according to its historical informal descriptions. The degree of acceptance is not nearly as great as it is for Turing's analysis of algorithms. It is an open question whether it is possible to attain such a high level of acceptance. Nevertheless, there is no competing analysis of predicative analysis with anything like the same level of acceptance.

This usual analysis of predicativity takes the form of what amounts to the formal system $ATR(<\Gamma_0)$ of arithmetic, based on ACA_0 and arithmetic transfinite recursion up to any ordinal (notation) $<\Gamma_0$. Its minimum ω model consists of the hyperarithmetical sets of level $<\Gamma_0$.

Competing analyses of predicativity generally differ only in the choice of ordinal, but do take the form of a system $ATR(<\lambda)$, for some effectively given ordinal λ .

Recall our system ATR_0 , which plays a prominent role in Reverse Mathematics. We proved a striking matchup between ATR_0 and the standard formalization of predicative analysis.

THEOREM 0.9A.1. ATR_0 is a conservative extension of $ATR(<\Gamma_0)$ for Π^1_1 sentences. The provably recursive functions of ATR_0 and $ATR(<\Gamma_0)$ are the $<\Gamma_0$ recursive functions. The following are provably equivalent in RCA_0 .

- i. Π^1_1 reflection on ATR_0 .
- ii. Γ_0 is well ordered.

These are provable in ATR but not in ATR_0 . For ATR , use Γ_{ϵ_0} throughout instead of Γ_0 . The first claim is provable in SEFA.

Proof: For these results of ours about ATR_0 , see our announcement [Fr76], our proof in [FMS82], section 4, and [Si02]. For ATR , see [Ja80]. QED

Let (N, R) be a primitive recursively given well ordering of N . The system $ATI(<R)$ is in $L(PA)$, and extends PA by the

scheme of arithmetic transfinite induction on any proper initial segment of R determined by any given point.

Below, $ATI(<\Gamma_0)$ refers to $ATI(<R)$, where R is a standard notation system for Γ_0 . All such standard R lead to equivalent systems $ATI(<R)$.

THEOREM 0.9A.2. ATR_0 is a conservative extension of $ATI(<\Gamma_0)$. The following are provably equivalent in SEFA.

- i. $1-Con(ATR_0)$.
- ii. $1-Con(ATR(<\Gamma_0))$.
- iii. $1-Con(ATI(<\Gamma_0))$.
- iv. Every primitive recursive (elementary recursive, polynomial time computable) sequence from Γ_0 stops descending.

These are provable in ATR but not in ATR_0 . For ATR , use Γ_{ϵ_0} throughout instead of Γ_0 .

Proof: For these results of ours about ATR_0 , see [FMS82], section 4, and [Si02]. For ATR , see [Ja80]. QED

However, ATR_0 cannot be considered part of predicative analysis because of the following.

THEOREM 0.9A.3. Every ω -model of ATR_0 properly includes all hyperarithmetical subsets of N .

Proof: See [Si99,09], p. 346, notes for section VIII.4. QED

Theorem 0.9A.3 is especially powerful for establishing that a Π^1_2 sentence cannot be proved predicatively. By showing that the Π^1_2 sentence implies ATR_0 over RCA_0 (or even ACA_0), it is clear that the Π^1_2 sentence cannot hold in any subset of the hyperarithmetical sets, and therefore cannot be proved in any system $ATR(<\lambda)$, where λ is effectively given.

Let TI be the subsystem of second order arithmetic consisting of ACA_0 plus the scheme of transfinite induction on all countable well orderings. Often this is referred to as BI = bar induction, but we prefer to call this TI = transfinite induction.

For $n \geq 1$, we define $\Pi^1_n-TI_0$ and $\Sigma^1_n-TI_0$ as ACA_0 together with transfinite induction on all countable well orderings, with respect to Π^1_n and Σ^1_n formulas, respectively. Here Π^1_n (Σ^1_n) formulas start with a universal (existential) set quantifier, followed by at most $n-1$ set quantifiers, followed by an arithmetical formula. If we use ACA instead

of ACA_0 (which is ACA_0 with full induction), then we write Π^1_n -TI and Σ^1_n -TI.

Also, ATR is ATR_0 with full induction.

THEOREM 0.9A.4. ATR and Σ^1_1 -TI are equivalent. ATR_0 and Σ^1_1 -TI have the same ω -models. $ATR_0 + \Sigma^1_1$ induction and Σ^1_1 -TI $_0$ are equivalent.

Proof: See [Si82]. QED

The next two theorems are proved in [RW93]. Here $\langle \theta\Omega^\omega$ refers to a standard notation system for the proof theoretic ordinal $\theta\Omega^\omega$, as defined in [RW93].

THEOREM 0.9A.5. Π^1_2 -TI $_0$ is a conservative extension of $ATR(\langle \theta\Omega^\omega)$ for Π^1_1 sentences. The provably recursive functions of Π^1_2 -TI $_0$ and $ATR(\langle \theta\Omega^\omega)$ are the $\langle \theta\Omega^\omega$ recursive functions. The following are provably equivalent in RCA_0 .

i. Π^1_1 reflection on Π^1_2 -TI $_0$.

ii. $\theta\Omega^\omega$ is well ordered.

These are provable in Π^1_2 -TI but not in Π^1_2 -TI $_0$.

THEOREM 0.9A.6. Π^1_2 -TI $_0$ is a conservative extension of $ATI(\langle \theta\Omega^\omega)$. The following are provably equivalent in SEFA.

i. 1-Con(Π^1_2 -TI $_0$).

ii. 1-Con($ATR(\langle \theta\Omega^\omega)$).

iii. 1-Con($ATI(\langle \theta\Omega^\omega)$).

iv. Every primitive recursive (elementary recursive, polynomial time computable) sequence from $\theta\Omega^\omega$ stops descending.

These are provable in Π^1_2 -TI but not in Π^1_2 -TI $_0$.

0.9B. Kruskal's Theorem.

A poset is a pair (D, \leq) where D is a nonempty set and \leq is a reflexive transitive relation obeying

$$(x \leq y \wedge y \leq x) \rightarrow x = y.$$

A tree is a poset $T = (V, \leq)$ where there is a minimum element called the root, and where for each $x \in V$, $\{y: y \leq x\}$ is linearly ordered by \leq .

The elements of $V = V(T)$ are called the vertices of T . A tree is said to be finite if it has finitely many vertices.

If $x < y$ then we call x a predecessor of y and y a successor of x .

If $x < y$ and there is no z such that $x < z < y$ then we call y an immediate successor of x and x the immediate predecessor of y .

We say that x, y are comparable if and only if $x = y \vee x < y \vee y < x$. Otherwise, we say that x, y are incomparable.

For finite trees, we have the crucial inf operation on V , where $x \text{ inf } y$ is the greatest z such that $z \leq x \wedge z \leq y$.

The valence of a vertex is the number of its immediate successors. The valence of a tree is the maximum of the valences of its vertices (for finite trees).

The vertices of valence 0 are called the terminal vertices. The remaining vertices are called the internal vertices.

For definiteness, we will require that the domain of any finite tree is $\{1, \dots, n\}$, where n is the number of its vertices. Thus the set of all finite trees exists. Note that many pairs of distinct finite trees are isomorphic.

We will also consider what we call structured trees. These are finite trees with a left/right structure. I.e., where for any vertex i , there is a strict linear ordering (left/right) of the immediate successors of i . This induces the following relation on vertices: x is to the left of y if and only if x, y are incomparable and the immediate successor of $x \text{ inf } y$ comparable with x is to the left of the immediate successor of $x \text{ inf } y$ comparable with y . This relation is irreflexive and transitive.

A quasi order is a pair (D, \leq) where D is a nonempty set and \leq is a reflexive and transitive relation on D .

A well quasi order (wqo) is a quasi order (D, \leq) , where for any x_1, x_2, \dots from D , there exists $i < j$ such that $x_i \leq x_j$.

Let (D, \leq) be a quasi order. A (D, \leq) labeled (structured) tree is a (structured) tree with a labeling function from its vertices into D . We write $l(x)$ for the label of x . Although we consider only finite (D, \leq) labeled (structured) trees, the D itself may be infinite.

We introduce the following notation for certain important tree classes. Here Q is a quasi order.

$TR(n)$. The finite trees of valence $\leq n$.
 $TR(<\infty)$. The finite trees.
 $TR(n;Q)$. The finite Q labeled trees of valence $\leq n$.
 $TR(<\infty;Q)$. The finite Q labeled trees.
 $STR(n)$. The finite structured trees of valence $\leq n$.
 $STR(<\infty)$. The finite structured trees.
 $STR(n;Q)$. The finite Q labeled structured trees of valence $\leq n$.
 $STR(<\infty;Q)$. The finite Q labeled trees.

If we write an integer $r \geq 2$ instead of Q , then we mean the quasi order $Q = \{1, \dots, r\}$ under $=$. If we write ω instead of Q , then we mean the quasi order of ω under \leq (which is the usual linear ordering).

All of these tree classes come with their own notion of embedding.

$TR(n)$, $TR(<\infty)$. We say that h is an embedding from S into T if and only if $h:V(S) \rightarrow V(T)$, where for all $x, y \in V(S)$, $x \leq_S y \Leftrightarrow hx \leq_T hy$.

$STR(n)$, $STR(<\infty)$. We say that h is an embedding from S into T if and only if $h:V(S) \rightarrow V(T)$, where for all $x, y \in V(S)$

- i. $x \leq_S y \Leftrightarrow hx \leq_T hy$.
- ii. x is to the left of y in S if and only if hx is to the left of hy in T .

$TR(n;Q)$, $TR(<\infty;Q)$. We say that h is an embedding from S into T if and only if $h:V(S) \rightarrow V(T)$, where for all $x, y \in V(S)$,

- i. $x \leq_S y \Leftrightarrow hx \leq_T hy$.
- iii. $l(x) \leq_Q l(hx)$.

$STR(n;Q)$, $STR(<\infty;Q)$. We say that h is an embedding from S into T if and only if $h:V(S) \rightarrow V(T)$, where for all $x, y \in V(S)$,

- i. $x \leq_S y \Leftrightarrow hx \leq_T hy$.
- ii. x is to the left of y in S if and only if hx is to the left of hy in T .
- iii. $l(x) \leq_Q l(hx)$.

Additional conditions are often placed on embeddings.

Inf Preservation. $h:V(S) \rightarrow V(T)$ is said to be inf preserving if and only if for all $x, y \in V(S)$, $h(x \text{ inf } y) = hx \text{ inf } hy$.

Valence Preservation. $h:V(S) \rightarrow V(T)$ is said to be valence preserving if and only if for all x in $V(S)$, the valence of x is the same as the valence of hx .

In this section, we will always use inf preservation.

THEOREM 0.9B.1. Kruskal's Tree Theorem. If Q is a wqo then $STR(<\infty;Q)$ is a wqo under inf preserving embeddability.

Proof: This was proved in [Kr60]. The simplest proof is in [NW65]. The proof is not any easier for $TR(<\infty,Q)$. QED

THEOREM 0.9B.2. Higman's Wqo Theorem. If Q is a wqo then $STR(n;Q)$ is a wqo under inf and valence preserving embeddability.

Proof: See [Hig52]. This is weaker than Kruskal's Theorem (except for the valence preserving), but predates it. It is easy to encode the valence in the labels, so that this is easily obtained from Kruskal's Tree Theorem. The original language in [Hig52] is couched in algebraic terms, and our present reformulation is in terms of trees. QED

THEOREM 0.9B.3. Theorems 0.9B.1 and 0.9B.2 are provable in Π^1_2 -TI. For each fixed $n \geq 1$, Theorem 0.9B.2 is provable in Π^1_2 -TI₀.

Proof: This is proved in [Fr84]. Provability in TI is in [Fr81a]. QED

THEOREM 0.9B.4. The following are provably equivalent in RCA_0 .

- i. $TR(<\infty)$ is a wqo under inf preserving embeddability.
- ii. For all n , $TR(n)$ is a wqo under inf preserving embeddability.
- iii. For all n,r , $TR(n;r)$ is a wqo under inf and valence preserving embeddability.
- iv. For all n , $TR(n;\omega)$ is a wqo under inf and valence preserving embeddability.
- v. $STR(<\infty)$ is a wqo under inf preserving embeddability.
- vi. For all n , $STR(n)$ is a wqo under inf preserving embeddability.
- vii. For all n,r , $STR(n;r)$ is a wqo under inf and valence preserving embeddability.
- viii. For all n , $STR(n;\omega)$ is a wqo under inf and valence preserving embeddability.
- ix. $\theta\Omega^\omega$ is well ordered.

In particular, i-ix are provable in $\Pi_2^1\text{-TI}$, but not in $\Pi_2^1\text{-TI}_0$.

THEOREM 0.9B.4. The following are provably equivalent in RCA_0 .

- i. $\text{STR}(<\omega)$ is a wqo under inf preserving embeddability.
- ii. For all n , $\text{TR}(n)$ is a wqo under inf preserving embeddability.
- iii. For all n , $\text{STR}(n;\omega)$ is a wqo under inf and valence preserving embeddability.
- iv. $\theta\Omega^\omega$ is well ordered.

In particular, i-iii are provable in $\Pi_2^1\text{-TI}$, but not in $\Pi_2^1\text{-TI}_0$.

Proof: The equivalence of i,iii,iv is in [Fr84], using Theorem 0.9A.6. The implication iii \rightarrow iv is by assigning ordinals to trees. The implication iv \rightarrow iii uses the provability in $\Pi_2^1\text{-TI}_0$ of iii for each fixed n .

For unstructured trees, ii $\rightarrow \Gamma_0$ is well ordered was shown in [Fr81a], and appeared in [Si85]. ii \rightarrow iv appears in [RW93], p. 53, extending the construction (it was attributed to us in [Si85]). Hence i-iii are equivalent to iv. QED

THEOREM 0.9B.5. The following are provable in $\Pi_2^1\text{-TI}$.

- i. If Q is a countable wqo then $\text{STR}(<\omega;Q)$ is a wqo under inf preserving embeddability.
 - ii. If Q is a countable wqo and $n < \omega$, then $\text{STR}(n;Q)$ is a wqo under inf and valence preserving embeddability.
- For each fixed n , ii) is provable in $\Pi_2^1\text{-TI}_0$.

Proof: This is proved in [Fr84]. QED

We now come to effective and finite forms of Kruskal's Theorem.

THEOREM 0.9B.6. Subrecursive Kruskal Theorem. In any infinite primitive recursive (elementary recursive, polynomial time computable) sequence of finite trees, one tree is embeddable in a later tree.

THEOREM 0.9B.7. Recursive Kruskal Theorem. In any infinite recursive sequence of finite trees, one tree is inf preserving embeddable in a later tree.

THEOREM 0.9B.8. Finite Kruskal Theorem. For all $c \geq 0$ there exists n such that the following holds. Let T_1, \dots, T_n be

finite trees, where each T_i has at most $i+c$ vertices. There exist $i < j$ such that T_i is inf preserving embeddable in T_j .

The finite Kruskal theorem has been refined in an interesting way in [LM87].

For $f:N \rightarrow N$, let FKT_f assert the following.

For all $c \geq 0$ there exists n such that the following holds. Let T_1, \dots, T_n be finite trees, where each T_i has at most $f(i)+c$ vertices. There exist $i < j$ such that T_i is inf preserving embeddable in T_j .

The following is proved in [LM87].

Let $f_r(i)$ be $r(\log_2(i))$. If $r \leq 0.5$ then PA does prove FKT_{f_r} .

If $r \geq 4$ then PA does not prove FKT_{f_r} .

Note the gap between .5 and 4. In [We03] there is an exact calculation of the transition point from PA provability to PA unprovability, using analytic combinatorics.

This result led to further systematic investigations on critical phenomena related to independence results. For example, the phase transition corresponding to the relatively large Ramsey theorem is classified in [We04]. Also see [We09].

There is also a phase transition analysis of the regressive Ramsey theorems (see section 0.8D and [KM87]). See [CLW11].

We now proceed from Theorem 0.9B.4 exactly as we proceeded from Theorem 0.8H.3 in section 0.8H.

THEOREM 0.9B.9. The following are provably equivalent in SEFA.

- i. Subrecursive Kruskal Theorem.
- ii. Finite Kruskal Theorem.
- iii. Every primitive recursive sequence from $\theta\Omega^\theta$ stops descending.
- iii. $1\text{-Con}(\text{ATI}(<\theta\Omega^\theta))$.
- iv. $1\text{-Con}(\Pi^1_2\text{-TI}_0)$.

THEOREM 0.9B.10. The following are provably equivalent in SEFA.

- i. Recursive Kruskal Theorem.
- ii. Every recursive sequence from $\theta\Omega^\theta$ stops descending.

- iii. $2\text{-Con}(\text{ATI}(\langle \theta \Omega^m \rangle))$.
- iv. $2\text{-Con}(\Pi_2^1\text{-TI}_0)$.

We now focus on Γ_0 and ATR_0 .

THEOREM 0.9B.11. The following are provably equivalent in RCA_0 .

- i. $\text{TR}(2;2)$ is a wqo under inf preserving embeddability.
- ii. $\text{STR}(2;2)$ is a wqo under inf preserving embeddability.
- iii. Γ_0 is well ordered.

In particular, i-iii are provable in ATR but not in ATR_0 .

Proof: ii \leftrightarrow iii is in [Fr84]. i \rightarrow ii is a result of A. Weiermann that will appear in [FWa]. QED

Again, proceeding as before, we obtain the following.

THEOREM 0.9B.12. The following are provably equivalent in SEFA .

- i. Subrecursive Kruskal Theorem for $\text{TR}(2;2)$.
- ii. Finite Kruskal Theorem for $\text{STR}(2;2)$.
- iii. Every primitive recursive sequence from Γ_0 stops descending.
- iv. $1\text{-Con}(\text{ATI}(\langle \Gamma_0 \rangle))$.
- v. $1\text{-Con}(\text{ATR}_0)$.

An old unpublished result of ours from the 1980's also concerns binary trees. See [FMW ∞] for planned publication. Here is the result in its most primitive form.

THEOREM 0.9B.13. $\text{RCA}_0 +$ "If Q is a countable wqo, then $\text{TR}(2;Q)$ is a wqo under inf preserving embeddability", proves ATR_0 .

Here is a more refined form. Let $\text{TR}^*(2;Q)$ be the set of finite trees of valence ≤ 2 , where vertices of valence 2 are unlabeled, and vertices of valence 0 or 1 are labeled from Q . Embeddings are required to be label increasing (\geq) on the labeled vertices. Both forms will appear in [FWb].

THEOREM 0.9B.14. The following are provably equivalent in RCA_0 .

- i. If Q is a countable wqo, then $\text{TR}^*(2;Q)$ is wqo under inf preserving embeddability.
- ii. If X is a well ordering then θX_0 is a well ordering.
- iii. ATR_0 .

In [Fr02] the innovation was to use internal tree embeddings in favor of sequences of trees.

We use the following important subclass of $TR(k;n)$. We define $FUTR(n;m)$ as the set of all $T \in TR(k;n)$ such that

- i. All vertices of valence 0 have the same height.
- ii. All vertices are of valence 0 or k .

Here FU means "full".

The height of a vertex in a finite tree is the number of its predecessors. Thus the height of the root is 0. The height of a finite tree is the maximum of the heights of its vertices.

Let $T \in FUTR(k;n)$. The truncations of T are obtained by restricting T to all vertices whose height is at most a given nonnegative integer. Thus the number of truncations of T is exactly one more than the height of T .

THEOREM 0.9B.15. Internal Finite Tree Embedding Theorem. Let $k, n \geq 1$ and $T \in FUTR(k;n)$ be sufficiently tall. There is an inf and valence preserving embedding from some truncation of T into some truncation of T of greater height.

Proof: This appears as Theorem 1.3 in [Fr02]. Fix $k, n \geq 1$, and suppose this is false. Then we obtain a finitely branching tree of counterexamples, growing in height as we go up the tree. Therefore there is an infinite path, which forms an infinite full n -labeled tree S of valence k . Now look at its sequence of finite truncations, S_0, S_1, \dots . As a consequence of iii in Theorem 0.9B.4, there exists $i < j$ such that S_i is inf and valence preserving embeddable into S_j . This contradicts the construction of the tree of counterexamples. QED

THEOREM 0.9B.16. The following are provably equivalent in SEFA.

- i. Internal Finite Tree Embedding Theorem.
- ii. Version of i) for structured trees.
- iii. Every primitive recursive descending sequence through $\theta\Omega^\theta$ stops descending.
- iv. $1\text{-Con}(\text{ATI}(\langle \theta\Omega^\theta \rangle))$.
- v. $1\text{-Con}(\Pi_2^1\text{-TI}_0)$.

For valence 2, SEFA proves that i) implies $1\text{-Con}(\text{ATI}(\langle \Gamma_0 \rangle))$, and, equivalently, $1\text{-Con}(\text{ATR}_0)$.

Proof: See [Fr02]. For valence 2, Γ_0 here can be raised to ordinals considerably higher than, say, Γ_{ϵ_0} , thereby going past ATR. QED

0.9C. Comparability.

A number of Comparability Theorems are known to be equivalent to ATR_0 over RCA_0 . They are naturally in Π^1_2 form. By Theorem 0.9A.3 and the comments after its proof, they are not predicatively provable in a strong sense.

The original Comparability Theorem equivalent to ATR_0 , was the comparability of well orderings. See i) in the next theorem.

THEOREM 0.9C.1 The following are provably equivalent in RCA_0 .

- i. For any two countable well orderings, there is an order preserving map from one onto an initial segment of the other.
- ii. For any two countable well orderings, there is an order preserving map from one into the other.
- iii. ATR_0 .

Proof: $i \leftrightarrow iii$ is a result of ours that appears in [Si99,09], section V.6. (The derivation of ATR_0 (ATR) from i) in [St76], that was cited in [Si99,09] as an "early" version, uses a technical strengthening of $\Delta^1_1\text{-CA}$ for the base theory.) For $ii \leftrightarrow iii$, see [FH90]. QED

THEOREM 0.9C.2. The following are provably equivalent in RCA_0 .

- i. For any two countable metric spaces, there is a pointwise continuous one-one map from one into the other.
- ii. For any two sets of rationals, there is a pointwise continuous one-one map from one into the other.
- iii. For any two compact well ordered sets of rationals, there is a pointwise continuous one-one map from one into the other.
- iv. For any two closed sets of reals, there is a pointwise continuous one-one map from one into the other.
- v. ATR_0 .

Proof: See [Fr05a]], Theorem 4.5. We were the first to prove i,ii even in ZFC. Comparability for closed sets of reals was known much earlier - although we don't know of a reference.

We now verify $v \rightarrow iv$. If A is uncountable, then A has a perfect subset (uses ATR_0). Hence B will continuously embed in A , unless B has interior (this requires at most ACA_0). But if B has interior, then A continuously embeds in B (this is obviously in RCA_0). This establishes comparability if at least one of the two sets is uncountable. If both are countable, then we are in a special case of i). QED

There is a natural descriptive set theoretic consequence one can draw immediately from the fact that a Π^1_2 sentence implies ATR_0 over RCA_0 . Actually we can use ACA .

THEOREM 0.9C.3. Let φ be a Π^1_2 sentence, and suppose that ACA proves $\varphi \rightarrow ATR_0$. Then φ has no Borel choice function.

Proof: Suppose φ is $(\forall x)(\exists y)(A(x, y))$, where A is arithmetical, and ACA proves $\varphi \rightarrow ATR_0$. Suppose $(\forall x)(A(x, fx))$, where f is Borel. Choose a countable set $K \subseteq \wp(\omega)$ such that K is f closed and arithmetically closed. Then K forms an ω model of $ACA + \varphi$, where K is contained in the hyperarithmetical sets. Hence K forms an ω model of ATR_0 , contradicting Theorem 0.9A.3. QED

0.10. Incompleteness in Iterated Inductive Definitions and Π^1_1 - CA_0 .

0.10A. Preliminaries.

0.10B. Extended Kruskal and Graph Minors.

0.10C. Extended Hercules Hydra Game.

0.10D. Equivalences with Π^1_1 - CA_0 .

0.10A. Preliminaries.

We discuss three kinds of Concrete Mathematical Incompleteness in this section.

The first is our extension of the work on finite trees discussed in section 0.9B. The second is an extension of the work on the Hercules Hydra Game discussed in section 0.8E. The third is equivalences with Π^1_1 - CA_0 .

Here is the basic proof theoretic information on Π^1_1 - CA_0 . The theories of iterated inductive definitions, ID_n , do not have any quantifiers over sets, but instead introduce predicate symbols for inductively defined sets. The predicates introduced in ID_1 correspond to Π^1_1 sets, whereas, the predicates introduced in ID_n , $n \geq 2$, correspond

to sets Π_1^1 in the $(n-1)$ -st hyperjump of 0. $ID_{<\omega}$ is the union of the ID_n , $n \geq 1$. See [BFPS81].

The following reduction of Π_1^1 -CA₀ to $ID_{<\omega}$ prepared the way for a proof theoretic analysis of Π_1^1 -CA₀ via a proof theoretic analysis of the ID_n .

THEOREM 0.10A.1. Π_1^1 -CA₀ proves Con(TI). In fact, Π_1^1 -CA₀ proves the existence of a β -model of TI. Π_1^1 -CA₀ is a conservative extension of $ID_{<\omega}$ for arithmetical sentences. In fact, it is a conservative extension of $ID_{<\omega}$ for sentences of the form "n lies in Kleene's O".

Proof: For the first two claims, see [Fr69]. For the last two claims, see [Fr70]. These papers appeared before my focus on systems with only set induction, such as RCA₀, ACA₀, WKL₀, ATR₀, and Π_1^1 -CA₀, in connection with our introduction of the Reverse Mathematics program. These systems were introduced in [Fr76] (the systems RCA, WKL, ATR in [Fr75], with ACA, Π_1^1 -CA having been previously formulated by others, including S. Feferman and G. Kreisel). The proof in [Fr69] is carried out in Π_1^1 -CA₀. In [Fr70], the considerably more involved result that Π_1^1 -CA (even Σ_2^1 -AC) is a conservative extension $ID_{<\omega}$ is established. After we introduced the naught systems, it was evident that a specialization and simplification of the proof establishes the last two claims (even for Σ_2^1 -AC₀). QED

Here is the basic proof theory for Π_1^1 -CA₀. See [BFPS81], [Tak75], and [Sch77] for proofs.

THEOREM 0.10A.2. Π_1^1 -CA₀ is a conservative extension of $ATR(<\theta\Omega_\omega)$ for Π_1^1 sentences. The provably recursive functions of Π_1^1 -CA₀ and $ATR(<\theta\Omega_\omega)$ are the $<\theta\Omega_\omega$ recursive functions. The following are provably equivalent in RCA₀.

- i. Π_1^1 reflection on Π_1^1 -CA₀.
- ii. $\theta\Omega_\omega$ is well ordered.

These are provable in Π_1^1 -CA but not in Π_1^1 -CA₀.

For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

THEOREM 0.10A.3. Π_1^1 -CA₀ is a conservative extension of $ATI(<\theta\Omega_\omega)$. The following are provably equivalent in SEFA.

- i. 1-Con(Π_1^1 -CA₀).
- ii. 1-Con($ATR(<\theta\Omega_\omega)$).
- iii. 1-Con($ATI(<\theta\Omega_\omega)$).

iv. Every primitive recursive (elementary recursive, polynomial time computable) sequence from $\theta\Omega_\omega$ stops descending.

These are provable in Π_1^1 -CA but not in Π_1^1 -CA₀.

0.10B. Extended Kruskal and Graph Minors.

In [Fr82], we sought to strengthen Kruskal's theorem in a way that would make it independent of yet stronger systems such as Π_1^1 -CA₀. We succeeded with this through our introduction of the gap embedding condition. This turned out to have profound connections with ongoing work at the time by Robertson and Seymour on their Graph Minor Theorem. In fact, it completely encapsulates the only logically high level part of their proof, at least in the case of bounded tree width.

The gap condition concerns the tree classes $TR(k;n)$ and $STR(k;n)$ from section 0.9B. Let $S, T \in TR(k;n)$ (or $STR(k;n)$). We say that h is a gap embedding from S into T if and only if h is an embedding from S into T such that for all $x, y \in V(S)$, if y is an immediate successor of x , then for all z in the gap (hx, hy) , $l(z) \geq l(hy)$.

THEOREM 0.10B.1. The Extended Kruskal Theorem. For $k, n \geq 1$, $TR(k;n)$ ($STR(k;n)$) is wqo under inf preserving gap embeddability.

Proof: See [Fr82], [Si85]. QED

THEOREM 0.10B.2. The following are provably equivalent in RCA_0 .

- i. Extended Kruskal Theorem (structured and unstructured).
- ii. Extended Kruskal Theorem for full binary trees (structured and unstructured).
- iii. $\theta\Omega_\omega$ is well ordered.

These are provable in Π_1^1 -CA but not in Π_1^1 -CA₀.

Proof: See [Fr82] for $i \rightarrow iii$ (unstructured), and a proof of i) (structured) for each k, n , in Π_1^1 -CA₀. Applying 0.10A.2, we have $i \leftrightarrow iii$. For $ii \rightarrow i$ (unstructured), see [FRS87]. Also see [Si85] and [Fr02]. QED

Let G, H be finite graphs. We say that G is minor included in H if and only if G can be obtained from H (up to isomorphism) by successive applications of the following operations.

- i. Deleting a vertex (and all edges involving that vertex).
- ii. Deleting an edge.
- iii. Contracting an edge. I.e., if v,w is an edge, $v \neq w$, remove w and replace all edges involving w that are not loops by replacing w with v .

The Graph Minor Theorem asserts that in any infinite sequence of finite graphs, one graph is minor included in a later one. The Graph Minor Theorem is proved in a series of papers culminating with [RS04].

The entire proof consists of very detailed structure theory, with a brief logically strong part, involving minimal bad sequence constructions. We communicated our earlier Extended Kruskal Theorem to Robertson and Seymour. Robertson and Seymour adapted and extended these ideas to their later proof of the Graph Minor Theorem.

The Bounded Graph Minor Theorem is the Graph Minor Theorem specialized to trees of bounded tree width (see [FRS87]).

Our work on the Extended Kruksal Theorem was applied in a striking way to the Graph Minor Theorem in [FRS87].

THEOREM 0.10B.3. The following are provably equivalent in RCA_0 .

- i. Extended Kruskal Theorem (structured and unstructured).
- ii. Bounded Graph Minor Theorem.
- iii. $\theta\Omega_\omega$ is well ordered.

These are provable in $\Pi^1_1\text{-CA}$ but not in $\Pi^1_1\text{-CA}_0$.

Proof: See [FRS87]. QED

As before, we obtain subrecursive, recursive, and finite forms.

THEOREM 0.10B.4. The following are provably equivalent in SEFA.

- i. Extended Kruskal Theorem for primitive recursive (elementary recursive, polynomial time computable) sequences of finite trees (all four forms above).
- ii. Bounded Graph Minor Theorem for primitive recursive (elementary recursive, polynomial time computable) sequences of finite graphs.
- iii. $1\text{-Con}(\Pi^1_1\text{-CA}_0)$.
- iv. $1\text{-Con}(\text{ATI}(\langle \theta\Omega_\omega \rangle))$.

These are provable in $\Pi^1_1\text{-CA}$ but not in $\Pi^1_1\text{-CA}_0$.

Proof: The ordinal assignments involved are very effective, and i,ii are Π^0_2 statements. Use that for a fixed number of labels, or fixed tree width, the statements are provable in Π^1_1 -CA₀. QED

THEOREM 0.10B.5. The following are provably equivalent in SEFA.

- i. Extended Kruskal Theorem for recursive sequences of finite trees (all four forms above).
- ii. Bounded Graph Minor Theorem for recursive sequences of finite graphs.
- iii. Every recursive sequence from $\theta\Omega_\omega$ stops descending.
- iii. 2-Con(Π^1_1 -CA₀).
- iv. 2-Con(ATI($\langle\theta\Omega_\omega\rangle$)).

These are provable in Π^1_1 -CA but not in Π^1_1 -CA₀.

Proof: See the proof of Theorem 0.8H.10. QED

We can proceed with the finite forms. For the Extended Kruskal Theorems, there are no surprises. We can use my usual finite sequences where the i-th term has at most i+c vertices, where the parameter c is universally quantified.

THEOREM 0.10B.6. The following are provably equivalent in SEFA.

- i. The Finite Extended Kruskal Theorem (all four forms above).
- ii. 1-Con(Π^1_1 -CA₀).
- iii. 1-Con(ATI($\langle\theta\Omega_\omega\rangle$)).

These are provable in Π^1_1 -CA but not in Π^1_1 -CA₀.

In [Fr02], the following Internal Embedding Theorem is treated.

THEOREM 0.10B.7. The Internal Finite Tree Gap Embedding Theorem. Let $k, n \geq 1$ and $T \in \text{FUTR}(k;n)$ be sufficiently tall. There is an inf and valence preserving gap embedding from some truncation of T into some truncation of T of greater height.

Proof: This appears as Theorem 7.7 in [Fr02]. QED

THEOREM 0.10B.8. The following are provably equivalent in SEFA.

- i. Internal Finite Tree Gap Embedding Theorem.
- ii. Variants of i) with structure and/or with valence 2.
- iii. Every primitive recursive sequence from $\theta\Omega_\omega$ stops descending.

iii. $1\text{-Con}(\text{ATI}(\langle \theta\Omega_\omega \rangle))$.

iv. $1\text{-Con}(\Pi_2^1\text{-TI}_0)$.

For valence 2, EFA proves that i) implies $1\text{-Con}(\text{ATI}(\langle \Gamma_0 \rangle))$, and, equivalently, $1\text{-Con}(\text{ATR}_0)$.

Proof: See [Fr02]. QED

The following Finite Bounded Graph Minor Theorem is treated in [FRS87].

THEOREM 0.10B.9. Finite Bounded Graph Minor Theorem. For all $p, c \geq 1$ there exists n such that the following holds. Let G_1, \dots, G_n be finite graphs of tree-width $\leq p$, where each $|G_i| \geq i+c$. There exist $i < j$ such that $G_i \leq_m G_j$.

Here $|G|$ denotes the sum of the number of vertices and edges in G , and \leq_m denotes graph minor inclusion.

THEOREM 0.10B.10. The following are provably equivalent in SEFA.

i. The Finite Bounded Graph Minor Theorem.

ii. Every primitive recursive sequence from $\theta\Omega_\omega$ stops descending.

iii. $1\text{-Con}(\text{ATI}(\langle \theta\Omega_\omega \rangle))$.

iv. $1\text{-Con}(\Pi_1^1\text{-CA}_0)$.

Proof: See [FRS87]. QED

It remains unclear just what is required to prove the full Graph Minor Theorem. Its proof has not been subject to a logical analysis sufficient to determine a reasonable upper bound.

0.10C. Extended Hercules Hydra Game.

The following treatment is taken directly from [Bu87].

A (Buchholz) hydra is a finite rooted planar labeled tree H which has the following properties:

i. The root has label $+$.

ii. Any other node of A is labeled by some ordinal $\alpha \leq \omega$,

iii. All nodes immediately above the root of H have label 0 .

If Hercules chops off a head (i.e. a top node) s of a given hydra, the hydra will choose an arbitrary number n and transform itself into a new hydra $H(s, n)$ as follows. Let t

be the node of H which is immediately below s , and let H^- denote the part of H which remains after s has been chopped off. The definition of $H(s,n)$ depends on the label of s .

case 1. $\text{label}(s) = 0$. If t is the root of H , we set $H(s,n) = H^-$. Otherwise $H(s,n)$ results from H^- by sprouting n replicas of H_{t^-} , from the node immediately below t . Here H_{t^-} denotes the subtree of H^- determined by t .

case 2. $\text{label}(s) = u+1$. Let e be the first node below s with a label $v \leq u$. Let T be that tree which results from the subtree H_e by changing the label of e to u and the label of s to 0 . $H(s,n)$ is obtained from H by replacing s by T . In this case $H(s,n)$ does not depend on n .

Case 3: $\text{label}(s) = \omega$. $H(s,n)$ is obtained from H simply by changing the label of s (which is ω) to $n+1$.

Let $H(n)$ be $H(s,n)$ where s is the rightmost head. Let $(+)$ be the hydra which consists of one node, namely its root. Let H^n be the hydra consisting of a chain of $n+2$ nodes where the root has label $+$, the successor of the root has label 0 and where all other nodes have label ω .

THEOREM. Let H be a fixed hydra. $\Pi_1^1\text{-CA} + \text{BI}$ proves that for all number theoretic functions F there exists k such that $H(F(1))(F(2))\dots(F(k)) = (+)$.

THEOREM. $\Pi_1^1\text{-CA} + \text{BI}$ does not prove that for all n there exists a k such that $H^n(1)(2)\dots(k) = (+)$.

0.10D. Equivalences with $\Pi_1^1\text{-CA}_0$.

There are a number of interesting equivalences with $\Pi_1^1\text{-CA}_0$.

THEOREM 0.10D.1. The following are provably equivalent in RCA_0 .

- i. Every tree of finite sequences of natural numbers with an infinite path, has a leftmost infinite path.
- ii. Every tree of finite sequences of natural numbers (bits) has a perfect subtree which contains all perfect subtrees.
- iii. If a quasi order on \mathbb{N} is not a wqo then it has a minimal bad sequence.
- iv. Every countable Abelian group G has a divisible subgroup which contains all divisible subgroups of G .
- v. $\Pi_1^1\text{-CA}_0$.

Proof: Clearly $v) \rightarrow i)$. Assume $i)$. Let T_1, T_2, \dots be any infinite sequence of finite sequence trees from N . We will derive the existence of $\{i: T_i \text{ has an infinite path}\}$. This is a well known equivalent of $\Pi^1_1\text{-CA}_0$ over RCA_0 (see [Si99,09], Lemma VI.1.1).

Let S be the tree of sequences $x[1], \dots, x[n]$, $n \geq 0$, from N , with the following properties.

- a. If $p \leq n$ is not a power of a prime, then $x[p] = 1$.
- b. Let $p \leq n$ be a prime, and $r \geq 1$ be largest such that $p^r \leq n$. Then
 - b.1. $x[p], x[p^2], \dots, x[p^r] = 1$; or
 - b.2. $x[p] = 0$, and $x[p^2], \dots, x[p^r]$ forms a path of length $r-1$ through T_i , starting at an immediate successor of the root (a length 1 sequence), where p is the i -th prime, and we view each term as coding a finite sequence from N .

S will have the infinite path $1, 1, \dots$. Let $x[1], x[2], \dots$ be a (the) leftmost infinite path P through S . Let p be the i -th prime. If $x[p] = 0$ then there is a path through T_i . Suppose $x[p] = 1$ and there is a path Q through T_i . Then we can retain the first $p-1$ terms, lower the p -th term to 0, and use Q so that we have another infinite path through S which is to the left of P . This is a contradiction. Hence $x[p] = 0$ if and only if there is an infinite path through T_i . Therefore $\{i: T_i \text{ has an infinite path}\}$ exists.

For $ii \leftrightarrow v$, see [Si99,09], Theorem VI.1.3.

For $iii \leftrightarrow v$, see [Mar96], Theorem 6.5.

In $\Pi^1_1\text{-CA}_0$, we can construct the union of all divisible subgroups, and so obviously $v \rightarrow iv$. Now suppose iv .

In [FSS87] it is shown that "every countable Abelian group is a direct sum of a divisible group and a reduced group" is equivalent to $\Pi^1_1\text{-CA}_0$ over RCA_0 (see [Si99,09], Theorem VI.4.1).

With a little bit of care, the derivation of $\Pi^1_1\text{-CA}_0$ there can be accomplished with just iv). QED

Here is a somewhat different kind of example.

THEOREM 0.10D.2. The following are provably equivalent in RCA_0 .

- i. Every countable algebra with an infinitely generated subalgebra has a maximal infinitely generated subalgebra.
- ii. Proposition i) for a single binary function.
- iii. Proposition i) for two unary functions.
- iv. Π_1^1 -CA₀.

Proof: See [Fr05b]. QED

The Borel Ramsey theorem, also known as the Galvin/Prikry theorem, asserts the following. Let $S \subseteq \wp(N)$ be Borel. There exists an infinite $A \subseteq N$ such that all infinite subsets of A lie in S , or all infinite subsets of A lie outside S .

With its use of Borel measurable sets of arbitrary high countable rank, the Borel Ramsey theorem is an example just beyond Concrete Mathematics.

We rely on the standard treatment of Borel sets in $\wp(N)$ in order to formulate the Borel Ramsey theorem in the language of RCA₀. This is achieved through the use of Borel codes, and is discussed in some detail in section 0.11.

Π_1^1 -TR₀ consists of ACA₀ together with Π_1^1 transfinite recursion. This is the same as arithmetic transfinite recursion - as in ATR₀ - except that the formula to which transfinite recursion is being applied is allowed to be Π_1^1 . This is equivalent to the existence of the hyperjump hierarchy on every countable well ordering, starting with any subset of ω .

Borel sets in and functions between complete separable metric spaces lie just beyond what we regard as Concrete Mathematics. We take finitely Borel to be at the outer limits of Concrete Mathematics.

Everything in sections 0.11, 0.12, and much of section 0.13, will be focused at this borderline between Concrete and Abstract Mathematics.

Some care is needed to properly formalize Borel sets and functions in RCA₀. A standard way of doing this has emerged. This will be discussed in section 0.11.

The Borel Ramsey Theorem sits in the context of $\wp(N)$ as a complete separable metric space, under $d(A, B) = 2^{-n}$, where $n = \min(A \Delta B)$ if $A \neq B$; 0 otherwise. It asserts that for any

Borel $S \subseteq \wp(N)$, there exists infinite $A \subseteq N$ such that $\wp(A) \subseteq S$ or $\wp(A) \cap S = \emptyset$.

THEOREM 0.10D.3. The following are provably equivalent in RCA_0 .

- i. The Borel Ramsey Theorem (or Galvin/Prikry Theorem).
- ii. Π^1_1 -TR₀.

Proof: See [Tan89]. QED

THEOREM 0.10D.4. The following are provably equivalent in RCA_0 .

- i. The Borel Ramsey Theorem (or Galvin/Prikry Theorem) for finitely Borel subsets of $\wp(N)$.
 - ii. $(\forall x \subseteq N)(\forall n)$ (the n -th hyperjump of x exists).
- In particular, i implies Π^1_1 -CA₀, and follows from Π^1_1 -CA (Π^1_1 -CA₀ with full induction).

L. Gordeev and I. Kriz have proved some transfinite extensions of my Extended Kruskal Theorem (Theorem 0.10B.1) using much stronger principles than Π^1_1 -CA₀. See [Gor89], [Gor90], [Gor93], [Kri89a], [Kri89b], [Kri95]. The proof of the main theorem of [Kri89b] given there (which was a conjecture of mine) requires Π^1_2 -CA₀. However, this was later sharply reduced to Π^1_1 -TR₀ by [Gor90], [Gor93], with a reversal to a level corresponding to Π^1_1 -TR₀.

There are a number of interesting mathematical statements which have been proved using systems significantly stronger than Π^1_1 -CA₀ - but it remains unknown whether that is necessary. We have already mentioned the Graph Minor Theorem.

Nash-Williams proved that infinite trees are wqo under inf preserving embeddability. See [NW65], [NW68], where his notions of better quasi orders and minimal bad arrays were introduced. He uses much stronger principles than Π^1_1 -CA₀. It is not known whether this is required. [Si85a] simplifies the notion of better quasi order. Also see [EMS87].

R. Laver proved in [La71] that the linear orderings on N form a wqo under embeddability. This is known as Fraïssé's conjecture. In [Sho93] this theorem is shown to imply ATR₀ over RCA_0 . However, it is not known if ATR₀ is sufficient, or even whether Π^1_1 -CA₀ and much stronger systems are sufficient. Π^1_2 -CA₀ certainly suffices. [Si85a] simplifies the proof of Fraïssé's conjecture.

0.11. Incompleteness in Second Order Arithmetic and ZFC\P.

0.11A. Preliminaries.

0.11B. Borel Determinacy in Z_2 .

0.11C. Borel Diagonalization.

0.11D. Borel Inclusion for $\mathfrak{R}^\infty \rightarrow \mathfrak{R}$, $\mathfrak{R}^\infty \rightarrow \mathfrak{R}^\infty$, $\text{GRP} \rightarrow \text{GRP}$.

0.11E. Borel Subalgebra Theorems.

0.11F. Borel Squaring Theorem and Function Agreement.

0.11A. Preliminaries.

The system Z_2 of "(full) second order arithmetic", and the closely related $\text{ZFC}\setminus\text{P}$, $\text{ZF}\setminus\text{P}$, have been discussed in section 0.4.

It will be useful to have a system stronger than Z_2 , which suffices to prove the various statements presented in this section, that are not provable in Z_2 .

For this purpose, it is convenient to use a weak fragment of $Z_3 = \text{"(full) third order arithmetic"}$. Here Z_3 has three sorts: N , PN , PPN . We use $0, S, +, \cdot, \in$, where $0, S, +, \cdot$ live in N , and \in connects N to PN , and PN to PPN . We will have equality only for sort N .

Recall the axioms of Z_2 :

1. $Sx \neq 0$, $Sx = Sy \rightarrow x = y$, $x+0 = x$, $x+Sy = S(x+y)$, $x \cdot 0 = 0$, $x \cdot Sy = (x \cdot y)+x$.
2. $0 \in A \wedge (\forall x)(x \in A \rightarrow Sx \in A) \rightarrow x \in A$.
3. $(\exists A)(\forall x)(x \in A \leftrightarrow \varphi)$, where φ is any formula in $L(Z_2)$ in which A is not free.

The axioms of Z_3 are very similar. The terms of sort N are the same as for Z_2 . The atomic formulas are the equations between terms of sort N , and $t \in x$, $x \in A$, where x is a variable of sort PN and A is a variable of sort PPN . Formulas are built up as usual using the connectives and sorted quantifiers.

1. $Sx \neq 0$, $Sx = Sy \rightarrow x = y$, $x+0 = x$, $x+Sy = S(x+y)$, $x \cdot 0 = 0$, $x \cdot Sy = (x \cdot y)+x$.
2. $0 \in A \wedge (\forall x)(x \in A \rightarrow Sx \in A) \rightarrow x \in A$.
3. $(\exists A)(\forall x)(x \in A \leftrightarrow \varphi)$, where φ is any formula in $L(Z_3)$ in which A is not free.
4. $(\exists \alpha)(\forall A)(A \in \alpha \leftrightarrow \varphi)$, where φ is any formula in $L(Z_3)$ in which α is not free.

The axioms of WZ_3 are very convenient (W for "weak"). The only change is that in axiom 4, we require that there be no quantifiers over PPN. WZ_3 is enough to extend the projective hierarchy along ω_1 . Z_3 proves the existence of a beta model of WZ_3 , and much more.

In this section 0.11, we will focus entirely on the outer limits of Concrete Mathematical Incompleteness, in that we will be using

Borel measurable sets in and functions between
complete separable metric spaces

throughout. We take finitely Borel to lie within Concrete mathematics, and arbitrary Borel to lie just outside.

In each case in this section, the incompleteness from Z_2 will emerge already using only Borel objects of finite rank in the Borel hierarchy (i.e., finitely Borel). In section 0.12, when we use Zermelo set theory, the incompleteness will emerge at Borel rank ω .

Our position that the finite levels of the Borel hierarchy for complete separable metric spaces lies at the outer limit of the Mathematically Concrete was discussed in section 0.3, with Theorem 0.3.1 used as some justification - particularly item ii there.

Let X be a complete separable metric space. We define the classes Σ_α and Π_α of subsets of X , $\alpha < \omega_1$, as follows.

Σ_0 consists of the sets of the form $\{y: d(x,y) < q\}$, for $x \in X$ and positive rationals q . Π_0 consists of the sets of the form $\{y: d(x,y) \geq q\}$, for $x \in X$ and positive rationals q .

For $0 < \alpha < \omega_1$, Σ_α consists of unions of sequences of sets from the Π_β , $\beta < \alpha$, and Π_α consists of intersections of sequences of sets from the Σ_β , $\beta < \alpha$.

The Borel subsets of X are the sets that are in Σ_α , for some $\alpha < \omega_1$. It is easily seen that the Borel sets form the least σ algebra of subsets of X containing all elements of Σ_0 .

It is also clear that each Π_α is the set of complements of the elements of Σ_α . Also, for $0 \leq \alpha \leq \beta < \omega_1$, $\Sigma_\alpha \subseteq \Sigma_\beta$ and $\Pi_\alpha \subseteq \Pi_\beta$.

If X is uncountable, then for all $\beta < \omega_1$, $\Sigma_\beta \neq \Sigma_{\beta+1}$, and $\Pi_\beta \neq \Pi_{\beta+1}$.

This is equivalent to the definition of the Borel hierarchy given in [Ke95], 11.B, p. 68, where these claims are proved.

We focus on the functions $f: X \rightarrow Y$, where X, Y are complete separable metric spaces. We say that f is Borel (Borel measurable) if and only if the inverse image of every open subset of Y is a Borel subset of X .

We also define the following important hierarchy of functions.

Baire class 0 consists of the $f: X \rightarrow Y$ which are pointwise limits of continuous $f: X \rightarrow Y$.

For $0 < \alpha < \omega_1$, Baire class α consists of the $f: X \rightarrow Y$ that are the pointwise limit of a sequence of $g: X \rightarrow Y$ that pointwise converges, where for each g there exists $\beta < \alpha$ such that g is in Baire class β .

We say that $f: X \rightarrow Y$ is Baire if and only if f is in Baire class α , for some $\alpha < \omega_1$.

It is a standard theorem of descriptive set theory that the Baire functions are exactly the Borel functions (in the context of $f: X \rightarrow Y$, where X, Y are complete separable metric spaces). See [Ke95], Theorem 24.3, p. 190,

Some authors define the Baire classes a little differently, where they start at Baire class 1, and define $f: X \rightarrow Y$ to be of Baire class 1 if and only if the inverse image of every open subset of Y is a Σ_2 subset of X .

According to [Ke95], Theorem 24.10, this definition agrees with our definition above (pointwise limits of continuous functions) in the case $Y = \mathfrak{R}$.

We must formalize these notions appropriately in $L(\text{RCA}_0)$. Some care is required. We adopt the approach of [Si99, 09].

Firstly, complete separable metric spaces are defined in $L(\text{RCA}_0)$ by means of codes. We henceforth refer to these spaces as Polish spaces.

As in [Si99,09], Definition II.5.1, a code for a Polish space T is a nonempty set $A \subseteq \mathbb{N}$ together with a function $d:A^2 \rightarrow \mathfrak{R}$ obeying the usual metric conditions. Points in T are then defined as infinite sequences from A that form a Cauchy sequence (using the estimates 2^{-i}). We don't factor out by the obvious equivalence relation. Similarly, when developing \mathfrak{R} as Cauchy sequences, we also don't factor out.

The metric d extends naturally to T , A becomes dense in T , and Cauchy completeness holds for the elements of T .

Open subsets of X are coded by sequences of pairs (a,q) , where $a \in A$ and $q > 0$ is rational. Membership of $x \in T$ in the open set means that $d(a,x) < q$. Closed subsets of X are viewed as complements of open sets.

Continuous functions from X into Y are coded in $L(RCA_0)$ by means of systems of neighborhood conditions. In [Si99,09], Definition II.6.1, they are sets of quintuples from $\mathbb{N} \times A \times \mathbb{Q}^+ \times B \times \mathbb{Q}^+$, where $A,B \subseteq \mathbb{N}$ are attached to the Polish spaces X,Y .

For Borel subsets of X , the usual vehicle for formalization in the language of RCA_0 is through Borel codes. These are well founded trees of finite sequences from \mathbb{N} where at the terminal vertices, there is a label (a,q) , where $a \in A$ and $q > 0$ is rational. The idea is that $x \in X$ is accepted at a terminal vertex with label (a,q) if and only if $d(a,x) < q$, and accepted at an internal vertex v if and only if

case 1. v is of odd length (as a finite sequence from \mathbb{N}). x is accepted at some immediate successor of v .

case 2. v is of even length. x is not accepted at any immediate successor of v .

Finally, x is considered to be in the Borel set with the given Borel code, if and only if x is accepted at the root of the tree.

A similar Borel coding scheme can be introduced for Borel functions $f:X \rightarrow Y$ that corresponds to the Baire classes.

This whole coding apparatus is very delicate for weak systems, particularly for RCA_0 , since in order to get accepted, a certain transfinite recursion must be realized. In weak systems, we can only provably realize very special transfinite recursions. To a much lesser extent, issues

arise in weak systems with regard to the codings of open and closed sets, and continuous functions.

We have no need to confront these issues in this section 0.11. The statements being reversed here derive ATR_0 over RCA_0 , using very little of this coding. We are then free to use ATR_0 as a base theory when dealing with Borel sets in and functions between Polish spaces.

0.11B. Borel Determinacy in Z_2 .

Determinacy concerns (two person zero sum) infinite games, where players I, II alternately play nonnegative integers, starting with player I. The outcome of the game is the element of \mathbb{N}^ω that results from the play of the game.

Specifically, for any $A \subseteq \mathbb{N}^\mathbb{N}$, we consider the game $G[A]$, where player I is considered the winner if the outcome of the game is an element of A . Otherwise, player II is considered to be the winner.

We say that $G[A]$ is determined if and only if one of the two players has a winning strategy. It is well known that there exists $A \subseteq \mathbb{N}^\mathbb{N}$ for which $G[A]$ has no winning strategy. See [GS53], [Ka94], chapter 6.

However, the proof of the existence of non determined $G[A]$ does not produce an A that is definable in set theory. There has been much work concerning the determinacy of $G[A]$, where A is explicitly definable in various senses. These investigations are tied up with large cardinal hypotheses. We refer the reader to [Mart69], [MSt89], [Ke95], [Lar04], [St09], [Ne ∞], [KW ∞].

Let K be a class of subsets of $\mathbb{N}^\mathbb{N}$. K determinacy asserts that for all $A \in K$, the game $G[A]$ is determined. Henceforth, we will be focused on K contained in the class of all Borel subsets of $\mathbb{N}^\mathbb{N}$.

The original "proof" of Borel determinacy was not conducted in ZFC.

THEOREM 0.11B.1. Assume that a measurable cardinal exists. Then Borel determinacy holds. I.e., all Borel subsets of $\mathbb{N}^\mathbb{N}$ are determined. In fact, the weaker large cardinal hypothesis $(\forall \alpha < \omega_1) (\exists \kappa) (\kappa \rightarrow \alpha)$ suffices.

Proof: See [Mart69], [Ke95], section 20. QED

Later, we showed that any proof of Borel determinacy in ZFC is not going to be "normal".

THEOREM 0.11B.2. There is no proof of Borel determinacy in Zermelo set theory with the axiom of choice (ZC). In fact, no countable transfinite iteration of the power set operation suffices.

Proof: See [Fr71]. We will discuss what exactly we mean by the second claim, in section 0.12. QED

A few years later, the gap between Theorems 0.11B.1 and 0.11B.2 was filled.

THEOREM 0.11B.3. Borel determinacy can be proved in ZFC. In fact, it suffices to use all countably transfinite iterations of the power set operation.

Proof: See [Mart75], [Ke95]. QED

Note that Theorems 0.11B.2 and 0.11B.3 properly lie in the domain of section 0.12.

There has been considerable work on determining just where in the Borel hierarchy determinacy is provable in full second order arithmetic, Z_2 . This investigation has culminated in [MS ∞], providing a complete answer.

Note that determinacy for the classes Borel, Σ_n^0 , Π_n^0 , and Δ_n^0 , are Π_3^1 statements. So we can use $ZFC \setminus P$ or $ZF \setminus P$, as all three of these systems prove the same Π_3^1 sentences. In fact, they prove the same Σ_4^1 sentences, as is shown in [MS ∞], Proposition 1.4 (although this is certainly not due to them, but it is not clear who first proved this). Here $\setminus P$ indicates "without the power set axiom".

Here is the historical record of Borel determinacy in Z_2 .

Borel determinacy. Not provable in Zermelo set theory with the axiom of choice. Not provable using only countably many transfinite iterations of the power set operation, [Fr71]. See section 0.12 for precise formulations.

Σ_5^0 determinacy. Not provable in Z_2 . [Fr71].

Borel determinacy. Proved in $ZFC \setminus P$ + "the cumulatively hierarchy on any well ordering of ω exists". [Mart75].

Σ^0_4 determinacy. Not provable in Z_2 . [Mart74].

Σ^0_1 determinacy. Equivalent to ATR over RCA. [St76]. Refined in [Si99,09] to equivalence with ATR_0 over RCA_0 .

$\Sigma^0_1 \wedge \Pi^0_1$ determinacy. Equivalent to $\Pi^1_1\text{-CA}_0$ over RCA_0 . [Tan90].

Δ^0_2 determinacy. Equivalent to $\Pi^1_1\text{-TR}_0$ over RCA_0 . [Tan90].

Σ^0_2 determinacy. Provable in $\Pi^1_2\text{-CA}_0$, but not in $\Pi^1_1\text{-TR}_0$. [Tan91].

Δ^0_3 determinacy. Provable in $\Delta^1_3\text{-CA}$, but not in $\Delta^1_3\text{-CA}_0$. [MT08].

Σ^0_3 determinacy. Provable in $\Pi^1_3\text{-CA}_0$. [Wel09].

Boolean combinations of Σ^0_3 determinacy. Not provable in Z_2 . For n -fold combinations, fixed $n < \omega$, provable in Z_2 , [MS ∞].

0.11C. Borel diagonalization on \mathfrak{R} .

We discovered Borel diagonalization on \mathfrak{R} by reflecting on Cantor's proof that \mathfrak{R} is uncountable. Put in very basic terms, Cantor proved by diagonalization that

*) in any infinite sequence of real numbers,
some real number is missing.

It occurred to me to consider witness functions for *). Let us say that $F:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$ is a diagonalizer if and only if $(\forall x \in \mathfrak{R}^\infty) (\forall n \in \mathbb{Z}^+) (F(x) \neq x_n)$.

For any topological space X , X^∞ is the infinite product space defined in the usual way. It is well known that if X is (can be made into) a complete separable metric space, then X^∞ is (can be made into) a complete separable metric space.

Cantor's diagonalization argument easily establishes the existence of a diagonalizer $F:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$.

LEMMA 0.11C.1. There is no continuous diagonalizer $F:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$. There is no continuous diagonalizer $F:I^\infty \rightarrow I$.

Proof: Let $F: \mathfrak{R}^\infty \rightarrow \mathfrak{R}$ be a continuous diagonalizer. Let $\alpha \in \mathfrak{R}^\infty$ be an enumeration of the rationals. Consider $F(x, \alpha)$ as a function of $x \in \mathfrak{R}$.

case 1. F is constant. Let c be the constant. Then $F(c, \alpha) = c$, which is impossible.

case 2. F is not constant. Let $F(x, \alpha) \neq F(y, \alpha)$, $x < y$. By the intermediate value theorem there exists $x < z < y$ such that $F(z, \alpha) \in \mathbb{Q}$. This is also impossible.

We can easily repeat the argument with \mathfrak{R} replaced by I . QED

We now construct a diagonalizer $F: I^\infty \rightarrow I$ in Baire class 1.

Let $x \in I^\infty$. First write the coordinates of x in base 2, always using infinitely many 0's. Then diagonalize in the usual way to construct $u \in \{0, 1\}^\infty$ which differs from these base 2 expansions. I.e., $u_i = 1 - x_i'$, where x_i' is this expansion of x_i in base 2. Take $F(x)$ to be the evaluation of u in I .

For $w \in \{0, 1\}^k$, $k \geq 1$, write $w^* \in I$ for the evaluation of w in base 2.

LEMMA 0.11C.2. Let $w \in \{0, 1\}^k$, $k \geq 1$. $A = \{x \in I^\infty: F(x) \in [w^*, w^* + 2^{-k}]\}$ is Δ_2^0 in I^∞ .

Proof: Let w be given. Let $x \in I^\infty$. Note that $x \in A$ if and only if

$F(x)$ has base 2 expansion starting with w .

$(\exists v_1, \dots, v_k \in \{0, 1\}^k) (\forall i \in \{1, \dots, k\}) (v_i \text{ is the first } k \text{ terms of the base 2 expansion of } x_i, \text{ and the standard diagonal construction produces } w \text{ from } v_1, \dots, v_k).$

$(\exists v_1, \dots, v_k \in \{0, 1\}^k) (\forall i \in \{1, \dots, k\}) (x_i \in [v_i, v_i + 2^{-k}]) \text{ and the standard diagonal construction produces } w \text{ from } v_1, \dots, v_k).$

QED

LEMMA 0.11C.3. Let $V \subseteq I$ be open. Then $F^{-1}(V)$ is Σ_2^0 in I^∞ .

Proof: Since every open subset of I is the countable union of intervals of the form $[w^*, w^* + 2^{-k})$, $w \in \{0, 1\}^k$, $k \geq 1$, this is immediate from Lemma 0.11C.2. QED

LEMMA 0.11C.4. Let $F:I^\infty \rightarrow I$, and suppose that the inverse image of any open set in I under F is Σ_2^0 in I^∞ . Then F is in Baire class 1.

Proof: By Theorem 24.3 in [Ke95], p. 190, credited to Lebesgue, Hausdorff, and Banach. QED

THEOREM 0.11C.5. There is a diagonalizer $F:I^\infty \rightarrow I$ in Baire class 1, but none that is continuous. There is a diagonalizer $G:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$ in Baire class 1, but none that is continuous. There is a continuous diagonalizer $H:X^\infty \rightarrow X$, where X is $\{0,1\}$ or $X = \mathbb{N}$.

Proof: The first claim is immediate from Lemmas 0.11C.1, 0.11C.3, and 0.11C.4. For the second claim, take $G(x) = f(x')$, where each $x'_i = 0$ if $x_i \leq 0$; 1 if $x_i \geq 1$; x otherwise. Note that $G:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$ is a diagonalizer, and x' defines a continuous function of x . Hence G is in Baire class 1. The last claim is essentially due to Cantor, with his diagonal argument. QED

We realized that in the constructions of diagonalizers $F:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$, the values $F(x_1, x_2, \dots)$ seem to depend critically on the order in which the x 's appear.

So we were led to the question: is there a diagonalizer $F:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$ which is suitably invariant? I.e., where for all $x, y \in \mathfrak{R}^\infty$, if x is "similar" to y , then $F(x) = F(y)$?

The weakest notion of "similar" that we consider in this section is "having the same coordinates" or "having the same image". I.e., $\text{rng}(x) = \text{rng}(y)$, for $x, y \in \mathfrak{R}^\infty$. Here $\text{rng}(x)$ is the set of all coordinates of x .

Thus we say that $f:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$ is image invariant if and only if for all $x, y \in \mathfrak{R}^\infty$, $\text{rng}(x) = \text{rng}(y) \rightarrow F(x) = F(y)$.

Of course, this definition applies to $f:X^\infty \rightarrow X$, where X is any set whatsoever.

THEOREM 0.11C.6. There is an image invariant diagonalizer $f:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$. In fact, there is an image invariant diagonalizer $f:X^\infty \rightarrow X$ if and only if X is uncountable.

Proof: By the axiom of choice. QED

Note that the proof of Theorem 0.11C.6 does not produce a definable example - even for the first claim. A related observation is that it proves the claim in ZFC, but not even the first claim is proved in ZF.

We will take this matter up in section 0.13, where we show that there is no definition that ZFC proves is an example for the first claim, and that ZF does not suffice to prove the existence of an example for the first claim.

We now come to a Concrete Mathematical Incompleteness result.

THEOREM 0.11C.7. Borel Diagonalization Theorem. There is no image invariant Borel diagonalizer $f:\mathfrak{N}^\infty \rightarrow \mathfrak{N}$. This is provable in WZ_3 but not in Z_2 .

Proof: See [Fr81]. The unprovability from Z_2 was proved there by first considering pZ_2 , which is Z_2 formulated without parameters. We established the equiconsistency of pZ_2 and Z_2 , and other relationships, and then showed how the Borel Diagonalization Theorem gives rise to an ω model of pZ_2 , and hence of Z_2 . We relied on our earlier experience with ZF formulated without parameters, from our Ph.D. thesis. See [Fr67] and [Fr71a]. QED

0.11D. Borel Inclusion for $\mathfrak{N}^\infty \rightarrow \mathfrak{N}$, $\mathfrak{N}^\infty \rightarrow \mathfrak{N}^\infty$, $GRP \rightarrow GRP$.

We now consider these three notions of similarity.

1. y is a permutation of x .
2. y is a permutation of x that moves only finitely many positions. Such permutations are called finitary permutations.
3. x, y have the same image.

The associated conditions on $F:\mathfrak{N}^\infty \rightarrow \mathfrak{N}$ are respectively called permutation invariant, finitary permutation invariant, and image invariant.

We also consider shift invariance. We say that $F:\mathfrak{N}^\infty \rightarrow \mathfrak{N}$ is shift invariant if and only if for all $x \in \mathfrak{N}^\infty$, $F(sx) = F(x)$. Here $sx = \text{shift of } x$, is the result of removing the first term of x .

We also find it convenient to switch to positive phraseology. We define an inclusion point of $F:\mathfrak{N}^\infty \rightarrow \mathfrak{N}$ as an $x \in \mathfrak{N}^\infty$ such that $F(x)$ is a coordinate of x .

THEOREM 0.11D.1. Borel Inclusion Point Theorem for $\mathfrak{N}^\infty, \mathfrak{N}$. Every permutation (finitary permutation, image, shift) invariant Borel $F: \mathfrak{N}^\infty \rightarrow \mathfrak{N}$ has an inclusion point. All four forms are provable in WZ_3 , but none are provable in Z_2 .

Proof: These results are proved by straightforward adaptations of the methods in [Fr81]. QED

We now consider $F: \mathfrak{N}^\infty \rightarrow \mathfrak{N}^\infty$. Here we say that x is an inclusion point for F if and only if $F(x)$ is a subsequence of x .

There are many natural notions of invariance here.

- a. Permutation commuting. This means that for all $x \in \mathfrak{N}^\infty$ and permutations π , $f(\pi x) = \pi f(x)$.
- b. Finitary permutation commuting. This means that for all $x \in \mathfrak{N}^\infty$ and finite permutations π , $f(\pi x) = \pi f(x)$.
- c. Permutation invariant. This means that for all $x, y \in \mathfrak{N}^\infty$, if y is a permutation of x then $F(x) = F(y)$.
- d. Finitary permutation invariant. This means that for all $x, y \in \mathfrak{N}^\infty$, if y is a finite permutation of x then $F(x) = F(y)$.
- e. Permutation preserving. This means that for all $x, y \in \mathfrak{N}^\infty$, if y is a permutation of x then $F(y)$ is a permutation of $F(x)$.
- f. Finitary permutation preserving. This means that for all $x, y \in \mathfrak{N}^\infty$, if y is a finitary permutation of x then $F(y)$ is a finitary permutation of $F(x)$.
- g. Image invariant. This means that for all $x, y \in \mathfrak{N}^\infty$, $\text{rng}(x) = \text{rng}(y) \rightarrow F(x) = F(y)$.
- h. Image preserving. This means that for all $x, y \in \mathfrak{N}^\infty$, $\text{rng}(x) = \text{rng}(y) \rightarrow \text{rng}(F(x)) = \text{rng}(F(y))$.
- i. Shift invariant. This means that for all $x \in \mathfrak{N}^\infty$, $F(sx) = F(x)$.
- j. Shift commuting. This means that for all $x \in \mathfrak{N}^\infty$, $F(sx) = s(F(x))$.

k. Tail invariant. This means that for all $x, y \in \mathfrak{N}^\infty$, if x, y have a common tail, then $F(x) = F(y)$.

l. Tail preserving. This means that for all $x, y \in \mathfrak{N}^\infty$, if x, y have a common tail, then $F(x), F(y)$ have a common tail.

THEOREM 0.11D.2. Borel Inclusion Theorem for $\mathfrak{N}^\infty, \mathfrak{N}^\infty$. Every Borel $F: \mathfrak{N}^\infty \rightarrow \mathfrak{N}^\infty$ with any of a-1 has an inclusion point. All twelve forms are provable in WZ_3 , but none are provable in Z_2 .

Proof: These results are proved by straightforward adaptations of the methods in [Fr81]. QED

Let GRP be the space of groups whose domain is N or a finite subset of N . Then GRP is a low level Borel subspace of a natural Baire space.

Let $F: \text{GRP} \rightarrow \text{GRP}$. An inclusion point for F is some $G \in \text{GRP}$ such that $F(G)$ is embeddable into G .

We say that $F: \text{GRP} \rightarrow \text{GRP}$ is isomorphic preserving if and only if for all $G, H \in \text{GRP}$, $G \approx H \rightarrow F(G) \approx F(H)$.

We write FGG for the subspace of finitely generated elements of GRP.

LEMMA 0.11D.3. Any two elements of FGG that agree on their intersection have a common extension in FGG.

Proof: This is by the free product construction. QED

Let FGG be the subspace consisting of the finitely generated $G \in \text{GRP}$.

THEOREM 0.11D.4. Every isomorphic preserving Borel function $F: \text{GRP} \rightarrow \text{GRP}$ has an inclusion point. This is provable in WZ_3 but not in Z_2 . In fact, Z_2 does not even prove this for $F: \text{GRP} \rightarrow \text{FGG}$. The same results hold for finitely Borel functions.

Proof: Let F be as given with Borel code u . Let M be a countable transitive model of a weak fragment of $ZFC + V = L$ containing u . Then F will remain isomorphic preserving in M . Build a generic tower of finitely generated groups of length ω , using finite length towers of finitely generated groups as the forcing conditions (this will collapse ω_1 to ω). Let G be the union of the tower. Then $F(G)$ is

embeddable into G using Lemma 0.11D.3, and that the FGG of the generic extension is the same as the FGG of the ground model. The proof can be adapted to be formalized in WZ_3 . For the final claim, let $G \in \text{GRP}$. Look at the union V of all Turing degrees associated with the finitely generated subgroups of G , and get a Turing degree that's missing, assuming that V is not a model of parameterless Z_2 . Then output the $H \in \text{FGG}$ associated with this Turing degree, as in [Fr07a]. The reduction of Z_2 to parameterless Z_2 is presented and used in [Fr81]. QED

THEOREM 0.11D.5. Let X be a Borel set of relational structures in a finite relational type with domain N or a finite subset of N . Suppose any two finitely generated substructures of any two respective elements of X that agree on their intersection have a common extension in X . Then every isomorphic preserving Borel function $F:X \rightarrow X$ has an inclusion point.

Proof: We have just isolated the essential feature needed to carry out the proof of Theorem 0.11D.4, which is Lemma 0.11D.3. QED

THEOREM 0.11D.6. Theorem 0.11D.5 is provable in WZ_3 but not in Z_2 . The same holds for finitely Borel sets and functions.

Proof: By Theorem 0.11D.4 and the proof of Theorem 0.11D.5. QED

0.11E. Borel Squaring Theorem and Function Agreement.

We seek a one dimensional form of the results on \mathfrak{N}^∞ . Let K be the Cantor space $\{0,1\}^\infty$, indexed from 1. For $x \in K$, the "square" of x , written $x^{(2)}$, is given by

$$x^{(2)} = (x_1, x_4, x_9, x_{16}, \dots).$$

THEOREM 0.11E.1. Borel Squaring Theorem. Every shift invariant Borel $F:K \rightarrow K$ maps some argument into its "square". I.e., there exists $x \in K$ such that $F(x) = x^{(2)}$. This is provable in WZ_3 but not in Z_2 . The same results hold for finitely Borel F .

Proof: See [Fr83]. QED

In [Fr83], we went on to try to prove such a one dimensional theorem for the circle group S , where $2x$ on S

replaces $s(x)$ on K . Thus we say that $F:S \rightarrow S$ is doubling invariant if and only if for all $x \in S$, $F(2x) = F(x)$.

But we were not able to find a nice function on S like "squaring" on K . However, we were able to find a continuous function on S that works.

THEOREM 0.11E.2. There is a continuous $F:S \rightarrow S$ which agrees somewhere with every doubling invariant Borel $G:S \rightarrow S$. This is provable in WZ_3 but not in Z_2 . The same results holds for finite Borel G .

Proof: See [Fr83]. QED

This opens up two closely related research topics:

Find a simple function that agrees somewhere with every function satisfying a given condition.

Find a function obeying a first given condition that agrees somewhere with every function satisfying a second given condition.

The results of section 0.11D can be put into the same form illustrated by Theorems 0.11E.1 and 0.11E.2, as follows.

THEOREM 0.11E.3. The first coordinate function from \mathfrak{R}^∞ into \mathfrak{R} agrees somewhere with every invariant Borel $F:\mathfrak{R}^\infty \rightarrow \mathfrak{R}$, in the various senses discussed in section 0.11D.

Proof: By [Fr81], [Fr83], and sometimes straightforward adaptation of the methods there. QED.

0.12. Incompleteness in Russell Type Theory and Zermelo Set Theory.

0.12A. Preliminaries.

0.12B. Borel Determinacy and Symmetric Borel Sets.

0.12C. Borel Selection.

0.12D. Borel Inclusion with Equivalence Relations.

0.12E. Borel Functions on Linear Orderings and Graphs.

0.12F. Borel Functions on Borel Quasi Orders.

0.12G. Countable Borel Equivalence Relations and Quasi Orders.

0.12H. Borel Sets and Functions in Groups.

0.12A. Preliminaries.

By Russell's Type Theory, we will mean his impredicative theory (obtained from his predicative theory using his axiom of reducibility), with the ground type corresponding to N . This modern form, which we call RTT, uses infinitely many sorts N, PN, PPN, \dots , with $0, S, +, \cdot$ operating at type N , and \in connecting each sort with the next. We use equality only at sort N . The axioms are as follows.

1. $Sx \neq 0, Sx = Sy \rightarrow x = y, x+0 = 0, x+Sy = S(x+y), x \cdot 0 = 0, x \cdot Sy = x \cdot y + x$, where x, y have type N .
2. $0 \in A \wedge (\forall x)(x \in A \rightarrow Sx \in A) \rightarrow x \in A$, where x has type N and A has type PN .
3. $(\exists A)(\forall B)(B \in A \leftrightarrow \varphi)$, where φ is a formula of $L(RTT)$, and A has type one higher than B .

The fragment involving only variables of the first n types, including N , is called Z_n , or n -th order arithmetic.

It proved quite awkward to formalize mathematics in RTT, even in its modern form. So it was supplanted by the single sorted system Z (Zermelo set theory), and later with Fraenkel's addition of Replacement, forming ZF. Still later, the axiom of choice became fully accepted, forming ZFC.

Z is a one sorted system with one binary relation symbol \in , in first order predicate calculus with equality. The axioms of Z are as follows.

- EXTENSIONALITY. $(\forall x)(x \in y \leftrightarrow x \in z) \rightarrow y = z$.
 PAIRING. $(\exists x)(y \in x \wedge z \in x)$.
 UNION. $(\exists x)(\forall y)(\forall z)(y \in z \wedge z \in w \rightarrow y \in x)$.
 SEPARATION. $(\exists x)(\forall y)(y \in x \leftrightarrow y \in z \wedge \varphi)$, where x is not free in φ .
 POWER SET. $(\exists x)(\forall y)((\forall z)(z \in y \rightarrow z \in w) \rightarrow y \in x)$.
 INFINITY. $(\exists x)(\emptyset \in x \wedge (\forall y, z)(y \in x \wedge z \in x \rightarrow y \cup \{z\} \in x))$.

This modern version of Z differs from what Zermelo wrote in [Ze08]. There he included the Axiom of Choice, and also used this form of Infinity:

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow \{y\} \in x)).$$

In the case of ZF, this, and other reasonable formulations of Infinity such as the most common

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow y \cup \{y\} \in x))$$

are provably equivalent from the remaining axioms. This is not the case for Z - see [Math01], Concluding Remarks. However, it is known that the variants of Z determined by reasonable formulations of Infinity are mutually interpretable.

Note that this version of Z can prove $(\forall n < \omega) (V(\omega+n) \text{ exists})$, but cannot prove the existence of $V(\omega+\omega)$. The former is enough to prove the consistency of RTT (see below).

We write ZC for Z together with the axiom of choice:

CHOICE. If x is a set of pairwise disjoint nonempty sets, there is a set which has exactly one element in common with each of the elements of x .

It is natural to weaken Separation in Z , where only Δ_0 formulas are allowed. We refer to this as WZ , where W indicates "weak". This is also sometimes called MacLane set theory. We also consider $WZC = WZ + AxC$.

We also use $WZ(\Omega)$, which is $WZ +$ "every well ordering of ω is isomorphic to an ordinal" + "for all countable ordinals α , $V(\alpha)$ exists".

The notions of ω model and β model are used for theories whose language extends that of Z_2 , or the language of set theory. An ω model is a model where the internal natural numbers are standard. A β model is an ω model where if an internal binary relation on the internal natural numbers is, internally, a well ordering, then it is a well ordering.

THEOREM 0.12A.1. Z proves the existence of a countable β model of RTT and WZC . WZ is a conservative extension of RTT, in the sense that any theorem of WZ that is suitably typed, is also a theorem of RTT.

Proof: For the first claim, Z can develop truth for bounded formulas, construct the proper class of constructible elements of the proper class $V(\omega+\omega)$, and pass to the internally definable elements. This forms the required β model. The conservative extension result is most easily proved model theoretically, expanding any model of RTT to a model of WZ . QED

In this section, we prove a number of equivalences over ATR_0 . Four main principles arise in this connection.

We make the following definition in ATR_0 . Let (A, R) be a well ordering, $A \subseteq \mathbb{N}$. A countable R model is a triple (B, S, rk) , where

- i. $B \subseteq \mathbb{N}$, $S \subseteq B^2$, and $rk: B \rightarrow A$ is surjective.
- ii. $rk(x) \leq u \leftrightarrow (\forall y) (S(y, x) \rightarrow rk(y) < u)$.
- iii. If $E \subseteq B$ is definable in (B, S) and $u \in A$, then there is a unique $x \in B$ whose S predecessors are exactly the elements of E of rank $< u$.

Assume (A, R) has length $> \omega$, and let (B, S, rk) be a countable R model. There is an obvious mapping from every $n \in \omega$ to a point n^* in (B, S, rk) with $rk(n^*) = n$. We say that (B, S, rk) encodes $x \subseteq \omega$ if and only if there exists $u \in B$ such that $x = \{n: S(n^*, u)\}$.

FRA (finite rank axiom). For each $n < \omega$ and $x \subseteq \omega$, there is a countable $\omega+n$ model that encodes x .

BFRA (beta finite rank axiom). For each $n < \omega$ and $x \subseteq \omega$, there is a countable $\omega+n$ model that encodes x , which is a β model.

CRA (countable rank axiom). For each well ordering (A, R) , $A \subseteq \mathbb{N}$, with a limit point, and $x \subseteq \omega$, there is a countable R model that encodes x .

BCRA (beta countable rank axiom). For each well ordering (A, R) , $A \subseteq \mathbb{N}$, with a limit point, and $x \subseteq \omega$, there is a countable R model that encodes x , which is a β model.

THEOREM 0.12A.2. BFRA is provable in Z . FRA is not provable in WZC . BCRA is provable in $WZ(\Omega)$. CRA is not provable in ZC . The following is provable in ATR_0 . FRA is equivalent to $(\forall n) (\forall x \subseteq \omega) (Z_n \text{ has an } \omega \text{ model encoding } x)$. BFRA is equivalent to $(\forall n) (\forall x \subseteq \omega) (Z_n \text{ has a } \beta \text{ model encoding } x)$. If CRA then ZC has a countable ω model encoding any given $x \subseteq \omega$. If BCRA then ZC has a countable β model encoding any given $x \subseteq \omega$.

Proof: For the first claim, fix $n < \omega$ and $x \subseteq \omega$. Use a countable elementary substructure of the $V(\omega+n)$ of the constructible universe relative to x .

For the second claim, suppose that FRA is provable in WZC. By a model theoretic argument, FRA is provable in the fragment of WZC obtained by replacing the power set axiom with the existence of $V(\omega+n)$, for some fixed n . However, the consistency of that fragment is provable in FRA, violating Gödel's second incompleteness theorem.

For the third claim, let (A,R) and x be given, and use a countable elementary substructure of the $V(\alpha)$ of the constructible universe relative to x , where (A,R) has type α .

For the fourth claim, suppose CRA is provable in ZC. Apply CRA to a specific well ordering of type $\omega+\omega$. Then CRA proves the consistency of ZC, which contradicts second incompleteness.

For the fifth claim, countable ω models of Z_n encoding x correspond to countable $\omega+n$ models encoding x .

For the sixth claim, countable β models of Z_n encoding x correspond to countable $\omega+n$ models encoding x that are β models.

For the seventh and eighth claims, use (A,R) of type $\omega+\omega$. QED

Let φ be a sentence in the language of set theory. We want to define what we mean by " φ cannot be proved using a definite countable iteration of the power set operation". This issue was addressed in [Fr81], [Fr05], [Fr07a].

We define the system DCIPS (definite countable iterations of the power set) as follows. The language has only \in in logic with equality. The axioms of DCIPS are given as follows.

- i. Every axiom of $ZFC \setminus P$ is an axiom of DCIPS.
- ii. Suppose $\varphi(x)$ is a Σ_1 formula of set theory with only the free variable shown, where $ZFC \setminus P$ proves $(\exists x)(\varphi(x) \wedge x \text{ is an ordinal})$. Then $(\exists x)(\varphi(x) \wedge V(x) \text{ exists})$ is an axiom of DCIPS.

We say that a sentence can be proved using a definite countable iteration of the power set operation if and only if it can be proved in DCIPS.

THEOREM 0.12A.3. $ATR_0 + CRA$ proves the existence of an ω model of DCIPS. CRA is not provable in DCIPS.

Proof: It is clear that the second claim follows from the first. We work in $ATR_0 + CRA$.

By applying CRA to, say, $\omega + \omega$, we obtain a countable β model M of $ZFC + V = L$. Let S be the set of all sentences $(\exists x)(\varphi(x) \wedge x \text{ is an ordinal})$, with only the free variable x , where φ is Σ_1 , that are provable in $ZFC \setminus P$. Clearly all sentences in S hold in M .

Let λ be the height of M . Apply CRA to a well ordering of type $\lambda + \omega$, obtaining a suitable (B, R) , B of type $\lambda + \omega$. Within (B, R) , cut back to the inner model of constructible sets in the sense of (B, R) . Thus M will correspond to the first λ levels of (B, R) . Then for each sentence $(\exists x)(\varphi(x) \wedge x \text{ is an ordinal})$ in S , the corresponding sentence $(\exists x)(\varphi(x) \wedge V(x) \text{ exists})$ holds in (B, R) , since the x can be taken to be an ordinal $< \lambda$.

(B, R) is not quite an ω model of DCIPS. We have only to extend (B, R) using the constructible hierarchy internally defined in (B, R) . QED

So in particular, if a sentence in $L(Z_2)$ implies CRA over ATR_0 , then that sentence "cannot be proved using a definite countable iteration of the power set operation".

0.12B. Borel Determinacy and Symmetric Borel Sets.

In [Fr71], we proved that Borel Determinacy is not provable in Z (or ZC). As was well known at the time, this can be strengthened to any "definite" countably transfinite iteration of the power set axiom. In [Fr71], we focused on the critical case of Z .

We also formulated the conjecture that Borel Determinacy could be proved in (a weak variant of) $WZ + (\forall \alpha < \omega_1)(V(\alpha) \text{ exists})$. Also, we recognized a problem with coming up with an appropriate proof theoretic formulation of "cannot be proved using any definite countable transfinite iteration". See the definition of DCIPS and Theorem 0.12A.3.

With the benefit of hindsight, we can place Borel Determinacy nicely in the realm of Reverse Mathematics.

THEOREM 0.12B.1. The following are provably equivalent in RCA_0 .

- i. Finitely Borel Determinacy.
- ii. BFRA.

In particular, i) is provable in Z but not in WZC .

Proof: Assume i). First use Borel Determinacy for open sets to obtain ACA_0 and then ATR_0 , as in [Si99,09]. Then argue as in [Fr71] for any given level $n < \omega$ of the Borel hierarchy. Build the ramified hierarchy of level $n+5$ as far as it goes, starting with x , using well orderings on ω , and use Σ_n^0 determinacy with parameter x to show that the hierarchy must stop.

Assume ii). From the formulation using Tarski's satisfaction relation, ACA_0 is immediate. Now $\Pi_1^1-CA_0$ is immediate. By [Mart75], for each n , we have a proof that Σ_n^0 sets are determined from Z_{n+c} , for some universal constant c . Let A be in Σ_n^0 with code $u \subseteq \omega$, and let M be a β model of Z_{n+c} containing u . Then M satisfies that the Σ_n^0 set with code u is determined. Since M is a β model, A is determined. QED

THEOREM 0.12B.2. The following are provably equivalent in RCA_0 .

- i. Borel Determinacy.
- ii. BCRA.

In particular, i) is provable in $WZ(\Omega)$ but not provable in $DCIPS$.

Proof: A straightforward adaptation of the proof of Theorem 0.12B.1. Also uses Theorem 0.12A.3. QED

We now come to our method of converting Borel determinacy to a statement in classical analysis. In [Fr71], we presented the following asymmetric form:

For every Borel $Y \subseteq K \times K$,
 either Y contains the graph of a
 continuous function on K ,
 or the converse of Y is disjoint from
 the graph of a continuous function on K .

In [Fr71], we claimed that the independence proofs work equally well for the above. The proof from Borel Determinacy is utterly straightforward, the winning strategy giving us the continuous function F .

Later we discovered that we can work with only symmetric Borel $Y \subseteq K \times K$, and still have the same independence results. Here a set of ordered pairs E is said to be symmetric if and only if for all $(x, y) \in E$, we have $(y, x) \in E$.

THEOREM 0.12B.3. The following are provably equivalent in ATR_0 (all forms).

- i. Every symmetric finitely Borel set in $K \times K$ ($\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$) contains or is disjoint from the graph of a continuous (finitely Borel, Borel) function on K ($\mathbb{N}^{\mathbb{N}}$).
- ii. Every symmetric finitely Borel set in $\mathfrak{R} \times \mathfrak{R}$ ($I \times I$) contains or is disjoint from the graph of a left continuous (right continuous, finitely Borel, Borel) selection on \mathfrak{R} (I).
- iii. Finitely Borel Determinacy.
- iv. BFRA.

In particular, i-iv are provable in Z but not in WZC .

THEOREM 0.12B.4. The following are provably equivalent in ATR_0 (all forms).

- i. Every symmetric Borel set in $K \times K$ ($\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$) contains or is disjoint from the graph of a continuous (Borel) function on K ($\mathbb{N}^{\mathbb{N}}$).
- ii. Every symmetric Borel set in $\mathfrak{R} \times \mathfrak{R}$ ($I \times I$) contains or is disjoint from the graph of a left continuous (right continuous, finitely Borel, Borel) selection on \mathfrak{R} (I).
- iii. Borel Determinacy.
- iv. BCRA.

In particular, i-iv are provable in $\text{WZ}(\Omega)$ but not in ZC .

We need to explain the choices allowed in Theorems 0.12B.3 and 0.12B.4. Note that in each of the two Theorems, we have the following items for making a choice:

$$\begin{array}{c} K \times K \ (\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}) \\ \text{continuous (finitely Borel, Borel)} \\ K \ (\mathbb{N}^{\mathbb{N}}) \end{array}$$

$$\begin{array}{c} \mathfrak{R} \times \mathfrak{R} \ (I \times I) \\ \text{left continuous (right continuous, finitely Borel, Borel)} \\ \mathfrak{R} \ (I) \end{array}$$

Here is the list of choices that can be made:

$K \times K$; any of continuous, finitely Borel, Borel; K
 $\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$; any of continuous, finitely Borel, Borel; $\mathbb{N}^{\mathbb{N}}$

$\aleph \times \aleph$; any of left continuous, right continuous, finitely Borel, Borel; either of \aleph , \aleph

Proof: The above two theorems are essentially proved in [Fr81]. QED

0.12C. Borel Selection.

The work in this section appears in [Fr05], and was inspired by [DS96], [DS99], [DS01], [DS04], and [DS07].

Let S be a set of ordered pairs and A be a set. Then f is a selection for S on A if and only if $\text{dom}(f) = A$ and for all $x \in A$, $(x, f(x)) \in S$.

The following statement is well known to be refutable from $\text{ZFC} + V = L$, and relatively consistent with ZFC by a forcing argument.

DOM. $(\forall f \in \mathbb{N}^{\mathbb{N}}) (\exists g \in \mathbb{N}^{\mathbb{N}}) (\forall h \in \mathbb{N}^{\mathbb{N}} \cap L[f]) (g \text{ eventually strictly dominates } h)$.

All of the statements considered here are local/global in the sense that if we have a continuous or Borel selection on every compact subset of E , then we have a continuous or Borel section on all of E .

We consider the following two Templates.

TEMPLATE A. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ be Borel (finitely Borel). If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact subset of \mathbb{N}^{ω} , then there is a constant (continuous, finitely Borel, Borel) selection for S on $\mathbb{N}^{\mathbb{N}}$.

TEMPLATE B. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ and $E \subseteq \mathbb{N}^{\mathbb{N}}$ be Borel (finitely Borel). If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact subset of E , then there is a constant (continuous, finitely Borel, Borel) selection for S on E .

Note that Template A is just Template B for $E = \mathbb{N}^{\mathbb{N}}$.

The choices in these Templates are independent of each other. In other words, each Template has 32 instances - with two first options, four second options, and four third options.

THEOREM 0.12C.1. The following fourteen instances of Templates A,B are refutable in RCA_0 :

- i. Borel or finitely Borel, constant, constant.
- ii. Borel or finitely Borel, continuous, constant.
- iii. Borel or finitely Borel, finitely Borel, constant.
- iv. Borel or finitely Borel, finitely Borel, continuous.
- v. Borel or finitely Borel, Borel, constant.
- vi. Borel or finitely Borel, Borel, continuous.
- vii. Borel or finitely Borel, Borel, finitely Borel.

Proof: To refute i-iii,v, set $S(x,y) \leftrightarrow y$ everywhere dominates x . To refute iv,vi, let S be the graph of some $f:N^N \rightarrow N^N$ that is finitely Borel but not continuous. To refute vii), let S be the graph of some $f:N^N \rightarrow N^N$ that is Borel but not finitely Borel. QED

THEOREM 0.12C.2. The following eight instances below of Templates A,B are provable in Z but not in WZC .

- finitely Borel, constant, continuous.
- finitely Borel, constant, finitely Borel.
- finitely Borel, constant, Borel.
- finitely Borel, continuous, continuous.
- finitely Borel, continuous, finitely Borel.
- finitely Borel, continuous, Borel.
- finitely Borel, finitely Borel, finitely Borel.
- finitely Borel, finitely Borel, Borel.

Proof: In each case, the provability is implicit in [DS04], and reproved in [Fr05]. The unprovability is from [Fr05]. QED

THEOREM 0.12C.3. The following eight instances below of Templates A,B are provable in $WZ(\Omega)$, but are unprovable in $DCIPS$.

- Borel, constant, continuous.
- Borel, constant, finitely Borel.
- Borel, constant, Borel.
- Borel, continuous, continuous.
- Borel, continuous, finitely Borel.
- Borel, continuous, Borel.
- Borel, finitely Borel, finitely Borel.
- Borel, finitely Borel, Borel.

Proof: In each case, the provability is implicit in [DS04], and reproved in [Fr05]. The unprovability is from [Fr05]. QED

THEOREM 0.12C.4. The following two instances below of Templates A,B are provably equivalent, over ZFC, to DOM.

finitely Borel, Borel, Borel.
Borel, Borel, Borel.

Proof: The provability in ZFC + DOM for Templates A,B, is due to [DS07]. We prove DOM from these instances, for Templates A,B, over ZFC, in [Fr05]. We also give a proof of these instances from ZFC + DOM for Template A only, in [Fr05]. QED

We can use \mathfrak{R} instead of the Baire space $\mathbb{N}^{\mathbb{N}}$ as follows.

TEMPLATE A'. Let $S \subseteq \mathfrak{R} \times \mathfrak{R}$ be Borel (finitely Borel). If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact set of irrationals, then there is a constant (continuous, finitely Borel, Borel) selection for S on the irrationals.

TEMPLATE B'. Let $S \subseteq \mathfrak{R} \times \mathfrak{R}$ and E be a Borel (finitely Borel) set of irrationals. If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact subset of E , then there is a constant (continuous, finitely Borel, Borel) selection for S on the irrationals in E .

As in Templates A,B, the choices in these Templates are independent of each other. Thus each Template has 32 instances - with two first options, four second options, and four third options.

THEOREM 0.12C.1. The 32 instances of Template A and the corresponding instances of Template A' are respectively provably equivalent in ATR_0 . The 32 instances of Template B and the corresponding instances of Template B' are respectively provably equivalent in ATR_0 .

Proof: See [Fr05]. QED

The reason that we have run into independence from ZFC here is that in the

(finitely) Borel, Borel, Borel

instance of the Templates, the second Borel uses arbitrarily high levels of the Borel hierarchy. We regard this as just beyond the scope of Concrete Mathematical Incompleteness.

We also point out that these instances that are independent of ZFC, are Π^1_4 , and since they are provably equivalent to DOM, they are refutable in ZFC + V = L. (V = L is Gödel's axiom of constructibility [Go38], [Je76,06]).

In sections 13 and 14, we will encounter Concrete Mathematical Incompleteness from ZFC. In section 13, the use of finitely Borel leads to independence from ZFC.

For all of our examples of Concrete Mathematical Incompleteness from ZFC, we have independence from ZFC + V = L. For all of our examples of Concrete Mathematical Incompleteness from fragments T of ZFC, we have independence from T + V = L, where V = L is the standard analog of the axiom of constructability adapted to T.

0.12D. Borel Inclusion with Equivalence Relations.

Let $E \subseteq \mathfrak{N}^2$ be a Borel equivalence relation with field \mathfrak{N} . There has been considerable work in descriptive set theory concerning the classification of Borel equivalence relations under the Borel reducibility notion that was introduced in [FSt89]. See, e.g., [Ke95], [BK96], [HK96], [HK97], [HKL98], [HK01].

We say that x, y are E equivalent if and only if $E(x, y)$. We write E^* for the equivalence relation on \mathfrak{N}^∞ given by

$$E^*(x, y) \leftrightarrow \text{every coordinate of } x \text{ is E equivalent to a coordinate of } y, \text{ and vice versa.}$$

We give two forms of Borel Inclusion for E.

- i. Let $F: \mathfrak{N}^\infty \rightarrow \mathfrak{N}$ be Borel, where E* equivalent arguments are sent to E equivalent values. There exists $x \in \mathfrak{N}^\infty$ such that $F(x)$ is E equivalent to a coordinate of x .
- ii. Let $F: \mathfrak{N}^\infty \rightarrow \mathfrak{N}^\infty$ be Borel, where E* equivalent arguments are sent to E* equivalent values. There exists $x \in \mathfrak{N}^\infty$ such that every coordinate of $F(x)$ is E equivalent to a coordinate of x .

THEOREM 0.12D.1. Both forms of Borel Inclusion for Borel equivalence relations hold.

Proof: The first claim is proved in [Fr81], p. 235. For the second claim, let $F: \mathfrak{N}^\infty \rightarrow \mathfrak{N}^\infty$ be Borel, where E^* equivalent arguments are sent to E^* equivalent values. Let $G: (\mathfrak{N}^\infty)^\infty \rightarrow \mathfrak{N}^\infty$ be defined for all $x \in (\mathfrak{N}^\infty)^\infty$ by

$$G(x) = F(x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \dots).$$

We use E^{**} for the Borel equivalence relation on $(\mathfrak{N}^\infty)^\infty$ given by

$$E^{**}(x, y) \Leftrightarrow \text{every coordinate of } x \text{ is } E^* \text{ equivalent to a coordinate of } y, \text{ and vice versa.}$$

We claim that G maps E^{**} equivalent arguments to E^* equivalent values. To see this, let $x, y \in (\mathfrak{N}^\infty)^\infty$ be E^{**} equivalent. Then

$$\begin{aligned} &(x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \dots) \\ &(y_{11}, y_{12}, y_{21}, y_{13}, y_{22}, y_{31}, \dots) \end{aligned}$$

are E^* equivalent, and so their values under F are E^* equivalent.

By the first claim, let $G(x)$ be E^* equivalent to x_i .

$F(x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \dots)$ is E^* equivalent to $(x_{i1}, x_{i2}, x_{i3}, \dots)$.

QED

THEOREM 0.12D.2. The following are provably equivalent in ATR_0 .

i. Both forms of (finitely) Borel Inclusion for finitely Borel Equivalence Relations.

ii. FRA.

In particular, i) is provable in Z but not in WZC .

Proof: See [Fr81]. QED

THEOREM 0.12D.3. The following are provably equivalent in ATR_0 .

i. Both forms of Borel Inclusion for Borel Equivalence Relations.

ii. CRA.

In particular, i) is provable in $WZ(\Omega)$ but not in $DCIPS$.

Proof: See [Fr81]. QED

In [Fr81], we go on to deal with Borel Inclusion for N^N under conjugation. I.e., $f \approx g \leftrightarrow (\exists h)(g = hgh^{-1})$. This is a complete analytic equivalence relation. We again obtain Theorems 0.12D.2, 0.12D.3 for this equivalence relation. Subsequently, we improved this to analytic equivalence relations.

THEOREM 0.12D.4. The following are provably equivalent in ATR_0 .

i. Both forms of Borel Inclusion for Analytic Equivalence Relations, N^N under conjugation, graphs on N under isomorphism (a total of 6 forms).

ii. CRA.

In particular, each of the 6 forms of i) can be proved in $WZ(\Omega)$ but not in DCIPS.

Proof: For our proof of Borel Inclusion for Analytic Equivalence Relations, see [Sta85], p. 23. The second form is obtained from the first form as in the proof of Theorem 0.12D.1. QED

0.12E. Borel Functions on Linear orderings and Graphs.

The formulations in this section avoid infinite sequences, and attain the same level of strength as the statements in section 0.12D.

It is particularly convenient to think of countable linear orderings, up to isomorphism, as subsets of Q up to order isomorphism. Thus we have the nice Cantor space $\wp Q$ of subsets of Q . We say that $A, B \in \wp Q$ are isomorphic if and only if they are isomorphic as linearly ordered sets, in the induced order.

We say that $F: \wp Q \rightarrow \wp Q$ is isomorphic preserving if and only if isomorphic arguments are assigned isomorphic values.

Let $A_1, A_2, \dots \in \wp Q$. A dense mix is obtained by starting with Q , and replacing each point with some A_i , in such a way that for all i, j , strictly between any two copies of A_i , there is a copy of A_j . (We regard the A 's as distinct for this purpose). Note that all dense mixes of A_1, A_2, \dots are isomorphic.

THEOREM 0.12E.1. Every isomorphic preserving Borel $F: \wp Q \rightarrow \wp Q$ sends some A to an isomorphic copy of an interval in A with endpoints in A .

Proof: See [Sta85], where the result is derived from Borel Inclusion for Analytic Equivalence Relations. The idea is as follows. Given F , define $G: (\wp Q)^\infty \rightarrow \wp Q$ by $G(A_1, A_2, \dots) = F(B)$, where $B \in \wp Q$ is a canonically constructed dense mix of A_1', A_2', \dots , where each A_i' is the result of adding a left and right endpoint to A_i .

Now apply Borel inclusion for Analytic Equivalence Relations to G , and take the dense mix of the coordinates of the infinite sequence from $\wp Q$, after adding endpoints to these coordinates. QED

Let GPH be the space of all graphs whose vertex set is N or a finite subset of N . Here graphs are viewed as irreflexive symmetric relations on their vertex set.

We say that $F: GPH \rightarrow GPH$ is isomorphic preserving if and only if isomorphic arguments have isomorphic values (via ordinary graph isomorphism).

Let $CGPH$ be the subspace of all connected graphs.

THEOREM 0.12E.2. Every isomorphic preserving Borel $F: GPH \rightarrow CGPH$ maps some G to an isomorphic copy of a connected component of G .

Proof: Let F be as given, and define $H: CGPH^\infty \rightarrow CGPH$ by $H(G_1, G_2, \dots) = F(G^*)$, where G^* is the disjoint union of the G 's. Apply Borel inclusion for Analytic Equivalence Relations to H , and take the disjoint union of the infinite sequence from GPH . Thus we have G' such that $F(G')$ is isomorphic to one of the terms in the disjoint union representation of G' . I.e., $F(G')$ is isomorphic to a connected component of G' . QED

THEOREM 0.12E.3. The following are provably equivalent in ATR_0 .

- i. Every isomorphic preserving Borel $F: \wp Q \rightarrow \wp Q$ maps some A to an isomorphic copy of an interval in A (with endpoints in A).
- ii. Every isomorphic preserving Borel $F: GPH \rightarrow CGPH$ maps some G to an isomorphic copy of a connected component of G .
- iii. CRA.

In particular, i),ii) can be proved in $WZ(\Omega)$ but not in DCIPS.

Proof: For iii \rightarrow i,ii, use Theorem 0.12D.3, and the proofs of Theorems 0.12E.1, and 0.12E.2. For i \rightarrow ii, see [Sta85], p. 31. For ii \rightarrow iii, use a similar coding mechanism that associates hereditarily countable sets of a given countable rank or less, to connected graphs. QED

0.12F. Borel Functions on Borel Quasi Orders.

We say that (\mathfrak{R}, \leq) is a quasi order if and only if \leq is transitive and reflexive. We write $a \equiv b$ if and only if $(a \leq b \wedge b \leq a)$, $a < b$ if and only if $a \leq b \wedge \neg b \leq a$.

We say that (\mathfrak{R}, \leq) is ω -closed if every strictly increasing sequence from X has a (unique up to \equiv) least upper bound, and ω -complete if and only if every countable set has a least upper bound.

We say that $F: \mathfrak{R} \rightarrow \mathfrak{R}$ is invariant if and only if $a \equiv b \rightarrow F(a) \equiv F(b)$. A fixed point for F is an x such that $F(x) \equiv x$.

The following three Theorems are proved in [Fr81] using Borel determinacy.

THEOREM 0.12F.1. Let (\mathfrak{R}, \leq) be an ω -closed (ω -complete) Borel quasi order. Let $F: \mathfrak{R} \rightarrow \mathfrak{R}$ be an invariant Borel function such that for all x , $F(x) \geq x$. Then F has a fixed point.

THEOREM 0.12F.2. Let (\mathfrak{R}, \leq) be an ω -closed (ω -complete) Borel quasi order. Then there is no invariant Borel function such that for all x , $F(x) > x$.

THEOREM 0.12F.3. Let (\mathfrak{R}, \leq) be an ω -complete Borel quasi order. Let $F: \mathfrak{R} \rightarrow \mathfrak{R}$ be an invariant Borel function. Then for some x , $F(x) \leq x$.

THEOREM 0.12F.4. The following is provable in ATR_0 . $BCRA \rightarrow$ Theorems 0.12F.1 - 0.12F.3 \rightarrow CRA. In particular, Theorems 0.12F.1 - 0.12F.3 are provable in $WZ(\Omega)$ but not in DCIPS.

Proof: This is proved in [Fr81]. QED

Note that the definitions of ω -closed and ω -complete are Π^1_3 . In [Fr81], we strengthen these two notions to explicitly ω -closed and explicitly ω -complete, by requiring

that there be a Borel witness function giving a least upper bound.

THEOREM 0.12F.5. The following are provably equivalent in ATR_0 .

- i. Theorems 0.12F.1 - 0.12F.3 with explicitly ω -closed and ω -complete.
- ii. CRA.

In particular, i) is provable in $\text{WZ}(\Omega)$ but not in DCIPS.

Proof: This is proved in [Fr81]. QED

0.12G. Countable Borel Equivalence Relations and Quasi Orders.

In this section, we consider Borel equivalence relations E on \mathfrak{R}^n . We say that $A \subseteq \mathfrak{R}^n$ is E invariant if and only if $E(x, y) \rightarrow (x \in A \leftrightarrow y \in A)$. We say that $f: \mathfrak{R}^n \rightarrow \mathfrak{R}$ is E invariant if and only if $E(x, y) \rightarrow f(x) = f(y)$.

Let x_1, x_2, \dots be a sequence of real numbers that converges absolutely. We write $\text{SUM}(x_1, x_2, \dots)$ for the set of all sums of one or more of the x 's, without repetition of subscripts. We make this definition only if the x 's converge absolutely.

We say that a Borel equivalence relation E on \mathfrak{R} has the (finitely) Borel translation property if and only if every E invariant (finitely) Borel set contains or is disjoint from some translate of $\text{SUM}(4^{-1}, 4^{-2}, \dots)$.

We now present a stronger property.

We say that a Borel equivalence relation E on \mathfrak{R} has the strong (finitely) Borel translation property if and only if every E invariant (finitely) Borel $F: \mathfrak{R} \rightarrow \mathfrak{R}$ is constant on some translate of $\text{SUM}(4^{-1}, 4^{-2}, \dots)$.

THEOREM 0.12G.1. $\{(x, y): x, y \in \mathfrak{R} \wedge x = y\}$ does not satisfy the finitely Borel translation property.

Proof: In [Fr07a], Lemma 2.2, we showed how to construct elements of each $\text{SUM}(4^{-1}, 4^{-2}, \dots) + x$ from which we can reconstruct x . Let A be the set of all reals so constructed. Then obviously A meets every translate of $\text{SUM}(4^{-1}, 4^{-2}, \dots)$. Also every $y \in A$ lies in exactly one $\text{SUM}(4^{-1}, 4^{-2}, \dots) + x$.

Suppose A contains $\text{SUM}(4^{-1}, 4^{-2}, \dots) + x$. Then Let s, t be distinct elements of $\text{SUM}(4^{-1}, 4^{-2}, \dots)$. Then $s+x, t+x \in A$. Hence $s+(x+t-s) \in A$. Therefore $s+x$ lies in $\text{SUM}(4^{-1}, 4^{-2}, \dots) + x$ and $\text{SUM}(4^{-1}, 4^{-2}, \dots) + x+t-s$. Thus some element of A lies in more than one translate of $\text{SUM}(4^{-1}, 4^{-2}, \dots)$. This is a contradiction.

Clearly A neither contains nor is disjoint from some translate of $\text{SUM}(4^{-1}, 4^{-2}, \dots)$. It is easily seen that A is finitely Borel by its construction. QED

THEOREM 0.12G.2. There is a countable finitely Borel equivalence relation on \mathfrak{R} with the strong Borel translation property. Turing equivalence has the strong Borel summation property.

Proof: This is proved in [Fr07a], Theorem 2.6. QED

THEOREM 0.12G.3. The following are equivalent over ATR_0 .

- i. There is a countable (finitely) Borel equivalence relation on \mathfrak{R} with the finitely Borel translation property.
- ii. There is a countable (finitely) Borel equivalence relation on \mathfrak{R} with the strong finitely Borel translation property.
- iii. BFRA.

In particular, i, ii are provable in Z but not in WZC .

Proof: This is proved in [Fr07a], Theorems 2.9, 2.11. QED

THEOREM 0.12G.4. The following are equivalent over ATR_0 .

- i. There is a countable (finitely) Borel equivalence relation on \mathfrak{R} with the Borel translation property.
- ii. There is a countable (finitely) Borel equivalence relation on \mathfrak{R} with the strong Borel translation property.
- iii. BCRA.

In particular, i) is provable in $\text{WZ}(\Omega)$ but not in DCIPS .

Proof: This is proved in [Fr07a], Theorems 2.9, 2.11. QED

It is clear that if a countable Borel equivalence relation on \mathfrak{R} has the Borel translation property, then any more inclusive countable Borel equivalence relation on \mathfrak{R} also has the Borel translation property. In fact, in [Fr07a], we assert that all sufficiently inclusive countable Borel equivalence relations on \mathfrak{R} have the (strong) Borel translation property.

So there remains the unanswered question of how to describe the threshold, whereby the (strong) Borel translation property kicks in.

What about Lebesgue or Baire measurable functions? Then the (finitely) Borel translation property is impossible.

THEOREM 0.12G.5. There is no countable Borel equivalence relation on \mathfrak{R} , where every E invariant set of measure 0 (or meager) contains or is disjoint from some translate of $\text{SUM}(4^{-1}, 4^{-2}, 4^{-3}, \dots)$.

Proof: This is proved in [Fr07a], Theorem 2.12. QED

In higher dimensions, these results take on a more geometric meaning. A curve is a homeomorphic image of $[0,1]$ in \mathfrak{R}^n .

We say that a Borel equivalence relation E on \mathfrak{R}^2 has the (finitely) Borel line, curve, vertical line, horizontal line, circle about the origin, property if and only if every invariant (finitely) Borel set contains or is disjoint from a line, curve, vertical line, horizontal line, circle about the origin.

We now present a stronger property.

We say that a Borel equivalence relation E on \mathfrak{R}^2 has the (finitely) Borel line, curve, vertical line, horizontal line, circle about the origin, property if and only if every invariant (finitely) Borel $F: \mathfrak{R}^2 \rightarrow \mathfrak{R}$ is constant on a line, curve, vertical line, horizontal line, circle about the origin.

THEOREM 0.12G.6. There is a countable finitely Borel equivalence relation on \mathfrak{R}^2 , with the strong Borel vertical line, horizontal line, circle about the origin, property.

Proof: This is proved in [Fr07a], Theorem 3.1, using Borel Turing degree determinacy. QED

Once again, there is the unanswered question of the threshold, since evidently all sufficiently inclusive countable (finitely) Borel equivalence relations on \mathfrak{R}^2 have these properties.

THEOREM 0.12G.7. The following are provably equivalent in ATR_0 .

- i. There is a countable (finitely) Borel equivalence relation on \mathfrak{R}^2 with the finitely Borel line, curve, vertical line, horizontal line, circle about the origin, property.
 - ii. There is a countable (finitely) Borel equivalence relation on \mathfrak{R}^2 with the strong finitely Borel line, curve, vertical line, horizontal line, circle about the origin, property.
 - iii. BFRA.
- In particular, i),ii) can be proved in Z but not in WZC.

Proof: This is implicit in [Fr07a]. QED

THEOREM 0.12G.8. The following are provably equivalent in ATR_0 .

- i. There is a countable (finitely) Borel equivalence relation on \mathfrak{R}^2 with the Borel line, curve, vertical line, horizontal line, circle about the origin, property.
- ii. There is a countable (finitely) Borel equivalence relation on \mathfrak{R}^2 with the strong Borel line, curve, vertical line, horizontal line, circle about the origin, property.
- iii. BCRA.

In particular, i-iii can be proved in $Z(\Omega)$ but not in DCIPS.

Proof: This is proved in [Fr07a]. QED

We say that (\mathfrak{R}, \leq) is a quasi order if and only if \leq is reflexive and transitive on X . We define $x \equiv y \leftrightarrow x \leq y \wedge y \leq x$. We say that (\mathfrak{R}, \leq) is an ω_1 like quasi order if and only if (X, \leq) is a quasi order where each $\{y: y \leq x\}$ is countable.

We say that $B \subseteq \mathfrak{R}$ is invariant if and only if $x \equiv y \rightarrow (x \in B \leftrightarrow y \in B)$. We say that $F: \mathfrak{R} \rightarrow \mathfrak{R}$ is invariant if and only if $x \equiv y \rightarrow f(x) = f(y)$.

A cone in (\mathfrak{R}, \leq) is a set of the form $\{y: x \leq y\}$, $x \in \mathfrak{R}$.

We say that a Borel quasi order \leq on \mathfrak{R} has the (finitely) Borel cone property if and only if every invariant (finitely) Borel set A contains or is disjoint from a cone.

We say that a Borel quasi order \leq on \mathfrak{R} has the strong (finitely) Borel cone property if and only if every invariant (finitely) Borel $F: \mathfrak{R} \rightarrow \mathfrak{R}$ is constant on a cone.

THEOREM 12G.9. There is a countable finitely Borel quasi order \leq on \mathfrak{R} with the strong Borel cone property.

Proof: This is proved in [Fr07a]. Turing reducibility, \leq_T , has the strong Borel cone property. QED

THEOREM 0.12G.10. The following are provably equivalent in ATR_0 .

- i. There is a countable (finitely) Borel quasi order on \mathfrak{R} with the finitely Borel cone property.
- ii. There is a countable (finitely) Borel quasi order on \mathfrak{R} with the strong finitely Borel cone property.
- iii. BFRA.

In particular, i),ii) are provable in Z but not in WZC .

Proof: This is implicit in [Fr07a]. QED

THEOREM 0.12G.11. The following are provably equivalent in ATR_0 .

- i. There is a countable (finitely) Borel quasi order on \mathfrak{R} with the Borel cone property.
- ii. There is a countable (finitely) Borel quasi order on \mathfrak{R} with the strong Borel cone property.
- iii. BCRA.

In particular, i),ii) are provable in $Z(\Omega)$ but not in DCIPS .

Proof: This is proved in [Fr07a]. QED

Let \leq be a quasi order on \mathfrak{R} . We say $F:\mathfrak{R}^\omega \rightarrow \mathfrak{R}$ is left/right invariant if and only if for all $x,y \in \mathfrak{R}^\omega$, if x,y are coordinatewise \approx , then $F(x) \approx F(y)$.

THEOREM 0.12G.12. There is a countable finitely Borel quasi order \leq on \mathfrak{R} such that the following holds. For all left/right invariant Borel $F:\mathfrak{R}^\omega \rightarrow \mathfrak{R}$, there exists $x \in \mathfrak{R}^\omega$ and $n < \omega$ such that $F(x) \leq x_n$.

Proof: We established in [Sta85], using Turing degrees. The proof lies in $\text{ZF}\setminus\text{P} + \text{V}(\omega+\omega)$ exists. QED

THEOREM 0.12G.13. Theorem 0.12G.12 is provable in $\text{ZF}\setminus\text{P} + \text{V}(\omega+\omega)$. Theorem 0.12G.12 is not provable in ZC , even for Borel \leq and finitely Borel F .

Which countable Borel quasi orders have the (strong) Borel cone property? $\{(x,y) : x,y \in \mathfrak{R} \wedge y-x \in \mathbb{N}\}$ does not have the finitely Borel cone property, using the invariant set $\{x \in \mathfrak{R} : \text{the integer part of } x \text{ is even}\}$. What can we say about the threshold?

We have recently discovered a kind of universality condition on a countable Borel quasi order \leq on $2^{\mathbb{N}}$ that is sufficient for the strong Borel cone property.

Let \leq be a Borel quasi order on $2^{\mathbb{N}}$. We say that \leq is continuously full if and only if for all continuous $F:2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}}$, there is a cone C in \leq such that $(\forall x \in C) (F(x) \leq x)$.

We say that \leq is strongly continuously full if and only if for all continuous $F_i:2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}}$, $i \geq 1$, there is a cone C in \leq such that $(\forall x \in C) (\forall i \geq 1) (F_i(x) \leq x)$.

We now formulate the Borel cone property, and the strong Borel cone property for \leq , using $2^{\mathbb{N}}$ everywhere instead of \mathfrak{R} .

THEOREM 0.12G.14. There is a finitely Borel quasi order on $2^{\mathbb{N}}$ which is strongly continuously full. In fact, $\leq_{\mathbb{T}}$ on $2^{\mathbb{N}}$ is strongly continuously full.

Proof: Let $F_i:2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}}$ be continuous, $i \geq 1$. Let $u_i \in 2^{\mathbb{N}}$ appropriately code F_i , respectively. Let u be the join of the u_i , $i \geq 1$. Let C be the cone in $\leq_{\mathbb{T}}$ with base u . We have only to verify that $v \geq_{\mathbb{T}} u \rightarrow F_i(v) \leq_{\mathbb{T}} v$. This is clear. QED

THEOREM 0.12G.15. Every continuously full Borel quasi order on $2^{\mathbb{N}}$ has the Borel cone property.

Proof: Let \leq be a continuously full Borel quasi order on $2^{\mathbb{N}}$. Let $A \subseteq 2^{\mathbb{N}}$ be Borel and \leq invariant.

I,II play a game, with outcomes $x,y \in 2^{\mathbb{N}}$. II wins if and only if $x \notin A \vee (\neg y < x \wedge y \notin A)$.

A winning strategy H is a continuous function from $2^{\mathbb{N}}$ into $2^{\mathbb{N}}$, with the identity function as a modulus of continuity. By continuous fullness, let u be the base of a cone C where $x \in C \rightarrow H(x) \leq x$.

case 1. I wins. If II plays $y \in C \setminus A$ then I plays $H(y) \leq y$, and we have $H(y) \in A$, $\neg(\neg y < H(y) \wedge y \notin A)$, which is a contradiction. Hence A contains the cone C .

case 2. II wins. If I plays $x \in C \cap A$ then II plays $H(x) \leq x$, and we have $\neg H(x) < x$, $H(x) \notin A$, $H(x) \equiv x$, $H(x) \in A$, which is a contradiction. Hence A is disjoint from the cone C .

QED

LEMMA 0.12G.16. In every strongly continuously full Borel quasi order on $2^{\mathbb{N}}$, every infinite sequence has an upper bound (\geq).

Proof: Let x_1, x_2, \dots . Use the sequence of continuous functions which are constantly x_1, x_2, \dots . QED

THEOREM 0.12G.17. Every strongly continuously full Borel quasi order on $2^{\mathbb{N}}$ has the strong Borel cone property.

Proof: Apply Lemma 0.12G.16 to the bases of the cones given by Theorem 0.12G.15. QED

THEOREM 0.12G.18. The following are provably equivalent in ATR_0 .

- i. Every continuously full finitely Borel quasi order on $2^{\mathbb{N}}$ has the finitely Borel cone property.
- ii. Every strongly continuously full finitely Borel quasi order on $2^{\mathbb{N}}$ has the strong finitely Borel cone property.
- iii. BFRA.

In particular, i,ii are provable in Z but not in WZC .

Proof: From the above, and the metamathematics of Borel determinacy and Borel Turing degree determinacy. QED

THEOREM 0.12G.19. The following are provably equivalent in ATR_0 .

- i. Every continuously full (finitely) Borel quasi order on $2^{\mathbb{N}}$ has the Borel cone property.
- ii. Every strongly continuously full (finitely) Borel quasi order on $2^{\mathbb{N}}$ has the strong Borel cone property.
- iii. BCRA.

In particular, i,ii are provable in $Z(\Omega)$ but not in DCIPS .

Proof: From the above, and the metamathematics of Borel determinacy and Borel Turing degree determinacy. QED

0.12H. Borel Sets and Functions in Groups.

As in section 0.11D, we define GRP as the space of groups whose domain is \mathbb{N} or a finite subset of \mathbb{N} . We let FGG be

the subspace of GRP consisting of the finitely generated elements of GRP.

We say that $F:GRP \rightarrow \mathfrak{R}$ is isomorphically invariant if and only if for all $G, H \in GRP$, if G, H are isomorphic then $F(G) = F(H)$.

We say that $A \subseteq GRP$ is unbounded if and only if every $G \in GRP$ is embeddable in an element of A .

THEOREM 0.12H.1. Every isomorphically invariant finitely Borel function $F:FGG \rightarrow \mathfrak{R}$ is constant on an unbounded Borel subset of FGG of finite rank. In fact, Borel rank ≤ 4 suffices.

Proof: This is proved in [Fr07a], Theorem 5.4. The exact rank needed depends on the exact setup of FGG as a Borel space. Here 4 is a crude upper bound that works for even naïve setups. QED

THEOREM 0.12H.2. Every isomorphically invariant Borel subset of FGG contains or is disjoint from an unbounded Borel set of finite Borel rank. In fact, Borel rank ≤ 4 suffices.

Proof: Immediate from Theorem 0.12H.1. QED

THEOREM 0.12H.3. Theorem 0.12H.1 is provable in Z but not in WZC. Theorem 12H.2 is provable in $Z(\Omega)$ but not using any countable iteration of the power set operation.

Proof: See [Fr07a]. QED

We now consider Borel $F:FGG^\infty \rightarrow FGG$. We say that F is isomorphic preserving if and only if for all $\alpha, \beta \in FGG^\infty$, if α, β are coordinatewise isomorphic, then $F(\alpha), F(\beta)$ are isomorphic.

THEOREM 0.12H.4. For all isomorphic preserving Borel $F:FGG^\infty \rightarrow FGG$, there exists $\alpha \in FGG^\infty$ such that $F(\alpha)$ is embeddable in a coordinate of α .

Proof: See [Sta85], p. 35. QED

We consider Borel $F:FGG^\infty \rightarrow GRP$. We say that F is isomorphic preserving if and only if for all $\alpha, \beta \in FGG^\infty$, if α, β are coordinatewise isomorphic, then $F(\alpha), F(\beta)$ are isomorphic.

THEOREM 0.12H.5. For all isomorphic preserving Borel $F:FGG^\infty \rightarrow GRP$, there exists $\alpha \in FGG^\infty$ such that $F(\alpha)$ is embeddable in some direct limit of $\alpha_1, \alpha_2, \dots$.

Proof: Implicit in [Sta85]. QED

THEOREM 0.12H.6. Theorems 0.12H.4 and 0.12H.5 are provable in $ZFC \setminus P + "V(\omega+\omega) \text{ exists}"$ but not in ZC. Theorems 0.12H.4 and 0.12H.5 for finitely Borel F are not provable in ZC.

Proof: Implicit in [Sta85]. QED

0.13. Incompleteness in ZFC using Borel Functions.

0.13A. Preliminaries.

0.13B. Borel Ramsey Theory.

0.13C. Borel Functions on Groups.

0.13D. Borel Functions on Borel Quasi Orders.

0.13E. Borel Functions on Countable Sets.

0.13A. Preliminaries.

ZF is the following well known axiom system with one binary relation symbol \in , in one sorted first order predicate calculus with equality.

EXTENSIONALITY. $(\forall x)(x \in y \leftrightarrow x \in z) \rightarrow y = z$.

PAIRING. $(\exists x)(y \in x \wedge z \in x)$.

UNION. $(\exists x)(\forall y)(\forall z)(y \in z \wedge z \in w \rightarrow y \in x)$.

SEPARATION. $(\exists x)(\forall y)(y \in x \leftrightarrow y \in z \wedge \varphi)$, where x is not free in φ .

POWER SET. $(\exists x)(\forall y)((\forall z)(z \in y \rightarrow z \in x) \rightarrow z \in x)$.

INFINITY. $(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow y \cup \{y\} \in x))$.

FOUNDATION. $y \in x \rightarrow (\exists y)(y \in x \wedge (\forall z)(\neg(z \in x \wedge z \in y)))$.

REPLACEMENT. $(\forall x)(x \in u \rightarrow (\exists! y)(\varphi)) \rightarrow (\exists z)(\forall x)(x \in u \rightarrow (\exists y \in z)(\varphi))$, where $\varphi \in L(\in)$, and z is not free in φ .

ZFC is ZF together with

CHOICE. If x is a set of pairwise disjoint nonempty sets, there is a set which has exactly one element in common with each of the elements of x .

As discussed in section 0.3, we sharply distinguish typical statements in set theory from statements involving at most finitely Borel sets and functions on complete separable metric spaces. In this section we will consider only Concrete Mathematical Incompleteness involving finitely

Borel sets and functions on complete separable metric spaces.

Recall that we have already presented the following Mathematical Incompleteness from ZFC in section 0.12C, using Borel sets.

FROM TEMPLATE A. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ be (finitely) Borel. If there is a Borel selection for S on every compact subset of E , then there is a Borel selection for S on E .

FROM TEMPLATE B. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ and $E \subseteq \mathbb{N}^{\mathbb{N}}$ be (finitely) Borel. If there is a Borel selection for S on every compact subset of E , then there is a Borel selection for S on E .

We don't classify these as Concrete Mathematical Incompleteness, as it is not confined to finitely Borel sets. See the last four paragraphs of section 0.12C.

In section 0.12C, we also discussed the versions with $\mathbb{N}^{\mathbb{N}}$ replaced by \mathfrak{R} , above.

The Concrete Mathematical Incompleteness in this section overshoots ZFC considerably.

In section 0.13B, we use strongly Mahlo cardinals of finite order. These also represent the level associated with the Exotic Case which preoccupies Chapters 4-6 of this book. The Mahlo cardinals of finite order are defined in section 0.14A.

In sections 0.13C and 0.13D, we use the much stronger large cardinal hypotheses asserting the existence of Ramsey cardinals and measurable cardinals. Yet stronger large cardinal hypotheses are used in section 0.13E.

A Ramsey cardinal is a cardinal κ with the partition property $\kappa \rightarrow \kappa^{<\omega}_2$, which asserts the following. If we partition the nonempty finite sequences from κ into 2 pieces, then there exists $A \subseteq \kappa$ of cardinality κ such that for all $1 \leq n < \omega$, all of the n -tuples from κ lie in the same piece.

A measurable cardinal is an uncountable cardinal κ such that there is a $\{0,1\}$ valued measure μ on $\wp(\kappa)$ which is $<\kappa$ additive, $\mu(\kappa) = 1$, and each $\mu(\{\alpha\}) = 0$.

It is well known that the first measurable cardinal (if it exists) is much larger than the first Ramsey cardinal. See, e.g., [Ka94], p. 83, and [Je78], p. 328.

In section 0.13E, we will use the yet much stronger Woodin cardinals. The notion of Woodin cardinal is a specialized notion that matches up exactly with determinacy (corresponding to infinitely many Woodin cardinals); see [MS89], [KW ∞].

A Woodin cardinal is a cardinal κ such that for any $f:\kappa \rightarrow \kappa$, there exists an elementary embedding $j:V \rightarrow M$, M transitive, with critical point $\alpha < \kappa$ such that $f[\alpha] \subseteq \alpha$ and $V_{j(f)(\alpha)} \subseteq M$.

A Woodin cardinal is a weakening of the more natural notion of superstrong cardinal: there exists an elementary embedding $j:V \rightarrow M$, M transitive, with critical point κ such that $V_{j(\kappa)} \subseteq M$. See [Ka94], p. 361. Every superstrong cardinal is a Woodin cardinal, but not vice versa (assuming there is a Woodin cardinal).

A Woodin cardinal is also a strengthening of the specialized notion of strong cardinal, in terms of consistency strength. We refer the reader to [Ka94], p. 358, for its definition.

Our first Concrete Mathematical Incompleteness from ZFC was Borel Ramsey Theory, involving (finitely) Borel functions on \mathfrak{R}^∞ . We have already encountered such functions in section 0.11C.

Later, we discovered statements involving Borel functions from infinite sequences of Turing degrees into Turing degrees, which can be proved using a measurable cardinal but not a Ramsey cardinal. An account of this work appears in [Sta85].

Still later, we converted the Turing degrees into finitely generated groups (FGG), and more recently, points in countable Borel quasi orders. See sections 0.13C and 0.13D. The extensions involving (finitely) Borel functions on countable sets discussed in section 0.13E are the strongest of all - reaching the level of multiple Woodin cardinals.

0.13B. Borel Ramsey Theory.

Recall the Borel Ramsey Theorem (otherwise known as the Galvin/Prikry theorem) discussed in section 0.10D. This combines Borel measurability with Ramsey theory.

We discovered yet more powerful combinations of Borel measurability with Ramsey theory, that go beyond ZFC.

For this development, we use the infinite product space \mathfrak{R}^ω , which is a complete separable metric space in the natural way. We write $x \sim y \leftrightarrow x, y \in \mathfrak{R}^\omega \wedge y$ is a permutation of x .

PROPOSITION 0.13B.1. Let $F: \mathfrak{R}^\omega \times (\mathfrak{R}^\omega)^n \rightarrow \mathfrak{R}$ be a (finitely) Borel function such that if $x \in \mathfrak{R}^\omega$, $y, z \in (\mathfrak{R}^\omega)^n$, and $y \sim z$, then $F(x, y) = F(x, z)$. Then there is a sequence $\{x_k\}$ from \mathfrak{R}^ω of length $m \leq \omega$ such that for all indices $s < t_1 < \dots < t_n \leq m$, $F(x_s, x_{t_1}, \dots, x_{t_n})$ is the first coordinate of x_{s+1} .

THEOREM 0.13B.2. Proposition 0.13B.1 for Borel functions is provable in $ZFC + (\forall n)\exists \kappa$ (κ is strongly n -Mahlo). However, for all n , $ZFC + (\exists \kappa)$ (κ is strongly n -Mahlo) + $V = L$ does not prove Proposition 0.13B.1 for finitely Borel functions, using $m < \omega$ (instead of $m \leq \omega$). $ZFC + V = L$ does not prove Proposition 0.13B.1 for $n = 4$ and finitely Borel functions, using $m < \omega$ (instead of $m \leq \omega$).

Proof: This is proved in [Fr01], section 5. QED

In [Fr01], Proposition 0.13B.1 is couched in terms of the Hilbert cube I^ω , which is, of course, equivalent to \mathfrak{R}^ω for present purposes.

In [Ka89], a more refined analysis of Proposition 0.13B.1 is presented. In [Ka91], a strengthening of Proposition 0.13B.1 that corresponds to the subtle cardinal hierarchy is presented. The subtle cardinal hierarchy is presented in section 0.14A.

0.13C. Borel Functions on Borel Quasi Orders.

Let \leq be a quasi order on \mathfrak{R} . We say that $F: \mathfrak{R}^\omega \rightarrow \mathfrak{R}$ is \approx preserving if and only if for all $x, y \in \mathfrak{R}^\omega$, if x, y are coordinatewise \approx , then $F(x) \approx F(y)$.

Recall that a quasi order is said to be countable if and only if the set of predecessors of any point is countable.

A finite deletion subsequence is a subsequence obtained by deleting finitely many terms.

PROPOSITION 0.13C.1. There is a countable (finitely) Borel quasi order \leq on \mathfrak{R} such that the following holds. For all \approx preserving (finitely) Borel $F:\mathfrak{R}^\omega \rightarrow \mathfrak{R}$, there exists $x \in \mathfrak{R}^\omega$ such that for all infinite subsequences y of x , there exists n such that $F(y) \leq x_n$.

PROPOSITION 0.13C.2. There is a countable (finitely) Borel quasi order \leq on \mathfrak{R} such that the following holds. For all \approx preserving (finitely) Borel $F:\mathfrak{R}^\omega \rightarrow \mathfrak{R}$, there exists $x \in \mathfrak{R}^\omega$ and $n < \omega$ such that for all infinite (finite deletion) subsequences y of x , $F(y) \leq y_n$.

THEOREM 0.13C.3. All forms of Proposition 0.13C.1 and 0.13C.2 are provable in ZFC + "there exists a measurable cardinal" but not in ZFC + "there exists a Ramsey cardinal". The same holds for their relativizations to the constructible universe, L , or even to the sets recursive in the first ω hyperjumps of \emptyset .

Proof: We originally proved this with "there exists a Ramsey cardinal" replaced by " $(\forall x \subseteq \omega) (x\# \text{ exists})$ ", at least breaking the constructibility barrier in large cardinals (see [Sta85]). However our arguments can be combined with the inner model theory of large cardinals below a measurable cardinal - as was first observed by R. Solovay (private communication and lectures). QED

PROPOSITION 0.13C.4. There is a countable (finitely) Borel quasi order \leq on \mathfrak{R} such that the following holds. For all \approx preserving (finitely) Borel $F:\mathfrak{R}^{\omega+\omega} \rightarrow \mathfrak{R}$, there exists $x \in \mathfrak{R}^{\omega+\omega}$ and $\alpha < \omega+\omega$ such that for all finite deletion subsequences y of x , $F(y) \leq y_\alpha$.

THEOREM 0.13C.5. All forms of Proposition 0.13C.4 are provable in ZFC + "there exists a strong cardinal", but not in ZFC + "there exists arbitrarily large measurable cardinals". The same holds for their relativizations to the constructible universe, L , or even to the sets recursive in the first ω hyperjumps of \emptyset .

Proof: This also combines work of ours reported in [Sta85] with the inner model theory of "strongly" measurable cardinals. QED

0.13D. Borel Functions on Groups.

This section is basically a reworking of section 0.13C using the space FGG of finitely generated groups. However, there are some additional statements involving the space GRP of all countable groups. Recall that we have already introduced these spaces in section 0.12H.

We say that x in GRP^ω is towered if and only if for all n , x_n is a subgroup of x_{n+1} .

We say that $F:FGG^\omega \rightarrow GRP$ is isomorphic preserving if and only if for all $x, y \in \mathfrak{N}^\omega$, if x, y are coordinatewise isomorphic, then $F(x), F(y)$ are isomorphic.

PROPOSITION 0.13D.1. For all isomorphic preserving (finitely) Borel $F:FGG^\omega \rightarrow GRP$, ($F:FGG^\omega \rightarrow FGG$), there exists towered $x \in FGG^\omega$ such that for all infinite subsequences y of x , $F(y)$ is embeddable in $\bigcup_n x_n$.

PROPOSITION 0.13D.2. For all isomorphic preserving (finitely) Borel $F:FGG^\omega \rightarrow FGG$, there exists $x \in FGG^\omega$ and $n < \omega$ such that for all infinite (finite deletion) subsequences y of x , $F(y)$ is embeddable in y_n .

THEOREM 0.13D.3. All forms of Proposition 0.13D.1 and 0.13D.2 are provable in ZFC + "there exists a measurable cardinal" but not in ZFC + "there exists a Ramsey cardinal". The same holds for their relativizations to the constructible universe, L , or even to the sets recursive in the first ω hyperjumps of \emptyset .

Proof: We originally proved this with "there exists a Ramsey cardinal" replaced by " $(\forall x \subseteq \omega) (x\# \text{ exists})$ ", at least breaking the constructibility barrier in large cardinals (see [Sta85]). However our arguments can be combined with the inner model theory of large cardinals below a measurable cardinal - as was first observed by R. Solovay (private communication and lectures). QED

PROPOSITION 0.13D.4. For all isomorphic preserving (finitely) Borel $F:FGG^{\omega+\omega} \rightarrow FGG$, there exists $x \in \mathfrak{N}^{\omega+\omega}$ and $\alpha < \omega+\omega$ such that for all finite deletion subsequences y of x , $F(y)$ is embeddable in y_α .

THEOREM 0.13D.5. All forms of Proposition 0.13D.4 are provable in ZFC + "there exists two measurable cardinals", but not in ZFC + "there exists a measurable cardinal". The same holds for their relativizations to the constructible

universe, L , or even to the sets recursive in the first ω hyperjumps of \emptyset .

Proof: This also combines work of ours reported in [Sta85] with the inner model theory of a measurable cardinal. QED

0.13E. Borel Functions on Countable Sets.

We write $CS(\mathfrak{N})$ for the space of countable subsets of \mathfrak{N} . This is to be viewed as the space \mathfrak{N}^ω , under the equivalence relation "having the same range".

The notions of a Borel function $F:CS(\mathfrak{N}) \rightarrow \mathfrak{N}$, or $F:CS(\mathfrak{N}) \rightarrow CS(\mathfrak{N})$ are very natural. For the former, we mean that there is a Borel function $G:\mathfrak{N}^\omega \rightarrow \mathfrak{N}$ such that $F(\text{rng}(x)) = G(x)$. Note that G must be invariant in the sense used in section 0.11C.

For the latter, we mean that there exists a Borel function $H:\mathfrak{N}^\omega \rightarrow \mathfrak{N}^\omega$ such that $F(\text{rng}(x)) = \text{rng}(H(x))$. Note that H must be image preserving in the sense used in section 0.11D.

THEOREM 0.13E.1. For all Borel $F:CS(\mathfrak{N}) \rightarrow \mathfrak{N}$, there exists $x \in CS(\mathfrak{N})$ such that $F(x) \in x$. For all Borel $F:CS(\mathfrak{N}) \rightarrow CS(\mathfrak{N})$, there exists $x \in CS(\mathfrak{N})$ such that $F(x) \subseteq x$.

Proof: The first claim is equivalent to Theorem 0.11D.1 using image invariance. The second claim is equivalent to Theorem 0.11D.2 using image preserving. Thus these two statements correspond to roughly Z_2 . QED

Now let \leq be a quasi order on \mathfrak{N} , and $A, B \subseteq \mathfrak{N}$. We say that x is a break point for A in B, \leq if and only if $x \in A \subseteq B$, and

- i. $(\forall y \in B) (y \geq x \rightarrow (\exists z \in A) (z \equiv y))$; or
- ii. $(\forall y \in B) (y \geq x \rightarrow (\exists z \notin B) (z \equiv y))$.

PROPOSITION 0.13E.2. There is a countable (finitely) Borel quasi order \leq such that for all (finitely) Borel $F:\mathfrak{N}^2 \times CS(\mathfrak{N}) \rightarrow CS(\mathfrak{N})$, there exists nonempty A such that each $F(x, y, A)$, $x, y \in A$, has a break point in A, \leq .

Let λ be a countable limit ordinal. A λ -model of Z_2 is an ω model $M \subseteq \wp\omega$, of Z_2 , where every subset of ω lying in the first λ levels of the constructible hierarchy starting with M and its elements, lies in M .

LEMMA 0.13E.3. Proposition 0.13E.2 (all four forms) is provable in $ZFC + L(\aleph)$ determinacy. In fact, $ZFC + L_{\omega_1}(\aleph)$ determinacy suffices. For finitely Borel, $ZFC +$ projective determinacy suffices.

Proof: We argue in $ZFC + L_{\omega_1}(\aleph)$ determinacy. We set $\leq = \leq_T$. Let $\lambda < \omega_1$, $u \subseteq \omega$, code $F: \aleph^2 \times CS(\aleph) \rightarrow CS(\aleph)$. Let M be the transitive collapse of a countable elementary substructure of $V(\omega_1 + \lambda)$ that contains the elements $\lambda + 1, u$, and the subset λ . Let $A = M \cap \wp\omega$. Then A is a countable λ -model of Z_2 containing u , and $L_\lambda(\aleph)$ determinacy holds in M .

By using an M generic enumeration of A (with finite conditions), we see that for all $x, y \in A$, $F(x, y, A)$ is a subset of A lying in the internal $L_\lambda(\aleph)$ of M . Therefore we can apply $L_\lambda(\aleph)$ determinacy within M , which implies $L_\lambda(\aleph)$ Turing degree determinacy. Thus we obtain the required break points in A . QED

By a degree, we mean a pair $\lambda < \omega_1$ and $x \subseteq \omega$ coding λ , where we use $y \leq_{\lambda, x} z \leftrightarrow y \in L_\lambda(x, z)$. By projective degree determinacy, we mean "there exists a degree such that every projective set of degrees contains or is disjoint from a cone".

LEMMA 0.13E.4. Proposition 0.13E.2 with "finitely" implies the existence of an ω model of Σ^1_n -CA + " Σ^1_n degree determinacy holds for some degree", for each $n < \omega$, over ATR_0 . Proposition 0.13E.2 implies the existence of an ω model of $L_{\omega+\omega}(\aleph)$ -CA + " $L_{\omega+\omega}(\aleph)$ determinacy holds for some degree".

Proof: This uses the techniques from [Fr81] for constructing ω models from Borel statements of this general form. Let \leq be given by Proposition 0.13E.2. Let u be a Borel code for \leq . Let $F: \aleph^2 \times CS(\aleph) \rightarrow CS(\aleph)$ be a finitely Borel function such that

- i. If $x < y$ then $F(x, y, A)$ is singleton of the $[x]$ -th Σ^1_n subset of ω with parameters x, y , provided $u \in A$; u otherwise.
- ii. If $x \geq y$ then $F(x, y, A)$ is the $[x]$ -th Σ^1_n subset of A with parameters x, y , provided $u \in A$; u otherwise.

Let A be nonempty, where each $F(x, y, A)$, $x, y \in A$, has a break point in A, \leq . In particular, each $F(x, y, A)$, $x, y \in A$, is a subset of A . It is now clear that $u \in A$, and that A is

an ω model of Σ^1_n -CA. We also see by the break points that A satisfies Σ^1_n determinacy for \leq .

The second claim is proved analogously. QED

LEMMA 0.13E.5. ZFC + "there exists infinitely many Woodin cardinals" proves projective determinacy. ZFC + "there exists a measurable cardinal above infinitely many Woodin cardinals" proves $L(\mathcal{R})$ determinacy.

Proof: The first claim is from [MSt89]. The second claim is from [Wo88] and [Lar04]. QED

THEOREM 1.13E.6. Proposition 0.13E.2 (all four forms) are provable in ZFC + "there exists a measurable cardinal above infinitely many Woodin cardinals", but not in ZFC + "there exists infinitely Woodin cardinals". Proposition 0.13E.2 for finitely Borel is provable in ZFC + "there exists infinitely many Woodin cardinal", but not in ZFC + "there exists at least n Woodin cardinals", for any $n < \omega$.

Proof: The provability claims are from Lemma 0.13E.3. The unprovability claims follow from Lemma 0.13E.4 together with the reversal of the Σ^1_n determinacy, $n < \omega$, for any degree, and of the reversal of $L_{\omega+\omega}(\mathcal{R})$ determinacy for any degree. The reversals can be carried out without choice and over Z_2 , and weak extensions thereof (communication from W. Woodin). See [KW10]. QED

0.14. Incompleteness in ZFC using Discrete Structures.

0.14A. Preliminaries.

0.14B. Function Assignments.

0.14C. Boolean Relation Theory.

0.14D - 0.14J. NEW MATERIAL AS AGREED.

0.14A. Preliminaries.

The first arguably natural examples of incompleteness in ZFC using discrete structures appeared in [Fr98], and are discussed in section 0.14B.

The second examples of incompleteness in ZFC using discrete structures are from Boolean Relation Theory, which is the subject of this book. BRT represents a more natural and far more systematic approach than Function Assignments, with much greater points of contact with existing mathematical

contexts. In section 0.14C, we give a brief account of BRT, reserving the extended account for section 0.15.

The third examples of incompleteness in ZFC using discrete structures are the culmination of recent developments since 2009, culminating with announcements made in May, 2011. These take a different direction from BRT, but rely on many technical insights from BRT. They result in statements equivalent to the consistency of certain large cardinal hypotheses, and thus are equivalent to Π^0_1 sentences. In contrast, function assignments and BRT result in statements equivalent to the 1-consistency of large cardinals, and thus equivalent to Π^0_2 sentences.

These new developments are discussed in sections 0.14D - 0.14I. This is work in progress, and proofs will appear elsewhere.

There are two hierarchies of large cardinal hypotheses relevant to this section (except for 0.14G). The weaker of the two is the hierarchy of strongly n -Mahlo cardinals. These are defined inductively as follows.

The strongly 0-Mahlo cardinals are the strongly inaccessible cardinals (uncountable regular strong limit cardinals).

The strongly $n+1$ -Mahlo cardinals are the infinite cardinals all of whose closed unbounded subsets contain a strongly n -Mahlo cardinal.

We define $\text{SMAH}^+ = \text{ZFC} + (\forall n < \omega) (\exists \kappa) (\kappa \text{ is a strongly } n\text{-Mahlo cardinal})$. $\text{SMAH} = \text{ZFC} + \{(\exists \kappa) (\kappa \text{ is a strongly } n\text{-Mahlo cardinal})\}_n$.

Mahlo cardinals were introduced surprisingly early, in [Mah11], [Mah12], [Mah13]. For more information about the strongly Mahlo hierarchy, and the related Mahlo hierarchy, see section 4.1.

The second, stronger hierarchy of large cardinal hypotheses relevant to this section is the stationary Ramsey cardinal hierarchy. This hierarchy originated with [Ba75]. Also see [Fr01].

We say that λ has the k -SRP if and only if λ is a limit ordinal, $k \geq 1$, and every partition of the unordered k -tuples from λ into two pieces has a homogeneous stationary subset of λ .

We define $\text{SRP}^+ = \text{ZFC} + (\forall k < \omega) (\exists \kappa) (\kappa \text{ has the } k\text{-SRP})$. $\text{SRP} = \text{ZFC} + \{(\exists \kappa) (\kappa \text{ has the } k\text{-SRP})\}_k$.

The SRP hierarchy is intertwined with the more technical subtle cardinal hierarchy. See [Fr01] for a detailed treatment of this level of the large cardinal hierarchy.

0.14B. Function Assignments.

The first published examples of arguably mathematically natural arithmetic sentences independent of ZFC appeared in [Fr98]. These examples are Π_2^0 , although it was left open in [Fr98] whether they are provably equivalent to $1\text{-Con}(\text{SRP})$, as we expect.

A function assignment for a set X is a mapping U which assigns to each finite subset A of X , a unique function

$$U(A) : A \rightarrow A.$$

The following is easily obtained from Theorem 0.8F.4 (Theorem 0.4 in [Fr98]). See section 0.8F for the definition of regressive values.

THEOREM 0.14B.1. Let $k, p > 0$ and U be a function assignment for N^k . Then some $U(A)$ has $\leq (k^k)p$ regressive values on some $E^k \subseteq A$, $|E| = p$.

In the set theoretic world, we have the following analog (Theorem 0.5 in [Fr98]).

THEOREM 0.14B.2. Let $k, r, p > 0$ and $F : \lambda^k \rightarrow \lambda^r$, where λ is a suitably large cardinal. Then F has $\leq k^k$ regressive values on some $E^k \subseteq \lambda^k$, $|E| = p$. It suffices that λ has the k -SRP.

We placed a natural condition on function assignments for N^k so that we get the improved estimate k^k in Theorem 0.14B.2 rather than the $(k^k)p$ in Theorem 0.14B.1.

Let U be a function assignment for N^k . We say that U is #-decreasing if and only if for all finite $A \subseteq N^k$ and $x \in N^k$,

$$\text{either } U(A) \subseteq U(A \cup \{x\}) \text{ or there exists } |y| > |x| \text{ such that } |U(A)(y)| > |U(A \cup \{x\})(y)|.$$

Here we have used $| \cdot |$ for max.

An alternative definition of #-decreasing is as follows. For all finite $A \subseteq N^k$ and $x \in N^k$, either $U(A) \subseteq U(A \cup \{x\})$, or there exists $|y| > |x|$ such that

- i. $|U(A)(y)| > |U(A \cup \{x\})(y)|$.
- ii. for all $z \in A$, if $|z| < |y|$, then $U(A)(z) = U(A \cup \{x\})(z)$.
- iii. for all $z \in A$, if $|z| = |y|$, then $U(A)(z) = U(A \cup \{x\})(z)$ or $|U(A)(z)| > |U(A \cup \{x\})(z)|$.

The following infinitary proposition is Proposition A in [Fr98].

PROPOSITION 0.14B.3. Let $k, p > 0$ and U be a #-decreasing function assignment for N^k . Then some $U(A)$ has $\leq k^k$ regressive values on some $E^k \subseteq A$, $|E| = p$.

The finite form is Proposition B in [Fr98].

PROPOSITION 0.14B.4. Let $n \gg k, p > 0$ and U be a #-decreasing function assignment for $[n]^k$. Then some $U(A)$ has $\leq k^k$ regressive values on some $E^k \subseteq A$, $|E| = p$.

Proposition 0.14B.4 takes the form

for all k, p there exists n such that every gadget bounded
by n has an internal property

and is therefore explicitly Π^0_2 .

As remarked in [Fr98], p. 808, Proposition 0.14B.3 immediately implies Proposition 0.14B.4, using a standard compactness (finitely branching tree) argument. The implication from Proposition 0.14B.4 to Proposition 0.14B.3 is immediate. So clearly Proposition 0.14B.3 is provably equivalent to a Π^0_2 sentence, over RCA_0 .

The following is proved in [Fr98]. See Theorems 4.18, 5.91.

THEOREM 0.14B.5. SRP^+ proves Propositions 0.14B.3, 0.14B.4, but not from any consequence of SRP that is consistent with ZFC. Propositions 0.14B.3, 0.14B.4 imply $Con(SRP)$ over ZFC.

We conjecture that Propositions 0.14B.3, 0.14B.4 are provably equivalent to $1-Con(SRP)$ over ZFC.

In fact, we conjecture that Proposition 0.14B.3 is provably equivalent to 1-Con(SRP) over ACA', and Proposition 0.14B.4 is provably equivalent to 1-Con(SRP) over EFA.

0.14C. Boolean Relation Theory.

We give a brief account of some highlights of Boolean Relation Theory (BRT), the subject of this book. A much more detailed account will be given in section 0.15.

BRT begins with two theorems proved well within ZFC that provides an excellent point of departure.

Let N be the set of all nonnegative integers.

COMPLEMENTATION THEOREM. Let $f:N^k \rightarrow N$ obey the inequality $f(x) > \max(x)$. There exists a (unique) $A \subseteq N$ with $f[A^k] = N \setminus A$.

THIN SET THEOREM. Let $f:N^k \rightarrow N$. There exists an infinite $A \subseteq N$ such that $f[A^k] \neq N$.

These theorems are discussed in detail in sections 1.3 and 1.4.

Note that the Complementation Theorem (without uniqueness) has the following structure:

for every function of a certain kind there is a set of a certain kind such that a given Boolean equation holds involving the set and its image under the function.

The Thin Set Theorem has the following structure:

for every function of a certain kind there is a set of a certain kind such that a given Boolean inequation holds involving the set and its image under the function.

In fact, the inequation in the Thin Set Theorem involves only the image of the set under the function.

Here, and throughout BRT, we use a particular notion of the image of a set A under a multivariate function f - namely $f[A^k]$. For notational brevity, we suppress the arity of f , and simply write fA for $f[A^k]$. In all contexts under consideration, the arity, k , of f will be apparent.

In addition, here N serves as the universal set for the Boolean algebra.

More specifically, we use MF for the set of all f such that for some $k \geq 1$, $f: N^k \rightarrow N$. SD for the set of all $f \in MF$ such that for all $x \in \text{dom}(f)$, $f(x) > \max(x)$. INF for the set of all infinite $A \subseteq N$.

We can restate these two theorems in the form

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N \setminus A$.

THIN SET THEOREM. For all $f \in MF$ there exists $A \in INF$ such that $fA \neq N$.

The Complementation Theorem is an instance of what we call

$$EBRT \text{ in } A, fA \text{ on } (SD, INF).$$

The Thin Set Theorem is an instance of what we call

$$IBRT \text{ in } A, fA \text{ on } (MF, INF).$$

Here $EBRT$ means "equational BRT", and $IBRT$ means "inequational BRT".

For our independence results, we use a somewhat different class of functions. We let ELG be the set of all $f \in MF$ of expansive linear growth; i.e., where there exist rational constants $c, d > 1$ such that for all but finitely many $x \in \text{dom}(f)$,

$$c|x| \leq f(x) \leq d|x|$$

where $|x|$ is the maximum coordinate of the tuple x .

The core finding of this book is the discovery and analysis of a particular instance of

$$EBRT \text{ in } A, B, C, fA, fB, fC, gA, gB, gC \text{ on } (ELG, INF)$$

that is independent of ZFC. More specifically, we show that this "special instance" has the following three metamathematical properties:

i. It is provable in $SMAH^+$.

- ii. It is not provable from any set of consequences of SMAH that is consistent with ACA'.
- iii. It is provably equivalent to the 1-consistency of SMAH over ACA'.

In fact, the special instance is an instance of

EBRT in A, B, C, fA, fB, gB, gC on (ELG, INF) .

Although this special instance is far simpler than a randomly chosen instance, it does not convey any clear compelling information.

We were very anxious to establish the necessary use of large cardinals in order to analyze EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) .

CONJECTURE. Every instance of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) is provable or refutable in $SMAH^+$.

This conjecture would establish a necessary and sufficient use of large cardinals in BRT in light of the "special instance".

There are 2^{512} instances of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) , there being nine terms involved. This proved far too difficult to analyze, even using theoretical considerations.

There are 2^{64} instances of EBRT in A, C, fA, fB, gB, gC on (ELG, INF) , and the special instance referred to above comes under this smaller set.

CONJECTURE. Every instance of EBRT in A, C, fA, fB, gB, gC on (ELG, INF) is provable or refutable in $SMAH^+$.

Unfortunately, this conjecture also appears out of reach.

What was needed is a natural fragment of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ that is small enough to be completely analyzable, yet large enough to include our instance.

We discovered the following class of $3^8 = 6561$ instances of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) .

TEMPLATE. For all $f, g \in \text{ELG}$ there exist $A, B, C \in \text{INF}$ such that

$$\begin{aligned} X \cup. fY &\subseteq V \cup. gW \\ P \cup. fR &\subseteq S \cup. gT. \end{aligned}$$

Here X, Y, V, W, P, R, S, T are among the three letters A, B, C .

Here we have used $\cup.$ for disjoint union. I.e.,

$$\begin{aligned} D \cup. E &\text{ is } D \cup E \text{ if } D \cap E = \emptyset; \\ &\text{ undefined otherwise.} \end{aligned}$$

The special instance is called the Principal Exotic Case throughout the book. It appears as Proposition A in section 4.2.

PRINCIPAL EXOTIC CASE. For all $f, g \in \text{ELG}$ there exist $A, B, C \in \text{INF}$ such that

$$\begin{aligned} A \cup. fA &\subseteq C \cup. gB \\ A \cup. fB &\subseteq C \cup. gC. \end{aligned}$$

There are obviously 12 symmetric forms of the Principal Exotic Case obtained by permuting A, B, C , and switching the two clauses. These 12 are called the Exotic Cases. The remaining $6561 - 12 = 6549$ instances of the Template are shown to be provable or refutable in Chapter 3.

In section 4.2, we prove the Principal Exotic Case from SMAH^+ . In section 4.4, we sharpen this by proving the Exotic Case from $\text{ACA}' + 1\text{-Con}(\text{SMAH})$.

In Chapter 5, we derive $1\text{-Con}(\text{SMAH})$ from $\text{ACA}' +$ the Exotic Case. In section 5.9, we establish that the Principal Exotic Case (Proposition A) is not provable from any set of consequences of SMAH that is consistent with ACA' .

In section 3.15, we also consider the modified, weaker Template

TEMPLATE'. For all $f, g \in \text{ELG}$ there exist arbitrarily large finite $A, B, C \subseteq \mathbb{N}$ such that

$$\begin{aligned} X \cup. fY &\subseteq V \cup. gW \\ P \cup. fR &\subseteq S \cup. gT. \end{aligned}$$

In section 3.15, we show that every instance of Template' is provable or refutable in RCA_0 , and that Template and Template' are equivalent for all but the 12 Exotic Cases.

We also show that the 12 Exotic Cases become provable in RCA_0 under Template'.

We then draw the conclusion that the assertion

Template and Template' are equivalent

which we refer to as the BRT Transfer Principle, has the same metamathematical properties i-iii enumerated two pages earlier. In this sense, the above assertion represents a necessary use of large cardinals for obtaining arguably clear and compelling information in the realm of discrete mathematics.

0.14D - 0.14J. NEW MATERIAL GOES HERE AS AGREED.

0.15. Detailed Overview of Book Contents.

We give an informal discussion of the contents of the book, section by section. This discussion is far more detailed than the overview given in section 0.14C above.

Chapter 1 Introduction to BRT

1.1. General Formulation

Here we begin with two Theorems that lie at the heart of Boolean Relation Theory (abbreviated BRT). These are the Thin Set Theorem and the Complementation Theorem. We repeat these here.

THIN SET THEOREM. Let $k \geq 1$ and $f: N^k \rightarrow N$. There exists an infinite set $A \subseteq N$ such that $f[A^k] \neq N$.

COMPLEMENTATION THEOREM. Let $k \geq 1$ and $f: N^k \rightarrow N$. Suppose that for all $x \in N^k$, $f(x) > \max(x)$. There exists an infinite set $A \subseteq N$ such that $f[A^k] = N \setminus A$.

Note that the Thin Set Theorem asserts that for every function in a certain class there is a set in a certain class such that a Boolean inequation holds between the set and its forward image under the function. In fact, the Boolean inequation does not even use the set.

Similarly, the Complementation Theorem asserts that for every function in a certain class there is a set in a certain class such that a Boolean equation holds between the set and its forward image under the function.

The notion of forward image used throughout BRT is the set of values of the multivariate function at arguments drawn from the set. Throughout BRT, we abbreviate this construction, $f[A^k]$, by fA .

Thus we can rewrite the Thin Set Theorem and the Complementation Theorem in the following form.

THIN SET THEOREM. For all $f \in MF$ there exists $A \in INF$ such that $fA \neq N$.

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N \setminus A$.

We say that the Thin Set Theorem is an instance of IBRT (inequational BRT) on the BRT setting (MF, INF) , and the Complementation Theorem is an instance of EBRT (equational BRT) on the BRT setting (SD, INF) .

More specifically, we say that

- i. The Thin Set Theorem is an instance of: IBRT in fA on (MF, INF) .
- ii. The Complementation Theorem is an instance of: EBRT in A, fA on (SD, INF) .

We then present the general formulation. We define the following concepts, starting with Definition 1.1.4.

As an aid to the reader, we give examples of most of these concepts based on the Thin Set Theorem (TST), and the Complementation Theorem (CT).

1. BRT set variable, BRT function variable. For CT, TST we use A and f .
2. BRT term. For CT, we use $fA, U \setminus A$. For TST, we use fA, U .
3. BRT equation, BRT inequation, BRT inclusion. For CT, we use the BRT equation $fA = U \setminus A$. For TST, we use the BRT inequation $fA \neq U$.
4. BRT formula. These are quantifier free. For CT, we use $fA = U \setminus A$. For TST, we use $fA \neq U$.
5. Formal treatment of multivariate function, arity, and the forward imaging fE .

6. BRT setting. For CT we use (SD, INF) . For TST we use (MF, INF) .
7. BRT assertion. BRT, \subseteq assertion. For CT, we use $(\forall f \in V)(\exists A \in K)(fA = U \setminus A)$. For TST, we use $(\forall f \in V)(\exists A \in K)(fA \neq U)$.
8. BRT valid formula, BRT, \subseteq valid formula.
9. BRT equivalent formulas, BRT, \subseteq equivalent formulas.
10. BRT environments. For CT, we use EBRT. For TST, we use IBRT.
11. BRT signatures. For CT, we use A, fA . For TST, we use fA .
12. BRT fragment. For CT, we use EBRT in A, fA on (SD, INF) . For TST, we use IBRT in fA on (MF, INF) .
13. The standard BRT signatures. For CT and TST, we use A, fA .
14. Standard BRT fragments. For CT we use EBRT in A, fA on (SD, INF) . For TST we use IBRT in A, fA on (MF, INF) .

The highlight of the book is the proof of the Principal Exotic Case (see Appendix A) from large cardinals, and its unprovability from weaker large cardinals. The proof is in Chapter 4, and the unprovability is from Chapter 5.

The Principal Exotic Case arises in Chapter 3, and lies in the standard BRT fragment

$$EBRT \text{ in } A, B, C, fA, fB, fC, gA, gB, gC \text{ on } (ELG, INF).$$

Here ELG is the class of $f \in MF$ which are of expansive linear growth (see section 0.14C).

In fact, the Principal Exotic Case lives in the considerably reduced flat BRT fragment

$$EBRT \text{ in } A, C, fA, fB, gB, gC, \subseteq \text{ on } (ELG, INF)$$

since Proposition A is not affected by inserting $A \subseteq B \subseteq C$ in its conclusion (see Appendix A).

Even the above BRT fragment is too rich for us to completely analyze at this time, let alone the standard fragment above.

In Chapter 2, we do give a complete analysis of several much more restricted BRT fragments, as indicated by their section headings.

The main BRT settings considered in this book are (MF, INF) , (SD, INF) , and (ELG, INF) . See Definitions 1.1.2 and 2.1.

The state of the art with regard to complete analyses of BRT fragments on these BRT settings can be summarized as follows.

In both EBRT and IBRT, we completely understand one function and two sets with \subseteq , in the sense that RCA_0 suffices to prove or refute every instance. See sections 2.4 - 2.7.

However, it remains to analyze one function and two sets without the substantial simplifier \subseteq . This is a very substantial challenge, although we are convinced that this is a manageable project.

Only very special parts of the standard fragment EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) are presently amenable to complete analysis. One very symmetric part consisting of $3^8 = 6561$ cases is completely analyzed in Chapter 3. All instances are provable or refutable in RCA_0 - except for the Principal Exotic Case and its eleven symmetric forms, forming the twelve Exotic Cases.

Section 1.1 presents a very useful canonical form for any Boolean equation (arising in the BRT fragments analyzed in the book) as a finite conjunction of Boolean inclusions of certain forms. This greatly facilitates work with the general Boolean equations that arise.

For instance, see the 16 A, B, fA, fB pre elementary inclusions listed right after Lemma 2.4.5 according to Definition 1.1.35. Also see the 9 A, B, fA, fB, \subseteq elementary inclusions listed right after Lemma 2.4.5 according to Definition 1.1.37.

1.2. Some BRT settings

In this section, we give an indication of the tremendous variety of BRT settings that arise from standard mathematical considerations.

We conjecture that the behavior of BRT fragments in BRT settings depends very delicately on the choice of BRT setting. Generally speaking, we believe that even small changes in the BRT setting lead to different classifications, even with BRT fragments in modest signatures.

This leads us to the conviction that BRT is a mathematically fruitful problem generator of unprecedented magnitude and scope.

Indications of this sensitivity are already present in the classifications of Chapter 2 as well as the results of section 1.4.

Even in the realm of natural subsets of the set MF of all functions from some N^k into N , the variety of subclasses is staggering. These are discussed in part I of section 1.2. In addition, a large variety of subclasses of INF are also very natural.

It is very compelling to use \mathbf{z} , \mathbf{Q} , \mathfrak{R} , and \mathbf{C} , instead of N , creating many additional natural BRT settings, involving algebraic, topological, and analytic considerations.

The use of function spaces is also compelling. We mention (V,K) , where V is the set of all bounded linear operators on L^2 , and K is the set of all nontrivial closed subspaces of L^2 . Then the famous invariant subspace problem for L^2 is expressed as the following instance of EBRT in A, fA on (V,K) :

$$(\forall f \in V) (\exists A \in K) (fA = A).$$

We can obviously use other function spaces for BRT settings.

We also propose Topological BRT, where we use the continuous functions - and even the multivariate continuous functions - on various topological spaces, and the open subsets of the spaces.

It also makes sense to investigate those BRT statements that hold in the continuous functions and nonempty open sets, on all topological spaces obeying certain conditions.

Section 1.2 concludes with a back of the envelope calculation of the number of BRT settings presented there, that are suspected of having different BRT behavior. We count only those on N .

The estimate given there is 1,000,000 naturally described individual BRT settings with substantially different BRT behavior.

The book focuses on only five BRT settings (MF, INF) , (ELG, INF) , (SD, INF) , $(EVSD, INF)$, $(ELG \cap SD, INF)$, and only scratches the surface of very simple BRT fragments even in these settings. For the definition of all these settings in one place, see Appendix A. As indicated by the classifications in Chapter 2, incredible complexities are expected to always arise in passing from BRT fragments to even slightly richer BRT fragments - even on these five BRT settings. When considering the number 1,000,000 above, we see how vast and deep BRT is expected to be.

1.3. Complementation Theorems

This section focuses on aspects of the Complementation Theorem (CT). Recall the discussion at the beginning of section 1.1.

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N \setminus A$.

COMPLEMENTATION THEOREM (with uniqueness). For all $f \in SD$ there exists a unique $A \subseteq N$ with $fA = N \setminus A$. Moreover, $A \in INF$.

A few equivalent formulations of CT are given, as well as the simple inductive proof.

CT is then extended to strictly dominating functions on well founded relations. This extension is used in Chapter 4 to prove the Principal Exotic Case (Proposition A).

We also show that for irreflexive transitive relations with an upper bound condition, CT is equivalent to well foundedness.

In CT, we define the complementation of $f \in SD$ to be the unique $A \subseteq N$ with $fA = N \setminus A$.

There is the expectation that even for very simple $f \in SD$, the unique complementation A of f can be very complicated - and have an intricate structure well worth exploring.

We present some basic examples, where we calculate the unique complementation. In particular, we consider some cases where f is an affine transformation from N^k into N .

It is also very natural to consider affine $f: N^k \rightarrow Z$. Only here we need to use the following variant of CT. This requires use of the "upper image" of f on A , defined by

$$f \triangleleft A = \{f(x_1, \dots, x_k) : f(x_1, \dots, x_k) > \max(x_1, \dots, x_k) \text{ and } x_1, \dots, x_n \in A\}.$$

An upper complement of f is an $A \subseteq N$ with $f \triangleleft A = N \setminus A$.

UPPER COMPLEMENTATION THEOREM. Every $f: N^k \rightarrow Z$ has a unique upper complementation. This unique upper complement is infinite.

This formulation has the advantage that it applies to all $f: N^k \rightarrow Z$, without requiring that f obey any inequalities.

We then present some calculations of upper complementations.

We then view CT as a fixed point theorem, and present a more general BRT Fixed Point Theorem.

We also consider a version on the reals, and present a continuous complementation theorem.

The Complementation Theorem is closely related to an important development in digraph theory. These are the kernels and dominators of digraphs. Kernels are used in the recent work reported in section 0.14D.

1.4. Thin Set Theorems

This section focuses on aspects of the Thin Set Theorem (TST). Recall the discussion at the beginning of section 1.1.

THIN SET THEOREM. For all $f \in \text{MF}$ there exists $A \in \text{INF}$ such that $fA \neq \mathbb{N}$.

We begin by tracing the origins of the Thin Set Theorem back to the square bracket partition calculus in combinatorial set theory. There, one uses unordered tuples instead of ordered tuples. However, we give an equivalence proof in RCA_0 (see Theorem 1.4.2).

This is followed by a discussion of the metamathematical status of TST, which is only partially understood.

We then present a simple proof of TST using the infinite Ramsey theorem.

We give a strong form of TST where the codomain is $[0, \omega(k)]$, and establish its metamathematical status. We show that it is provably equivalent to ACA' over RCA_0 .

We briefly consider TST with an infinite cardinal κ instead of \mathbb{N} . We cite [To87], [BM90], and [Sh95] to obtain some results.

TST makes sense on any BRT setting. We explore TST on some BRT settings in real analysis.

We first consider 8 natural families of unary functions from \mathfrak{R} to \mathfrak{R} , and 9 families of subsets of \mathfrak{R} , for a total of 72 BRT settings.

$\text{FCN}(\mathfrak{R}, \mathfrak{R})$. All functions from \mathfrak{R} to \mathfrak{R} .

$\text{BFCN}(\mathfrak{R}, \mathfrak{R})$. All Borel functions from \mathfrak{R} to \mathfrak{R} .

$\text{CFCN}(\mathfrak{R}, \mathfrak{R})$. All continuous functions from \mathfrak{R} to \mathfrak{R} .

$\text{C}^1\text{FCN}(\mathfrak{R}, \mathfrak{R})$. All C^1 functions from \mathfrak{R} to \mathfrak{R} .

$\text{C}^\infty\text{FCN}(\mathfrak{R}, \mathfrak{R})$. All C^∞ functions from \mathfrak{R} to \mathfrak{R} .

$\text{RAFCN}(\mathfrak{R}, \mathfrak{R})$. All real analytic functions from \mathfrak{R} to \mathfrak{R} .

$\text{SAFCN}(\mathfrak{R}, \mathfrak{R})$. All semialgebraic functions from \mathfrak{R} to \mathfrak{R} .

$\text{CSAFCN}(\mathfrak{R}, \mathfrak{R})$. All continuous semialgebraic functions from \mathfrak{R} to \mathfrak{R} .

$\text{cSUB}(\mathfrak{R})$. All subsets of \mathfrak{R} of cardinality c .

$\text{UNCLSUB}(\mathfrak{R})$. All uncountable closed subsets of \mathfrak{R} .

$\text{NOPSUB}(\mathfrak{R})$. All nonempty open subsets of \mathfrak{R} .

$\text{UNOPSUB}(\mathfrak{R})$. All unbounded open subsets of \mathfrak{R} .

$\text{DEOPSUB}(\mathfrak{R})$. All open dense subsets of \mathfrak{R} .

$\text{FMOPESUB}(\mathfrak{R})$. All open subsets of \mathfrak{R} of full measure.

$\text{CCOPSUB}(\mathfrak{R})$. All open subsets of \mathfrak{R} whose complement is countable.

$\text{FCSUB}(\mathfrak{R})$. All subsets of \mathfrak{R} whose complement is finite.
 $\leq 1\text{CSUB}(\mathfrak{R})$. All subsets of \mathfrak{R} whose complement has at most one element.

We determine the status of TST in all 72 BRT settings.

We then consider the corresponding 8 families of multivariate functions from \mathfrak{R} to \mathfrak{R} . I.e., functions whose domain is some \mathfrak{R}^n and whose range is a subset of \mathfrak{R} . We use the same 9 families of subsets of \mathfrak{R} .

$\text{FCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate functions from \mathfrak{R} to \mathfrak{R} .
 $\text{BFCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate Borel functions from \mathfrak{R} to \mathfrak{R} .
 $\text{CFCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate continuous functions from \mathfrak{R} to \mathfrak{R} .
 $\text{C}^1\text{FCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate C^1 functions from \mathfrak{R} to \mathfrak{R} .
 $\text{C}^\infty\text{FCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate C^∞ functions from \mathfrak{R} to \mathfrak{R} .
 $\text{RAFCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate real analytic functions from \mathfrak{R} to \mathfrak{R} .
 $\text{SAFCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate semialgebraic functions from \mathfrak{R} to \mathfrak{R} .
 $\text{CSAFCN}(\mathfrak{R}^*, \mathfrak{R})$. All multivariate continuous semialgebraic functions from \mathfrak{R} to \mathfrak{R} .

We again determine the status of TST in all 72 BRT settings.

The status of TST in all 144 BRT settings is displayed in a table at the end of section 1.4.

Chapter 2 Classifications

2.1. Methodology

In Chapter 2, we focus on five BRT settings, falling naturally into three groups according to their observed BRT behavior.

$$\begin{aligned} &(\text{SD}, \text{INF}), (\text{ELG} \cap \text{SD}, \text{INF}). \\ &(\text{ELG}, \text{INF}), (\text{EVSD}, \text{INF}). \\ &(\text{MF}, \text{INF}). \end{aligned}$$

The inclusion diagram for these five sets of multivariate functions is

$$\begin{array}{c} \text{ELG} \cap \text{SD} \\ \text{SD} \text{ ELG} \\ \text{EVSD} \\ \text{MF} \end{array}$$

(SD, INF) , (ELG, INF) , and (MF, INF) are the most natural of these five BRT settings. The remaining two BRT settings are closely related to these three, and serve to round out the theory.

In section 2.1, we present the treelike methodology for giving complete classifications for BRT fragments.

This treelike methodology is used in sections 2.4, 2.5, and the reader can absorb this methodology by looking at the physical layout of the classifications in those sections.

The formal treatment of the treelike methodology is given fully in section 2.1.

2.2. EBRT, IBRT in A, fA

In this section, we give a complete classification of EBRT in A, fA , and IBRT in A, fA , on our list of five basic BRT settings, (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , $(EVSD, INF)$, (MF, INF) .

The EBRT classifications are conducted entirely within RCA_0 . The IBRT classifications are conducted entirely within ACA' .

This establishes that every instance of the EBRT fragments is provable or refutable in RCA_0 , and every instance of the IBRT fragments is provable or refutable in ACA' .

Since there are only 16 instances for each of these simple BRT fragments, we can afford to simply list all of the A, fA elementary inclusions

$$\begin{aligned} A \cap fA &= \emptyset. \\ A \cup fA &= U. \\ A &\subseteq fA. \\ fA &\subseteq A. \end{aligned}$$

and consider all of the 16 subsets, interpreted conjunctively. For EBRT in A, fA , if we reject a subset of the elementary inclusions, then we automatically reject any superset. So in order to save work, we can first list the subsets (A, fA formats) of cardinality 0, then list the subsets of cardinality 1, and so forth, through the subset of cardinality 4. But of course we don't have to list any subset where some proper subset has already been rejected.

This kind of classification is called a tabular classification. We give a tabular classification for EBRT in A, fA on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , $(EVSD, INF)$, (MF, INF) , and present the results in a table that lists all sixteen of the A, fA formats.

For IBRT in A, fA on (SD, INF) , we dualize, and thus put the assertions in the form

$$(\exists f \in V) (\forall A \in K) (\varphi)$$

where φ is an A, fA format interpreted conjunctively. Once again, if we reject a format, then we automatically reject any superset. So we also give a tabular classification of IBRT in A, fA on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , $(EVSD, INF)$, (MF, INF) . We also present the results in a table listing all sixteen of the A, fA formats.

In the course of working out the classification on the IBRT side, we came across the following sharpening of the Thin Set Theorem, which we derive from TST.

THIN SET THEOREM (variant). For all $f \in MF$ there exists $A \in INF$ such that $A \cup fA \neq N$.

We conclude section 2.2 with a discussion of the effect of restricting the arity of the functions in the various classes.

The EBRT classifications are conducted in RCA_0 , and the IBRT classifications are conducted in ACA' .

As a Corollary, all instances of EBRT in A, fA on these five BRT settings are provable or refutable in RCA_0 , and all instances of IBRT in A, fA on these five BRT settings are provable or refutable in ACA' .

In fact, ACA' is used only in IBRT in A, fA on the setting (MF, INF) , and not on the other four settings.

2.3. EBRT, IBRT in A, fA, fU

Here we redo section 2.2 for the signature A, fA, fU , with the same five BRT settings (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , $(EVSD, INF)$, (MF, INF) . Here U stands for the universal set, which in these five BRT settings, is N .

Now we have the 6 A, fA, fU elementary inclusions

$$\begin{aligned} A \cap fA &= \emptyset. \\ A \cup fU &= U. \\ A &\subseteq fU. \\ fU &\subseteq A \cup fA. \\ A \cap fU &\subseteq fA. \\ fA &\subseteq A. \end{aligned}$$

There are 64 subsets of these 6 elementary inclusions. These are conveniently handled again by tabular classifications for both EBRT and IBRT.

Some interesting issues arise using N and fN , as presented in Theorems 2.3.2 and 2.3.3. We also examine the effect of arity on the class of functions, as in section 2.2.

As in section 2.2, the EBRT classifications are conducted in RCA_0 , and the IBRT classifications are conducted in ACA' .

As a Corollary, all instances of EBRT in A, fA, fU on these five BRT settings are provable or refutable in RCA_0 , and all instances of IBRT in A, fA, fU on these five BRT settings are provable or refutable in ACA' .

In fact, ACA' is used only in IBRT in A, fA, fU on (MF, INF) , and not on the other four settings.

- 2.4. EBRT in A, B, fA, fB, \subseteq on (SD, INF)
- 2.5. EBRT in A, B, fA, fB, \subseteq on (ELG, INF)

Here we use the treelike classification method in order to give complete classifications of EBRT in A, B, fA, fB, \subseteq on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , and $(EVSD, INF)$. EBRT on (MF, INF) is treated in section 2.6.

The classifications in sections 2.4, 2.5 are conducted in RCA_0 . As a Corollary, all instances of these four BRT fragments are provable or refutable in RCA_0 .

A substantial number of new issues arise in both of these classifications. The new issues can be seen from Lemmas 2.4.1 - 2.4.5, 2.5.1 - 2.5.14.

Both treelike classifications start with a listing of the 9 elementary inclusions in A, B, fA, fB, \subseteq .

$$A \cap fA = \emptyset.$$

$B \cup fB = N.$
 $B \subseteq A \cup fB.$
 $fB \subseteq B \cup fA.$
 $A \subseteq fB.$
 $B \cap fB \subseteq A \cup fA.$
 $fA \subseteq B.$
 $A \cap fB \subseteq fA.$
 $B \cap fA \subseteq A.$

Recall that the elementary inclusions originate from the 16 pre elementary inclusions through formal simplification using $A \subseteq B$.

The classifications provide a determination of the subsets S of the above nine inclusions for which

$(\forall f \in SD) (\exists A \subseteq B \text{ from INF}) (S)$
 $(\forall f \in ELG \cap SD) (\exists A \subseteq B \text{ from INF}) (S)$
 $(\forall f \in ELG) (\exists A \subseteq B \text{ from INF}) (S)$
 $(\forall f \in EVSD) (\exists A \subseteq B \text{ from INF}) (S)$

holds, where S is interpreted conjunctively.

We believe that obtaining complete classifications of EBRT in A, B, fA, fB on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , and $(EVSD, INF)$ is a manageable project, and can be completed within five years. The pre elementary inclusions in A, B, fA, fB number 16.

There needs to be a determination of the sets S of these sixteen inclusions for which

$(\forall f \in SD) (\exists A \subseteq B \text{ from INF}) (S)$
 $(\forall f \in ELG \cap SD) (\exists A \subseteq B \text{ from INF}) (S)$
 $(\forall f \in ELG) (\exists A \subseteq B \text{ from INF}) (S)$
 $(\forall f \in EVSD) (\exists A \subseteq B \text{ from INF}) (S)$

holds, where S is interpreted conjunctively.

The classifications are carried out entirely within RCA_0 . Hence every instance of these classifications is provable or refutable in RCA_0 .

2.6. EBRT in $A_1, \dots, A_k, fA_1, \dots, fA_k, \subseteq$ on (MF, INF)

Classifications in EBRT on (MF, INF) are substantially easier than on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , and $(EVSD, INF)$, at least under \subseteq . Here we handle one function

and k sets under \subseteq on (MF, INF) . Again, the classification is conducted in RCA_0 , and so we see that every instance of this BRT fragment is provable or refutable in RCA_0 .

We begin with a listing of the fifteen convenient types of elementary inclusions based on simple inequalities on the subscripts. Five of these are easily eliminated, leaving a sublist of ten. The conjunction of all of these is accepted.

Without \subseteq , we have an incomparably more difficult challenge, which we have not attempted.

2.7. IBRT in $A_1, \dots, A_k, fA_1, \dots, fA_k, \subseteq$

In this section, we give a complete classification of IBRT in $A_1, \dots, A_k, fA_1, \dots, fA_k, \subseteq$ on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , $(EVSD, INF)$, and (MF, INF) . We work entirely within RCA_0 , except for the BRT setting (MF, INF) , where we work within ACA' .

In fact, this classification for the first four of these BRT settings is seen to be trivial, and so section 2.7 focuses on the BRT setting (MF, INF) .

We start with the $A_1, \dots, A_k, fA_1, \dots, fA_k, \subseteq$ elementary inclusions, grouped into the same 15 categories based on simple inequalities of the subscripts that were used in section 2.6.

For each of these elementary inclusions, ρ , we will provide a useful description of the witness set for ρ , in the following sense: The set of all $f \in MF$ such that

$$(\forall A_1, \dots, A_k \in INF) (A_1 \subseteq \dots \subseteq A_k \rightarrow \rho).$$

We then calculate the witness sets for the sets of elementary inclusions by taking intersections.

It is easily seen that a format is correct if and only if this intersection is nonempty. Correctness of formats correspond to Boolean inequations. See item 4) just before Definition 1.1.40, with $n = 1$.

We completely determine the formats (sets of elementary inclusions) for which the intersection is nonempty.

Once again, without \subseteq , we have an incomparably more difficult challenge, which we have not attempted.

Chapter 3 6561 Cases of Equational Boolean Relation Theory
3.1. Preliminaries

Recall that EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) involves $2^9 = 512$ pre elementary inclusions, with 2^{512} statements. A complete classification is well beyond our capabilities. This is also true for EBRT in $A, B, C, fA, fB, fC, gA, gB, gC, \subseteq$ on (ELG, INF) , although the number of elementary inclusions reduces to 64, with 2^{64} statements.

Here we completely classify a modest, but significant, part of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) .

We use the notation $A \cup. B$ from Definition 1.3.1. In particular,

$$A \cup. B \subseteq C \cup. D$$

means

$$A \cap B = \emptyset \wedge C \cap D = \emptyset \wedge A \cup B \subseteq C \cup D.$$

This is a very natural concept, and is illustrated by a diagram in section 3.1.

The part of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) treated here is given as follows.

TEMPLATE. For all $f, g \in ELG$ there exist $A, B, C \in INF$ such that

$$\begin{aligned} X \cup. fY &\subseteq V \cup. gW \\ P \cup. fR &\subseteq S \cup. gT. \end{aligned}$$

Here X, Y, V, W, P, R, S, T are among the three letters A, B, C . We refer to the statements $X \cup. fY \subseteq V \cup. gW$, for $X, Y, V, W \in \{A, B, C\}$, as clauses.

In Chapter 3, we determine the truth values of all of these 6561 statements. We also read off a number of specific results about the Template. We do not know how to obtain these results without examining the classification.

In particular, every assertion in the Template is either provable or refutable in $SMAH^+$. In fact, there exist 12 assertions in the Template, which are obtained by permuting

A, B, C and interchanging the two clauses, so that the remaining 6549 assertions are each provable or refutable in RCA_0 .

These 12 exceptional cases are called the Exotic Cases. The Principal Exotic Case is as follows.

PROPOSITION A. For all $f, g \in ELG$ there exist $A, B, C \in INF$ such that

$$\begin{aligned} A \cup. fA &\subseteq C \cup. gB \\ A \cup. fB &\subseteq C \cup. gC. \end{aligned}$$

In Chapter 4, we prove Proposition A in $SMAH^+$. In Chapter 5, we show that Proposition A is provably equivalent to $1-Con(SMAH)$ over ACA' .

We also show that every one of the 6561 assertions in the Template, other than the 12 Exotic Cases, are provably equivalent to the result of replacing ELG by any of $ELG \cap SD$, SD , $EVSD$. All 12 Exotic Cases are refutable in RCA_0 if ELG is replaced by SD or $EVSD$ (Theorem 6.3.5).

The 6561 cases are organized into 10 manageable groups according to the inner trace (quadruple) of letters used. I.e., the Principal Exotic Case above (Proposition A) has inner quadruple $ACBC$.

Lemma 3.1.6 establishes that we need only consider single clauses, of which there are 14 up to symmetry - and these ten inner traces:

1. AAAA. 20 up to symmetry.
2. AAAB. 81. No symmetries.
3. AABA. 81. No symmetries.
4. AABB. 45 up to symmetry.
5. AABC. 81. No symmetries.
6. ABAB. 36 up to symmetry.
7. ABAC. 45 up to symmetry.
8. ABBA. 45 up to symmetry.
9. ABBC. 81. No symmetries.
10. ACBC. 45 up to symmetry.

This adds up to a total of 574 ordered pairs up to equivalence (including the 14 duplicates or single clauses).

3.2. Some Useful Lemmas

In this section, five useful lemmas are established that are used extensively throughout Chapter 3.

The first of these lemmas provides $f \in \text{ELG} \cap \text{SD}$ such that whenever A is nonempty and $fA \cap 2N \subseteq A$, we have fA is cofinite. This is useful for refuting instances of the Template, since if fA is cofinite then all instances of the Template in which fA appears must be false.

The second and fourth lemmas are variants of the first, also providing $g \in \text{ELG} \cap \text{SD}$ such that if g feeds any nontrivial A back into A , the gA is cofinite.

The third lemma decomposes any $f \in \text{ELG} \cap \text{SD}$ into a suitable composition of functions in $\text{ELG} \cap \text{SD}$. It is used to prove the fourth lemma.

The fifth lemma says that if we have finitely many terms in a set variable $A \subseteq N$, built out of functions from EVSD , then we can find $A \in \text{INF}$ which is disjoint from all of them. This is particularly straightforward.

3.3. Single Clauses (duplicates).

- 3.4. AAAA.
- 3.5. AAAB.
- 3.6. AABA.
- 3.7. AABB.
- 3.8. AABC.
- 3.9. ABAB.
- 3.10. ABAC.
- 3.11. ABBA.
- 3.12. ABBC.
- 3.13. ACBC.

In each section, every instance of the Template covered under the titles are either proved or refuted in RCA_0 , with one exception. That exception is in section 3.13, and is the Principal Exotic Case (Proposition A). The Principal Exotic Case is treated in Chapters 4,5.

3.14. Annotated Table

Here we present a table of all of the results in sections 3.3 - 3.13.

The Template is based on INF . In sections 3.3 - 3.13, we also treat four alternatives to INF .

AL is "arbitrarily large", which includes infinite.

ALF is "arbitrarily large finite", which does not include infinite.

FIN is "finite".

NON is "nonempty".

The Annotated Table has 584 entries, each treating the five attributes INF, AL, ALF, FIN, NON. Every one of the 6561 instances is symmetric - and therefore trivially equivalent - to one of the 584.

Thus the Annotated Table lists a total of $574 \times 5 = 2870$ determinations.

3.15 Some Observations

In this final section of Chapter 3, we read off some striking information from examination of the Annotated Table from section 3.14.

The following asserts that ALF and INF come out the same in the Template.

BRT TRANSFER. Let X, Y, V, W, P, R, S, T be among the letters A, B, C . The following are equivalent.

- i. for all $f, g \in \text{ELG}$ and $n \geq 1$, there exist finite $A, B, C \subseteq N$, each with at least n elements, such that $X \cup. fY \subseteq V \cup. gW, P \cup. fR \subseteq S \cup. gT$.
- ii. for all $f, g \in \text{ELG}$, there exist infinite $A, B, C \subseteq N$, such that $X \cup. fY \subseteq V \cup. gW, P \cup. fR \subseteq S \cup. gT$.

Of course, BRT Transfer has, as a consequence, the Principal Exotic Case (Proposition A). In fact, it is clearly provably equivalent to the Principal Exotic Case over RCA_0 .

BRT Transfer provides a way of stating a result in BRT for which it is necessary and sufficient to use large cardinals to prove, without having to give any particular BRT instance.

Chapter 4 Proof of Principal Exotic Case

4.1. Strongly Mahlo Cardinals of Finite Order

In this section, we introduce the large cardinals used to prove the Principal Exotic Case. These are the strongly Mahlo cardinals of finite order.

The relevant large cardinal combinatorics is developed in a self contained way using Erdős-Rado trees.

This large cardinal combinatorics first appeared in [Sc74]. We follow the treatment given in [HKS87].

We use SMAH^+ for $\text{ZFC} + (\forall n < \omega) (\exists \kappa) (\kappa \text{ is an } n\text{-Mahlo cardinal})$. We use SMAH for $\text{ZFC} + \{(\exists \kappa) (\kappa \text{ is a strongly } n\text{-Mahlo cardinal})\}_{n < \omega}$.

The large cardinal combinatorics used in the book is given by the following. We give a self contained proof.

LEMMA 4.1.6. Let $n, m \geq 1$, κ a strongly n -Mahlo cardinal, and $A \subseteq \kappa$ unbounded. For all $i \in \omega$, let $f_i: A^{n+1} \rightarrow \kappa$, and let $g_i: A^m \rightarrow \omega$. There exists $E \subseteq \kappa$ of order type ω such that
 i) for all $i \geq 1$, $f_i E$ is either a finite subset of $\text{sup}(E)$, or of order type ω with the same sup as E ;
 ii) for all $i \in \omega$, $g_i E$ is finite.

4.2. Proof using Strongly Mahlo Cardinals

In this section, we prove the Principal Exotic Case (Proposition A) in SMAH^+ . We actually prove the following sharp form of Proposition B.

PROPOSITION B. Let $f, g \in \text{ELG}$ and $n \geq 1$. There exist infinite sets $A_1 \subseteq \dots \subseteq A_n \subseteq \mathbb{N}$ such that
 i) for all $1 \leq i < n$, $f A_i \subseteq A_{i+1} \cup g A_{i+1}$;
 ii) $A_1 \cap f A_n = \emptyset$.

We start with $f, g \in \text{ELG}$ and $n \geq 1$, with a cardinal κ that is strongly Mahlo of sufficiently high finite order.

We begin with the discrete linearly ordered semigroup with extra structure, $M = (\mathbb{N}, <, 0, 1, +, f, g)$.

We first extend this structure to a countable structure

$$M^* = (\mathbb{N}^*, <^*, 0^*, 1^*, +^*, f^*, g^*, c_0^*, \dots)$$

generated by the atomic indiscernibles c_i^* , $i \in \mathbb{N}$. This construction uses the infinite Ramsey theorem, infinitely iterated.

After verifying a number of properties of M^* , we then extend transfinitely to

$$M^{**} = (N^{**}, <^{**}, 0^{**}, 1^{**}, +^{**}, f^{**}, g^{**}, c_0^{**}, \dots, c_\alpha^{**}, \dots)$$

where the c^{**} 's are indexed by the large cardinal κ . In particular, we verify that any partial substructure of M^{**} boundedly generated by 0^{**} , 1^{**} , and a set of c^{**} 's of order type ω , is embeddable back into M^* and M .

We then apply then Complementation Theorem for well founded relations (Theorem 1.3.1) to obtain a unique set W of nonstandard elements of M^{**} such that for all nonstandard x in M^{**} ,

$$x \in W \leftrightarrow x \notin g^{**}W.$$

We then build a Skolem hull construction of length ω consisting entirely of elements of W . The construction starts with the set of all c^{**} 's. Witnesses are thrown in from W that verify that values of f^{**} at elements thrown in at previous stages do not lie in W (provided they in fact do not lie in W). Only the first n stages of the construction will be used.

Every element of the n -th stage of the Skolem hull construction has a suitable name involving a bounded number of the c^{**} 's.

At this crucial point, we then apply Lemma 4.1.6 to the large cardinal κ , in order to obtain a suitably indiscernible subset of the c^{**} 's of order type ω , with respect to this naming system.

We can redo the length n Skolem hull construction starting with S . This is just a restriction of the original Skolem hull construction that started with all of the c^{**} 's.

Because of the indiscernibility, we generate a subset of N^{**} whose elements are given by terms of bounded length in c^{**} 's of order type ω . This forms a suitable partial substructure of M^{**} , so that it is embeddable back into M . The image of this embedding on the n stages of the Skolem hull construction will comprise the $A_1 \subseteq \dots \subseteq A_n$ satisfying the conclusion of Proposition B.

This completes the proof of Proposition B in SMAH^+ .

4.3. Some Existential Sentences

The proof of the Principal Exotic Case in section 4.2 from SMAH⁺ is not optimal. Proposition B can, in fact, be proved in ACA' + 1-Con(SMAH). This is more delicate, and is proved in section 4.4. Section 4.3 provides a crucial Lemma for that proof.

The Lemma needed is Theorem 4.3.8, which gives a primitive recursive algorithm for determining the truth value of all sentences of the first form

$$\begin{aligned} & (\exists \text{ infinite } B_1, \dots, B_n \subseteq \mathbb{N}^k) \\ & (\forall i \in \{1, \dots, n-1\}) (\forall x_1, \dots, x_m \in B_i) \\ & (\exists y_1, \dots, y_m \in B_{i+1}) (R_i(x_1, \dots, x_m, y_1, \dots, y_m)) \end{aligned}$$

where $k, n, m \geq 1$, and $R_1, \dots, R_{n-1} \subseteq \mathbb{N}^{2km}$ are order invariant relations. Recall that order invariant sets of tuples are sets of tuples where membership depends only on the order type of a tuple. Furthermore, it is provable in ACA' that this algorithm is correct.

We start with the simpler set of sentences of the second form

$$\begin{aligned} & (\exists \text{ infinite } B_1, \dots, B_n \subseteq \mathbb{N}^k) \\ & (\forall i \in \{1, \dots, n-1\}) \\ & (\forall x, y, z \in B_i) (\exists w \in B_{i+1}) (R_i(x, y, z, w)) \end{aligned}$$

where $k, n \geq 1$, and $R_1, \dots, R_{n-1} \subseteq \mathbb{N}^{4k}$ are order invariant relations. We primitive recursively convert every sentence of the first form to a corresponding sentence of the second form, without changing the truth value.

We then consider sentences of the third form

$$(\exists f: \mathbb{N}^p \rightarrow \mathbb{N}) (\forall x_1, \dots, x_q \in \mathbb{N}) (\varphi)$$

where φ is a propositional combination of atomic formulas of the forms $x_i < x_j$, $f(y_1, \dots, y_p) < f(z_1, \dots, z_p)$, where $x_i, x_j, y_1, \dots, y_p, z_1, \dots, z_p$ are among the (distinct) variables x_1, \dots, x_q . We primitive recursively convert every sentence of the second form to a corresponding sentence of the third form, without changing the truth value.

Sentences of the third form are analyzed using strong SOI's. It is shown that a sentence of the third form is

true if and only if there is a small finite set of strong SOI's of a certain kind associated with the sentence.

4.4. Proof using 1-consistency

In this section we show that Proposition B - and hence the Principal Exotic Case - can be proved in $ACA' + 1-Con(SMAH)$.

We first restate what is proved in section 4.2 in a different form with numerical parameters.

Recall that in section 4.2, we essentially proved in SMAH that for any suitable structure

$$M^* = (N^*, 0^*, 1^*, <^*, +^*, f^*, g^*, c_0^*, \dots)$$

there exist $r \geq 1$ and infinite sets $D[1] \subseteq \dots \subseteq D[n] \subseteq M^*[r]$ such that $D[1] \subseteq \{c_j^* : j \geq 0\}$, and for all $1 \leq i < n$, $f^*D[i] \subseteq D[i+1] \cup g^*D[i+1]$. Here we assume that $n \geq 1$ and the arities p, q of f^*, g^* , and a bound b on the ELG inequalities, are given in advance. See Lemma 4.4.1.

Since for fixed parameters n, p, q, b , the set of such M^* forms a compact space in an appropriate sense, we can choose r so large that it works even if the c^* s are only indiscernible with respect to atomic formulas of bounded complexity.

So these considerations allow us formulate an assertion of the form $(\forall n)(\exists m)(\sigma(n, m))$ that implies Proposition B, where for each n , $(\exists m)(\sigma(n, m))$ is provable in SMAH.

Note that if $\sigma(n, m)$ were a primitive recursive equation, then $(\forall n)(\exists m)(\sigma(n, m))$ would be provable in $ACA' + 1-Con(SMAH)$, and so would Proposition B, as required.

However, $\sigma(n, m)$ asserts the existence of a chain of infinite sets of length n satisfying some inclusion relations.

Now Theorem 4.3.8 comes to the rescue, telling us that $\sigma(n, m)$ can be put in primitive recursive form.

Chapter 5 is devoted to a proof of 1-Con(SMAH) in ACA' + the Principal Exotic Case.

In fact, we use a specialization of the Principal Exotic Case, to a subset of ELG.

This subset is $ELG \cap SD \cap BAF$, where BAF is the countable set of functions given by terms in $0, 1, +, -, \cdot, \uparrow, \log$. Here (see Definition 5.1.1),

1. Addition. $x+y$ is the usual addition.
2. Subtraction. Since we are in \mathbb{N} , $x-y$ is defined by the usual $x-y$ if $x \geq y$; 0 otherwise.
3. Multiplication. $x \cdot y$ is the usual multiplication.
4. Base 2 exponentiation. $x \uparrow$ is the usual base 2 exponentiation.
5. Base 2 logarithm. Since we are in \mathbb{N} , $\log(x)$ is the floor of the usual base 2 logarithm, with $\log(0) = 0$.

It is easier to work with EBAF (extended basic functions), defined in Definition 5.1.7. By Theorem 5.1.4, EBAF = BAF.

In Chapter 5, we give a proof of 1-Con(SMAH) in ACA' + Proposition C.

PROPOSITION C. For all $f, g \in ELG \cap SD \cap BAF$, there exist $A, B, C \in INF$ such that

$$\begin{aligned} A \cup fA &\subseteq C \cup gB \\ A \cup fB &\subseteq C \cup gC. \end{aligned}$$

Throughout Chapter 5, we assume Proposition C.

Note that Proposition C does not tell us that $A \subseteq B \subseteq C$. This is a very important condition to have, as we want to extend length 3 chains to chains of arbitrary finite length, and then apply compactness to get a single structure.

So in section 5.1, we obtain the badly needed chain of length 3 - but at the cost of degrading the two clauses in Proposition C. The tradeoff is well worth it - and needed.

Section 5.1 concludes with the following.

LEMMA 5.1.7. Let $f, g \in ELG \cap SD \cap BAF$ and $\text{rng}(g) \subseteq 6\mathbb{N}$.

There exist infinite $A \subseteq B \subseteq C \subseteq \mathbb{N} \setminus \{0\}$ such that

- i) $fA \cap 6\mathbb{N} \subseteq B \cup gB$;
- ii) $fB \cap 6\mathbb{N} \subseteq C \cup gC$;

- iii) $fA \cap 2N+1 \subseteq B$;
- iv) $fA \cap 3N+1 \subseteq B$;
- v) $fB \cap 2N+1 \subseteq C$;
- vi) $fB \cap 3N+1 \subseteq C$;
- vii) $C \cap gC = \emptyset$;
- viii) $A \cap fB = \emptyset$.

The remaining sections in Chapter 5 use only the last Lemma from the previous section, together with the previous definitions.

5.2. From length 3 towers to length n towers

In this section, we obtain a variant of Lemma 5.1.7 (Lemma 5.2.12) involving length n towers rather than length 3 towers.

However, we have to pay a serious cost. As opposed to Lemma 5.1.7, we will only have that the sets in the length n towers have at least r elements, for any given $r \geq 1$.

So it is important to make sure that the first sets in these towers be a suitable set of indiscernibles before we relinquish that the first sets be infinite.

In order to accomplish this, we first apply the infinite Ramsey theorem to shrink the infinite first sets coming from Lemma 5.1.7 to infinite subsets that are sets of indiscernibles of the right kind.

Section 5.2 concludes with the following.

LEMMA 5.2.12. Let $r \geq 3$ and $g \in \text{ELG} \cap \text{SD} \cap \text{BAF}$, where $\text{rng}(g) \subseteq 48N$. There exists (D_1, \dots, D_r) such that

- i) $D_1 \subseteq \dots \subseteq D_r \subseteq N \setminus \{0\}$;
- ii) $|D_1| = r$ and D_r is finite;
- iii) for all $x < y$ from D_1 , $x \uparrow < y$;
- iv) for all $1 \leq i \leq r-1$, $48\alpha(r, D_i; 1, r) \subseteq D_{i+1} \cup gD_{i+1}$;
- v) for all $1 \leq i \leq r-1$, $2\alpha(r, D_i; 1, r)+1, 3\alpha(r, D_i; 1, r)+1 \subseteq D_{i+1}$;
- vi) $D_r \cap gD_r = \emptyset$;
- vii) $D_1 \cap \alpha(r, D_2; 2, r) = \emptyset$;
- viii) Let $1 \leq i \leq \beta(2r)$, $x_1, \dots, x_{2r} \in D_1$, $y_1, \dots, y_r \in \alpha(r, D_2)$, where (x_1, \dots, x_r) and (x_{r+1}, \dots, x_{2r}) have the same order type and \min , and $y_1, \dots, y_r \leq \min(x_1, \dots, x_r)$. Then $t[i, 2r](x_1, \dots, x_r, y_1, \dots, y_r) \in D_3 \leftrightarrow t[i, 2r](x_{r+1}, \dots, x_{2r}, y_1, \dots, y_r) \in D_3$.

Note the partial shift toward the language driven notions using α . These are carefully defined sets of nonnegative integers given by terms with arguments from sets. Also, note the use of $t[i,2r]$.

5.3. Countable nonstandard models with limited indiscernibles

Our basic standard structure is $(\mathbb{N}, <, 0, 1, +, -, \cdot, \uparrow, \log)$ that provides the operations that generate BAF (see section 5.1).

We use Lemma 5.2.12 to create, for each $r \geq 3$, a structure $(\mathbb{N}, <, 0, 1, +, -, \cdot, \uparrow, \log, E_1, \dots, E_r)$ with a related set of properties. This is Lemma 5.3.2, which frees us from any further consideration of BAF. Thus we no longer see the $D \cup gD$ construction, or the $D \cap gD = \emptyset$ condition. See Lemma 5.3.2.

The next major step is to consolidate all of the structures given by Lemma 5.3.2 relative to each $r \geq 3$, to a single countable nonstandard structure based on a single tower $E_1 \subseteq E_2 \subseteq \dots$ of infinite sets of infinite length. Lemma 5.3.3 also has further simplifications.

One important point is the condition that the resulting single structure M is both a nonstandard model of some arithmetic - with primitives $0, 1, +, -, \cdot, \uparrow, \log$ - and also has the crucial tower of subsets $E_1 \subseteq E_2 \subseteq \dots$, acting like unary predicates. The arithmetic is simply the set of all true Π_1^0 sentences. This is important for obtaining $1\text{-Con}(\text{SMAH})$, instead of just $\text{Con}(\text{SMAH})$.

A second point is that the elements of the tower are cofinal in the structure.

This consolidation into a single structure is obtained by two steps. The first step is the compactness argument, which arranges for all of the properties except that the E 's are cofinal in the structure. The second step is to restrict this structure to the cut given by a subset of the first set in the tower that has order type ω . In fact, this subset of order type ω is just the interpretation of infinitely many constant symbols used in the compactness argument.

There is a considerable development of properties of M . One important development is internal finite sequence coding.

Because of the role of expansive linear growth - traces of which are carried through for several sections - we need the rather delicate way of handling coding provided by Definition 5.3.11.

Section 5.3 ends with the following.

LEMMA 5.3.18. There exists a countable structure $M = (A, <, 0, 1, +, -, \cdot, \uparrow, \log, E, c_1, c_2, \dots)$ such that the following holds.

- i) $(A, <, 0, 1, +, -, \cdot, \uparrow, \log)$ satisfies $TR(\Pi_1^0, L)$;
- ii) $E \subseteq A \setminus \{0\}$;
- iii) The c_n , $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E \setminus \alpha(E; 2, < \infty)$ with no upper bound in A ;
- iv) Let $r, n \geq 1$, $t(v_1, \dots, v_r)$ be a term of L , and $x_1, \dots, x_r \leq c_n$. Then $t(x_1, \dots, x_r) < c_{n+1}$;
- v) $2\alpha(E; 1, < \infty) + 1, 3\alpha(E; 1, < \infty) + 1 \subseteq E$;
- vi) Let $r \geq 1$, $a, b \in \mathbb{N}$, and $\varphi(v_1, \dots, v_r)$ be a quantifier free formula of L . There exist $d, e, f, g \in \mathbb{N} \setminus \{0\}$ such that for all $x_1 \in \alpha(E; 1, < \infty)$, $(\exists x_2, \dots, x_r \in E) (x_2, \dots, x_r \leq ax_1 + b \wedge \varphi(x_1, \dots, x_r)) \leftrightarrow dx_1 + e \notin E \leftrightarrow fx_1 + g \in E$;
- vii) Let $r \geq 1$, $p \geq 2$, and $\varphi(v_1, \dots, v_{2r})$ be a quantifier free formula of L . There exist $a, b, d, e \in \mathbb{N} \setminus \{0\}$ such that the following holds. Let $n \geq 1$ and $x_1, \dots, x_r \in \alpha(E; 1, < \infty) \cap [0, c_n]$. Then $(\exists y_1, \dots, y_r \in E) (y_1, \dots, y_r \leq \uparrow p(|x_1, \dots, x_r|) \wedge \varphi(x_1, \dots, x_r, y_1, \dots, y_r)) \leftrightarrow a \text{CODE}(c_{n+1}; x_1, \dots, x_r) + b \notin E \leftrightarrow d \text{CODE}(c_{n+1}; x_1, \dots, x_r) + e \in E$. Here CODE is as defined just before Lemma 5.3.11;
- viii) Let $k, n, m \geq 1$, and $x_1, \dots, x_k \leq c_n < c_m$, where $x_1, \dots, x_k \in \alpha(E; 1, < \infty)$. Then $\text{CODE}(c_m; x_1, \dots, x_k) \in E$;
- ix) Let $r \geq 1$ and $t(v_1, \dots, v_{2r})$ be a term of L . Let $i_1, \dots, i_{2r} \geq 1$ and $y_1, \dots, y_r \in E$, where (i_1, \dots, i_r) and (i_{r+1}, \dots, i_{2r}) have the same order type and \min , and $y_1, \dots, y_r \leq \min(c_{i_1}, \dots, c_{i_r})$. Then $t(c_{i_1}, \dots, c_{i_r}, y_1, \dots, y_r) \in E \leftrightarrow t(c_{i_{r+1}}, \dots, c_{i_{2r}}, y_1, \dots, y_r) \in E$.

Note that the infinite tower of sets from the M of Lemma 5.3.3 is removed in favor of a single subset E , and constants c_n , $n \geq 1$, enumerating the first term of the tower. The single set E is simply the union of the tower of E 's from the M of Lemma 5.3.3. The E is cofinal in the structure.

5.4. Limited formulas, limited indiscernibles,

x-definability, normal form

Note that the M of Lemma 5.3.18 obeys two special forms of existential comprehension (clauses vi, vii), and one form of quantifier free indiscernibility (clause ix).

We upgrade these to a single form of comprehension for formulas with bounded quantifiers, and indiscernibility for formulas with bounded quantifiers. The range of this comprehension is E only, and the objects used in the indiscernibility are also only from E .

In fact, the bounded quantifier comprehension is given in terms of a normal form. I.e., every suitable k -ary relation on E is given by fixing 8 parameters from E in a fixed atomic formula with $k+8$ variables.

Section 5.4 ends with the following.

LEMMA 5.4.17. There exists a countable structure $M = (A, <, 0, 1, +, -, \cdot, \uparrow, \log, E, c_1, c_2, \dots)$, and terms t_1, t_2, \dots of L , where for all i , t_i has variables among v_1, \dots, v_{i+8} , such that the following holds.

- i) $(A, <, 0, 1, +, -, \cdot, \uparrow, \log)$ satisfies $TR(\Pi^0_1, L)$;
- ii) $E \subseteq A \setminus \{0\}$;
- iii) The c_n , $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E \setminus \alpha(E; 2, < \infty)$ with no upper bound in A ;
- iv) Let $r, n \geq 1$ and $t(v_1, \dots, v_r)$ be a term of L , and $x_1, \dots, x_r \leq c_n$. Then $t(x_1, \dots, x_r) < c_{n+1}$;
- v) $2\alpha(E; 1, < \infty) + 1, 3\alpha(E; 1, < \infty) + 1 \subseteq E$;
- vi) Let $k, n \geq 1$ and R be a c_n -definable k -ary relation. There exists $y_1, \dots, y_8 \in E \cap [0, c_{n+1}]$ such that $R = \{(x_1, \dots, x_k) \in E^k \cap [0, c_n]^k : t_k(x_1, \dots, x_k, y_1, \dots, y_8) \in E\}$;
- vii) Let $r \geq 1$ and $\varphi(v_1, \dots, v_{2r})$ be a formula of $L(E)$. Let $1 \leq i_1, \dots, i_{2r} < n$, where (i_1, \dots, i_r) and (i_{r+1}, \dots, i_{2r}) have the same order type and the same min. Let $y_1, \dots, y_r \in E$, $y_1, \dots, y_r \leq \min(c_{i_1}, \dots, c_{i_r})$. Then $\varphi(c_{i_1}, \dots, c_{i_r}, y_1, \dots, y_r)^{c_n} \leftrightarrow \varphi(c_{i_{r+1}}, \dots, c_{i_{2r}}, y_1, \dots, y_r)^{c_n}$.

5.5. Comprehension, indiscernibles

Here we upgrade the bounded quantifier comprehension and indiscernibility to unbounded quantifier comprehension and indiscernibility. It is the indiscernibility itself that allows us to make this transition.

The comprehension produces bounded relations on E only.

A very robust and useful notion of internal relation emerges. These are the bounded relations on E that are definable with parameters from E and quantifiers ranging over E . See Lemma 5.5.4.

We pass to a second order structure where the internal relations are used to interpret the second order quantifiers.

We retain comprehension and indiscernibility in the appropriate forms.

Section 5.5 ends with the following.

LEMMA 5.5.8. There exists a countable structure $M^* = (A, <, 0, 1, +, -, \cdot, \uparrow, \log, E, c_1, c_2, \dots, X_1, X_2, \dots)$, where for all $i \geq 1$, X_i is the set of all i -ary relations on A that are c_n -definable for some $n \geq 1$; and terms t_1, t_2, \dots of L , where for all i , t_i has variables among x_1, \dots, x_{i+8} , such that the following holds.

- i) $(A, <, 0, 1, +, -, \cdot, \uparrow, \log)$ satisfies $TR(\Pi_1^0, L)$;
- ii) $E \subseteq A \setminus \{0\}$;
- iii) The c_n , $n \geq 1$, form a strictly increasing sequence of nonstandard elements of $E \setminus \alpha(E; 2, < \infty)$ with no upper bound in A ;
- iv) For all $r, n \geq 1$, $\uparrow r(c_n) < c_{n+1}$;
- v) $2\alpha(E; 1, < \infty) + 1, 3\alpha(E; 1, < \infty) + 1 \subseteq E$;
- vi) Let $k, n \geq 1$ and R be a c_n -definable k -ary relation. There exists $y_1, \dots, y_8 \in E \cap [0, c_{n+1}]$ such that $R = \{(x_1, \dots, x_k) \in E^k \cap [0, c_n]^k : t_k(x_1, \dots, x_k, y_1, \dots, y_8) \in E\}$;
- vii) Let $k \geq 1$, $m \geq 0$, and φ be an E formula of $L^*(E)$ in which R is not free, where all first order variables free in φ are among x_1, \dots, x_{k+m+1} . Then $x_{k+1}, \dots, x_{k+m+1} \in E \rightarrow (\exists R)(\forall x_1, \dots, x_k \in E)(R(x_1, \dots, x_k) \leftrightarrow (x_1, \dots, x_k \leq x_{k+m+1} \wedge \varphi))$;
- viii) Let $r \geq 1$, and $\varphi(x_1, \dots, x_{2r})$ be an E formula of $L^*(E)$ with no free second order variables. Let $1 \leq i_1, \dots, i_{2r}$, where (i_1, \dots, i_r) and (i_{r+1}, \dots, i_{2r}) have the same order type and the same min. Let $x_1, \dots, x_r \in E$, $x_1, \dots, x_r \leq \min(c_{i_1}, \dots, c_{i_r})$. Then $\varphi(c_{i_1}, \dots, c_{i_r}, x_1, \dots, x_r) \leftrightarrow \varphi(c_{i_{r+1}}, \dots, c_{i_{2r}}, x_1, \dots, x_r)$.

5.6. Π_1^0 correct internal arithmetic, simplification

The main focus of this section is the derivation of a suitable form of the axiom of infinity. This is the one place where it is essential to use that the c_n , $n \geq 1$, lie outside $\alpha(E; 2, < \infty)$. This is from Lemma 5.5.8 iii).

The axiom of infinity takes the form of the existence of an internal set containing 1, and closed under $+2c_1$.

We then define I to be the intersection of all internal sets containing 1, and closed under $+2c_1$. The set I will serve as the internal natural numbers.

It is important to link the arithmetic operations that are uniquely defined, internally, on I , with the arithmetic operations given by the structure M^* from Lemma 5.5.8. This is required in order to be able to use the fact that M^* satisfies the true Π_1^0 sentences. It allows us to conclude that the internal arithmetic on I satisfies the true Π_1^0 sentences.

The required link is provided by Lemma 5.6.11.

LEMMA 5.6.11. Every element of I is of the form $2xc_1+1$, with $x \in E-E$. $x \in I \wedge x > 1 \rightarrow x-2c_1 \in I$.

Thus we link each $2xc_1+1 \in I$ with $x \in E-E$. This suggests that we can define $+, \cdot, -, \uparrow, \log$ on I by applying the $+, \cdot, -, \uparrow, \log$ at relevant elements of $E-E$. But in order to do this, we need to know, e.g., that

$$2xc_1+1, 2yc_1+1 \in I \rightarrow 2xyc_1+1 \in I.$$

This is exactly what is established in Lemma 5.6.12.

So this defines the structure

$$M(I) = (I, <, 0', 1', +', -', \cdot', \uparrow', \log')$$

as in Definition 5.6.4, which is isomorphically embeddable in $(A, <, 0, 1, +, -, \cdot, \uparrow, \log)$.

Since $(A, <, 0, 1, +, -, \cdot, \uparrow, \log)$ satisfies the true Π_1^0 sentences, we would like to conclude that $M(I)$ also satisfies the true Π_1^0 sentences. However, because of the bounded quantifiers in Π_1^0 sentences, we can only conclude that $M(I)$ satisfies the true Π_1^0 sentences with no bounded quantifiers allowed.

However, in the presence of PA, every Π_1^0 sentence is equivalent to a Π_1^0 sentence with no bounded quantifiers, using the Y. Matiyasevich solution to Hilbert's 10th

problem (based on earlier work of J. Robinson, M. Davis, and H. Putnam). See [Da73], [Mat93].

By Lemma 5.6.13, $M(I)$ satisfies PA. Therefore $M(I)$ satisfies PA + the true Π^0_1 sentences.

We now introduce the linearly ordered set theory $K(\Pi)$ in Definition 5.6.10. It has a linear ordering of the universe, full separation, an initial segment serving as the integers, with operations $+, -, \cdot, \uparrow, \log$, obeying the true Π^0_1 sentences. There is also an infinite list of constants with axioms of indiscernibility.

A model of $K(\Pi)$ is explicitly constructed using M^* and $M(I)$. We put I at the bottom, and E (without the initial segment of E determined by I) on top. The arithmetical operations on I are inherited from $M(I)$. The c 's, after c_1 , serve as the indiscernibles. The \in relation is interpreted using the normal form relation σ from Lemma 5.6.17.

Section 5.6 ends with the following.

LEMMA 5.6.20. There exists a countable structure $M\# = (D, <, \in, \text{NAT}, 0, 1, +, -, \cdot, \uparrow, \log, d_1, d_2, \dots)$ such that the following holds.

- i) $<$ is a linear ordering (irreflexive, transitive, connected);
- ii) $x \in y \rightarrow x < y$;
- iii) The d_n , $n \geq 1$, form a strictly increasing sequence of elements of D with no upper bound in D ;
- iv) Let φ be a formula of $L\#$ in which v_1 is not free. Then $(\exists v_1) (\forall v_2) (v_2 \in v_1 \leftrightarrow (v_2 \leq v_3 \wedge \varphi))$;
- v) Let $r \geq 1$ and $\varphi(v_1, \dots, v_{2r})$ be a formula of $L\#$. Let $1 \leq i_1, \dots, i_{2r}$, where (i_1, \dots, i_r) and (i_{r+1}, \dots, i_{2r}) have the same order type and min. Let $y_1, \dots, y_r \leq \min(d_{i_1}, \dots, d_{i_r})$. Then $\varphi(d_{i_1}, \dots, d_{i_r}, y_1, \dots, y_r) \leftrightarrow \varphi(d_{i_{r+1}}, \dots, d_{i_{2r}}, y_1, \dots, y_r)$;
- vi) NAT defines a nonempty initial segment under $<$, with no greatest element, and no limit point, where all points are $< d_1$, and whose first two elements are $0, 1$, respectively;
- vii) $(\forall x)$ (if x has an element obeying NAT then x has a $<$ least element);
- viii) Let $\varphi \in \text{TR}(\Pi^0_1, L)$. The relativization of φ to NAT holds.
- ix) $+, -, \cdot, \uparrow, \log$ have the default value 0 in case one or more arguments lie outside NAT.

5.7. Transfinite induction, comprehension,
indiscernibles, infinity, Π^0_1 correctness

In $M\#$, the $<$ may not be internally well ordered. Moreover, we may not have extensionality.

The focus of section 5.7 is on creating a structure corresponding to the $M\#$ of Lemma 5.6.20 with an internally well founded $<$. However, this new structure will not be a model of a set theory, but rather a second order structure. I.e., we will have a linearly ordered set of points, with a family of relations on the points of each arity.

We will obtain full second order separation (second order of course limited to these families of relations), and an initial segment corresponding to the natural numbers. We will also obtain an infinite sequence of indiscernibles as in Lemma 5.6.20, cofinal in the linear ordering.

The idea is to first develop a theory of pre well orderings (as binary relations) within $M\#$. Every binary relation in $M\#$ is a point, since $M\#$ is a model of a set theory.

We use this theory of pre well orderings to place two closely related relations $<\#$, $\leq\#$, on points. See Definitions 5.7.21 and 5.7.22. These are, generally speaking, much stronger than the relations $<$, \leq . We define $x =\# y \leftrightarrow (x \leq\# y \wedge y \leq\# x)$.

By Lemma 5.7.18, we have the trichotomy

$$x <\# y \vee y <\# x \vee x =\# y, \text{ with exclusive } \vee.$$

The points in the desired structure with internal well foundedness are the equivalence classes under $=\#$, each of which forms an interval of points in M^* .

For the rest of the definition of the second order structure M^\wedge , see Definitions 5.7.26 - 5.7.34.

Section 5.7 ends with the following.

LEMMA 5.7.30. There exists a structure $M^\wedge = (C, <, 0, 1, +, -, \cdot, \uparrow, \log, \omega, c_1, c_2, \dots, Y_1, Y_2, \dots)$ such that the following holds.

- i) $(C, <)$ is a linear ordering;
- ii) $\{x: x < \omega\}$ forms an initial segment of $(C, <)$;
- iii) $(\{x: x < \omega\}, <, 0, 1, +, -, \cdot, \uparrow, \log)$ satisfies $\text{TR}(\Pi_1^0, L)$;
- iv) For all $x, y \in C$, $\neg(x < \omega \wedge y < \omega) \rightarrow x+y = x \cdot y = x-y = x \uparrow = \log(x) = 0$;

- v) The c_n , $n \geq 1$, form a strictly increasing sequence of elements of C , all $> \omega$, with no upper bound in C ;
- vi) For all $k \geq 1$, Y_k is a set of k -ary relations on C whose field is bounded above;
- vii) Let $k \geq 1$, and φ be a formula of L^\wedge in which the k -ary second order variable B_n^k is not free, and the variables B_r^m range over Y_r . Then $(\exists B_n^k \in Y_k) (\forall x_1, \dots, x_k) (B_n^k(x_1, \dots, x_k) \leftrightarrow (x_1, \dots, x_k \leq y \wedge \varphi))$;
- viii) Every nonempty M^\wedge definable subset of C has a $<$ least element;
- ix) Let $r \geq 1$ and $\varphi(v_1, \dots, v_{2r})$ be a formula of L^\wedge . Let $1 \leq i_1, \dots, i_{2r}$, where (i_1, \dots, i_r) and (i_{r+1}, \dots, i_{2r}) have the same order type and the same min. Let $y_1, \dots, y_r \in C$, $y_1, \dots, y_r \leq \min(c_{i_1}, \dots, c_{i_r})$. Then $\varphi(c_{i_1}, \dots, c_{i_r}, y_1, \dots, y_r) \leftrightarrow \varphi(c_{i_{r+1}}, \dots, c_{i_{2r}}, y_1, \dots, y_r)$.

5.8. ZFC + V = L, indiscernibles, and Π_1^0 correct arithmetic

Now that we have a second order structure M^\wedge from Lemma 5.7.30, we want to move back to a model of set theory. This time, the model will be of ZFC + V = L + the true Π_1^0 sentences, with an unbounded infinite sequence of ordinals with indiscernibility.

We need to build the constructible hierarchy in order to fully utilize the indiscernibility afforded by Lemma 5.7.30. In particular, the definable well ordering arising from L is needed in order to derive power set from indiscernibility.

Because of the internal well foundedness, the points in M^\wedge already behave like ordinals. In M^\wedge , we can perform various transfinite recursions, resulting in second objects in M^\wedge . Sometimes in order to accomplish this, we make use of the indiscernibles in M^\wedge .

Extensionality, pairing, and union are verified in L by Lemma 5.8.24. Infinity is verified in L by Lemma 5.8.25. Foundation is verified in L by Lemma 5.8.26. Separation and Collection, both of which are schemes, are verified in L by Lemma 5.8.29.

We then show that power set holds in L with heavy use of indiscernibility.

It suffices to show that if, in L , every element of $x \in L$ is constructed before stage c_2 , then $x < c_3$. (We can obtain

such a strong conclusion because extensionality is built into the construction of L). This is Lemma 5.8.32.

If this is false, then by indiscernibility, for each $n \geq 3$, there is an $x \geq c_n$ such that every element of x in L is constructed before stage c_2 .

Using the definable well ordering of L , we can set $J(n)$ to be the $<$ least $x \geq c_n$ such that every element of x in L is constructed before stage c_2 .

But by indiscernibility, $J(4) < J(5)$ and $J(4), J(5)$ will have the same elements in L . This is a contradiction. The treatment in section 5.8 is fully detailed. See Lemma 5.8.34.

We now obtain a model of ZF of the required kind. See Lemma 5.8.36. We can then relativize to L to obtain $ZFC + V = L$.

Section 5.8 ends with the following.

LEMMA 5.8.37. There exists a countable model M^+ of $ZFC + V = L + TR(\Pi_1^0, L)$, with distinguished elements d_1, d_2, \dots , such that

- i) The d 's are strictly increasing ordinals in the sense of M^+ , without an upper bound;
- ii) Let $r \geq 1$, and $i_1, \dots, i_{2r} \geq 1$, where (i_1, \dots, i_r) and (i_{r+1}, \dots, i_{2r}) have the same order type and min. Let R be a $2r$ -ary relation M^+ definable without parameters. Let $\alpha_1, \dots, \alpha_r \leq \min(d_{i_1}, \dots, d_{i_r})$. Then $R(d_{i_1}, \dots, d_{i_r}, \alpha_1, \dots, \alpha_r) \leftrightarrow R(d_{i_{r+1}}, \dots, d_{i_{2r}}, \alpha_1, \dots, \alpha_r)$.

5.9. $ZFC + V = L + \{(\exists \kappa) (\kappa \text{ is strongly } k\text{-Mahlo})\}_k + TR(\Pi_1^0, L)$, and 1-Con(SMAH) .

We first give a complete proof of a result in combinatorial set theory, of independent interest and not involving any developments in the book from sections 1.1 through 5.8. It is closely related to [Sc74] and the treatment is inspired by [HKS87]. The result is as follows.

THEOREM 5.9.5. The following is provable in ZFC. Let $k < \omega$ and α be an ordinal. Then $R(\alpha \setminus \omega, k+3, k+5)$ if and only if there is a strongly k -Mahlo cardinal $\leq \alpha$.

We then return to the model M^+ of $ZFC + V = L +$ the true Π_1^0 sentences, given by Lemma 5.8.37.

We show that the indiscernibles themselves (the d 's of M^+) essentially obey the relevant partition properties.

LEMMA 5.9.6. Let $k, r \geq 1$ be standard integers. Then $R(d_{r+2+1} \setminus \omega, k, r)$ holds in M^+ .

This is proved by first assuming that it is false, and then taking the L least counterexample. We can do this since M^+ obeys $V = L$. Then apply the indiscernibility in M^+ from Lemma 5.8.37.

We then easily obtain that M^+ satisfies $ZFC + V = L + \{\text{there exists a strongly } k\text{-Mahlo cardinal}\}_k + \text{the true } \Pi_1^0 \text{ sentences}$. In fact, we conclude

THEOREM 5.9.11. ACA' proves the equivalence of each of Propositions A, B, C and $1\text{-Con}(MAH), 1\text{-Con}(SMAH)$.

The above is shown by checking that all of the relevant steps in Chapter 5 can be carried out within ACA' , and quoting Theorem 4.4.11.

Chapter 5 ends with the following.

THEOREM 5.9.12. None of Propositions A, B, C are provable in any set of consequences of $SMAH$ that is consistent with ACA' . The preceding claim is provable in RCA_0 . For finite sets of consequences, the first claim is provable in EFA .

Chapter 6 Further Results

6.1. Propositions D-H

In section 6.1, we establish Theorem 5.9.11 for several variants of Propositions A, B, C . This requires various adaptations of Chapters 4 and 5.

The strongest proposition considered in this book that is proved from large cardinals is the following.

PROPOSITION D. Let $f \in LB \cap EVSD$, $g \in EXPN$, $E \subseteq \mathbb{N}$ be infinite, and $n \geq 1$. There exist infinite $A_1 \subseteq \dots \subseteq A_n \subseteq \mathbb{N}$ such that

- i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup gA_{i+1}$;
- ii) $A_1 \cap fA_n = \emptyset$;
- iii) $A_1 \subseteq E$.

Proposition D immediately implies Proposition B. We then adapt Chapter 4 to derive Proposition D in $ACA' + 1-Con(SMAH)$.

We then consider the remaining main variants of Propositions A,B,C in section 6.1.

PROPOSITION E. For all $f, g \in ELG \cap SD \cap BAF$ there exist $A \subseteq B \subseteq C \subseteq \mathbb{N}$, each containing infinitely many powers of 2, such that

$$\begin{aligned} fA &\subseteq B \cup gB \\ fB &\subseteq C \cup gC. \end{aligned}$$

PROPOSITION F. For all $f, g \in ELG \cap SD \cap BAF$ there exist $A \subseteq B \subseteq C \subseteq \mathbb{N}$, each containing infinitely many powers of 2, such that

$$\begin{aligned} fA &\subseteq C \cup gB \\ fB &\subseteq C \cup gC. \end{aligned}$$

PROPOSITION G. For all $f, g \in ELG \cap SD \cap BAF$ there exist $A, B, C \subseteq \mathbb{N}$, whose intersection contains infinitely many powers of 2, such that

$$\begin{aligned} fA &\subseteq C \cup gB \\ fB &\subseteq C \cup gC. \end{aligned}$$

PROPOSITION H. For all $f, g \in ELG \cap SD \cap BAF$ there exist $A, B, C \subseteq \mathbb{N}$, where $A \cap B$ contains infinitely many powers of 2, such that

$$\begin{aligned} fA &\subseteq C \cup gB \\ fB &\subseteq C \cup gC. \end{aligned}$$

We first observe that in RCA_0 , $D \rightarrow E \rightarrow F \rightarrow G \rightarrow H$. See Lemma 6.1.5.

Section 6.1 ends with an adaptation of part of Chapter 5 in order to resolve the status of Propositions E-H. I.e., ACA' proves Propositions E-H are equivalent to $Con(SMAH)$. See Theorem 6.1.10.

6.2. Effectivity

Section 6.2 begins with a straightforward proof that Propositions A-H hold in the arithmetic sets. The proof is conducted in ACA^+ . See Definition 6.2.1.

Next in section 6.2, we show that Propositions C,E-H hold in the recursive sets (and even in the sets with primitive

recursive enumeration functions). We also show that this result is provably equivalent to 1-Con(SMAH) over ACA'.

We don't know if any or all of Propositions A,B,D hold in the recursive sets. We conjecture that they do not.

Recall that in the proofs of Propositions C,E-H coming out of Chapter 4, we rely on an infinite set of indiscernibles for functions in BAF. These sets of indiscernibles are given by applying the infinite Ramsey theorem, and so go up the arithmetic hierarchy, and are far from being recursive.

A key idea of section 6.2 is the development of appropriate infinite sets of indiscernibles for functions in BAF that are recursive - and even primitive recursive or better.

This relies on properties of the structure $(\mathbb{N}, +, \uparrow)$, or base 2 exponential Presburger arithmetic. It has a primitive recursive decision procedure going back to [Se80], [Se83]. A modern treatment of quantifier elimination for this structure (with additional predicates) appears in [CP85], and also a more recent version appears as Appendix B in this book, authored by F. Point.

The required infinite sets of indiscernibles are given by Lemma 6.2.17.

Section 6.2 continues with an adaptation of sections 4.3 and 4.4 primitive recursively. This culminates with Theorem 6.2.20.

6.3. A Refutation

Section 6.3 is devoted to a refutation of the following.

PROPOSITION α . For all $f, g \in \text{SD} \cap \text{BAF}$ there exist $A, B, C \in \text{INF}$ such that

$$\begin{aligned} A \cup fA &\subseteq C \cup gB \\ A \cup fB &\subseteq C \cup gC. \end{aligned}$$

Note that this shows the need for using ELG in Propositions A,B,C. In fact, section 6.3 contains a refutation of the following.

PROPOSITION β . Let $f, g \in \text{SD} \cap \text{BAF}$. There exist $A, B, C \subseteq \mathbb{N}$, $|A| \geq 4$, such that

$$\begin{aligned} A \cup fA &\subseteq C \cup gB \\ A \cup fB &\subseteq C \cup gC. \end{aligned}$$

The proof proceeds by assuming Proposition β , and first adapting Lemma 5.1.8. See Lemma 5.1.8'. This is followed by a combinatorial construction that provides the required contradiction.

0.16. Some Open Problems.

1. Is the set of all true instances of EBRT (or IBRT) in $A_1, \dots, A_k, f_1A_1, \dots, f_1A_m, \dots, f_nA_1, \dots, f_nA_m$ on (MF, INF) (or (SD, INF) , (ELG, INF) , $(EVSD, INF)$) recursive? Here n, m are not fixed. We expect a positive result to be hugely intractable, and so we are raising the possibility of a negative result.
2. PBRT was introduced in section 1.1, but not investigated in this book. It is spectacularly more complex than EBRT and IBRT. See Definition 1.1.26, and the brief discussion of PBRT right after the proof of Theorem 1.1.2. What can we say about PBRT in A, fA on (MF, INF) (or (SD, INF) , (ELG, INF) , $(EVSD, INF)$)? What about question 1 for PBRT?
3. Does the behavior of BRT fragments in the various BRT settings presented in section 1.2 depend very delicately on the choice of BRT setting, as we believe? Give some precise formulations of this question and determine whether they hold.
4. This concerns the Upper Complementation Theorem of section 1.3. Is there a decision procedure for determining whether, given two affine functions $f: \mathbb{N}^k \rightarrow \mathbb{Z}$, whether their unique upper complementations are equal? What if the two functions are quadratics? Polynomials? For any given affine f , what can we say about the computational complexity of its unique upper complementation?
5. Every instance of EBRT in A, B, fA, fB, \subseteq on (SD, INF) , (ELG, INF) , $(EVSD, INF)$ is provable or refutable in RCA_0 . This is shown in sections 2.4, 2.5. Is every instance of EBRT in A, B, fA, fB on (SD, INF) , $(ELG \cap SD, INF)$, (ELG, INF) , $(EVSD, INF)$ provable or refutable in RCA_0 ? As a presumably smaller step, what about using $A, B, fA, fB, fU, \subseteq$?
6. Every instance of EBRT in $A_1, \dots, A_k, fA_1, \dots, fA_k, \subseteq$ on (MF, INF) is provable or refutable in RCA_0 . This is shown in section 2.6. Is every instance of EBRT in $A_1, \dots, A_k, fA_1, \dots, fA_k$ on (MF, INF) provable or refutable in RCA_0 ? What if $k = 2$?

7. What about question 5 for IBRT in light of section 2.7?

Recall the Template of Chapter 3:

TEMPLATE. For all $f, g \in \text{ELG}$ there exist $A, B, C \in \text{INF}$ such that

$$\begin{aligned} X \cup. fY &\subseteq V \cup. gW \\ P \cup. fR &\subseteq S \cup. gT. \end{aligned}$$

Consider two richer Templates.

TEMPLATE'. For all $f, g \in \text{ELG}$ there exist $A, B, C \in \text{INF}$ such that

$$\begin{aligned} X \cup. fY &\subseteq V \cup. gW \\ P \cup. fR &\subseteq S \cup. gT. \\ D \cup. fE &\subseteq J \cup. gK. \end{aligned}$$

TEMPLATE''. For all $f, g \in \text{ELG}$ there exist $A, B, C \in \text{INF}$ such that

$$\begin{aligned} X \cup. \alpha Y &\subseteq V \cup. \beta W \\ P \cup. \gamma R &\subseteq S \cup. \delta T. \end{aligned}$$

where $\alpha, \beta, \gamma, \delta$ are among the letters f, g .

8. Every instance of the above Template is provable or refutable in SMAH^+ . This is shown in Chapter 3. Is this true for Template'? Is this true for Template''?

9. The Principal Exotic Case (Proposition A) universally quantifies over eight numerical parameters. The upper and lower rational constant factors for $f \in \text{ELG}$, the lower and upper rational constant factors for $g \in \text{ELG}$, constants for sufficiently large associated with each of these four rational constant factors, the arity of f , and the arity of g . In the case of Proposition B, there is an additional parameter, namely the length of the tower. In section 4.2, we proved Proposition B by fixing $p, n \geq 1$, where p is the arity of f , and n is the length of the tower. We used a strongly p^{n-1} -Mahlo cardinal. This amounts to using a strongly p^2 -Mahlo cardinal to prove the Principal Exotic Case (Proposition A). What is the least order of strong Mahloness needed here? Also, what is the metamathematical status of Propositions A (B) if we fix various combinations of the eight (nine) parameters and let the others vary? For some combinations, we expect to get independent statements, and for other combinations we expect to get Σ_1^0 statements,

which are, of course provable. But do we get length of proof results corresponding to the provably recursive functions of SMAH?

10. The Principal Exotic Case, is an instance of EBRT in A, C, fA, fB, gB, gC on (ELG, INF) . The Principal Exotic Case with $A \subseteq B \subseteq C$ is an instance of EBRT in $A, C, fA, fB, gB, gC, \subseteq$ on (ELG, INF) . They are both provable in $SMAH^+$ but not in SMAH. This is shown in section 4.2 and in Chapter 5. Is every instance of EBRT in $A, B, C, fA, fB, fC, gA, gB, gC$ on (ELG, INF) provable or refutable in $SMAH^+$? What about in $A, B, C, fA, fB, fC, gA, gB, gC, \subseteq, A, C, fA, fB, gB, gC,$ or $A, C, fA, fB, gB, gC, \subseteq$?

11. ACA' proves that Propositions A-H are each equivalent to $1-Con(SMAH)$. This is shown in section 6.1. For which of these Propositions, can ACA' be replaced by RCA_0 , or by WKL_0 in either the forward or the reverse direction of the equivalence?

12. Propositions A-H hold in the arithmetic sets. This is shown in section 6.2. Does the Principal Exotic Case (Proposition A) hold in the recursive sets? What about Propositions B, D?

13. Propositions C, E-H hold in the recursive sets, and even in the sets with primitive recursive enumeration functions. This is shown in section 6.2. Do Propositions C, E-H hold in the sets with superexponential enumeration functions as discussed at the end of section 6.2?

14. What is the status of Proposition D[5] presented in section 6.1? What is the status of Proposition G[1], also presented in section 6.1?

0.17. Concreteness in the Hilbert Problem List.

We now discuss the levels of Concreteness associated with Hilbert's famous list of 23 problems, 1900. See [Br76], and http://en.wikipedia.org/wiki/Hilbert's_problems#Table_of_problems

[Br76] includes a reprint of Hilbert's article. For ready web access, see

<http://aleph0.clarku.edu/~djoyce/hilbert/toc.html>

<http://aleph0.clarku.edu/~djoyce/hilbert/problems.html>

It is important to distinguish between two quite different but overlapping projects. We use HP for "Hilbert's Problems".

HP PROOF THEORY. An analysis of levels of Concreteness in the **proofs of theorems** surrounding the Hilbert problem list.

HP STATEMENT THEORY. An analysis of levels of Concreteness in the **statements of propositions** surrounding the Hilbert problem list.

In this section, we focus entirely on HP Statement Theory. We view it as preliminary to a systematic development of HP Proof Theory.

There is a very limited amount of work in HP Proof Theory. We view HP Proof Theory as part of a wider Mathematical Proof Theory limited to theorems surrounding the Hilbert problem list. Here Mathematical Proof Theory is the systematic study of Concreteness in mathematical proofs, generally in the sense of Reverse Mathematics and Strict Reverse Mathematics as discussed in section 0.4.

We view HP Statement Theory as part of a wider Mathematical Statement Theory limited to propositions (which may or may not be theorems) surrounding the Hilbert problem list. HP Mathematical Statement Theory is the systematic study of Concreteness in mathematical statements. We make full use of the basic framework laid out in section 0.3, consisting of the categories of sentences

$$\Pi^0_n, \Sigma^0_n, \Pi^1_n, \Sigma^1_n, 0 \leq n \leq \infty$$

discussed there. In Mathematical Statement Theory, we begin with a mathematical proposition P , and proceed as follows.

- a. We first examine a fully detailed statement of P and find the lowest category in which it resides, without significant reformulation of P . We say that P is literally Π^i_j (or Σ^i_j).
- b. We then find a reformulation P' of P , so that we can prove the equivalence $P \leftrightarrow P'$, where P' is in the lowest category of sentences above that we can find. We say that P is essentially Π^i_j (or Σ^i_j).

c. If P has already been proved (or refuted), then b) is not to be taken literally, because we can always take P' to be $0 = 0$ (or $1 = 0$), and declare any P to be essentially Π^0_0 . In other words, if we just follow b) uncritically, then Mathematical Statement Theory does not apply to theorems - only to propositions of unknown status.

d. In case P has already been proved (or refuted), we demand that the proof of the equivalence $P \leftrightarrow P'$ be based on generally applicable principles, and not involve substantial ideas from the proof (or refutation) of P .

e. Of special note in the theory are implications $P' \rightarrow P$, where P' is in the lowest category we can find, and P is interesting. I.e., P' is a strengthening of P . If P is not (yet) a theorem, then we want P' to represent a reasonable path toward proving P . If P is a theorem, then we want the proof of the implication $P' \rightarrow P$ to not involve substantial ideas from the proof of P , and ideally, P' should also be a theorem. This often occurs when one discovers the "combinatorial essence" of a proof. P' is based on the combinatorial essence of P .

We acknowledge the informal nature of d), but submit that in practice, d) is rather objective. To a lesser extent, there are fuzzy issues regarding a) as well. In fact, a) and d) appear to be sufficiently objective in practice to support the viability of Mathematical Statement Theory.

Coming back to HP Proof Theory, the principal tool used for analyzing levels of Concreteness in proofs is our Reverse Mathematics program (RM). The RM program was discussed in detail in section 0.3.

However, not much of the work surrounding the Hilbert problems falls under the scope of RM. One reason is that so much of the work on these problems falls below the radar screen of RM - the proof is already carried out (or easily seen to be carried out) in the base theory, RCA_0 , of RM.

As discussed in section 0.3, our Strict Reverse Mathematics program (SRM), which was conceived of even before RM, has a far more ambitious scope than RM. However, SRM is at a very early stage of development, having been effectively launched only with the recent [Fr09], [Fr09a] - and only there in certain limited directions. Yet more substantial work needs to be done in order to bring SRM to anything like the level of development RM even decades ago.

It would seem premature to apply SRM to HP Proof Theory at this point, although such a venture will be a great test for the SRM program.

It would be of great interest to investigate Smale Problems Statement Theory, and Clay Problems Statement Theory, based on the 18 Smale problems, 1998, and the 7 Clay Millennium Prize Problems, 2000. See [Sm00] and [<http://www.claymath.org>].

There are many gaps in our limited discussion of HP Statement Theory. We view the treatment below as a good starting point for an intensive and systematic investigation. This, in turn, should serve as a prototype for Mathematical Statement Theory.

However, it must be said that it is not yet clear just what the most fruitful and illuminating frameworks are for a suitable discussion of Concreteness and Abstraction in mathematics. Even though the framework of Mathematical Statement Theory needs to be solidified and amplified, we expect it will remain an integral part of subsequent formulations.

H1. Cantor's problem of the cardinal number of the continuum

This well known problem of Cantor in abstract set theory - called the continuum hypothesis - can be conveniently stated as follows. Every infinite set of real numbers is in one-one correspondence with the integers of the real numbers. Assuming ZFC is consistent, this statement is not provable in ZFC ([Co63,64]), and not refutable in ZFC ([Go38], [Go86-03]). The use of all sets of real numbers (and functions onto the reals) means that it is a statement of Abstract Mathematics as opposed to Concrete Mathematics.

Furthermore, it is well known that the Continuum Hypothesis is not provably equivalent, over ZFC, to any Π^1_n sentence, $n \geq 1$, and hence lies essentially outside of Concrete Mathematics.

The easiest way to prove this claim is to start with a countable model M of $ZFC + 2^\omega = \omega_2$. Let M' be a generic extension of M obtained by collapsing ω_2 to ω_1 using countable functions from ω_1 into ω_2 . Then $2^\omega = \omega_1$ holds in M' , yet M and M' have the same real numbers.

The continuum hypothesis has well known specializations to (more) concrete mathematical objects. For instance, it is provable in ZFC that every infinite Borel set of real numbers is in one-one correspondence with the integers or the real numbers.

To be fully coherent, we also need to treat the maps. It is also provable in ZFC that every infinite Borel set of real numbers is in Borel one-one correspondence with the integers or the real numbers. In fact, we can replace Borel by "Borel of finite rank".

This Borel form of the continuum hypothesis follows easily from the classic theorem of Alexandrov and Hausdorff that every Borel set of real numbers is either countable or contains a Cantor set, and the obvious Borel form of the Cantor-Bernstein theorem. See [Ke95], p. 83, and [Je78,06].

H2. The compatibility of the arithmetical axioms

This is properly viewed as a metamathematical problem as opposed to a mathematical problem. However, it did generate a considerable amount of work on formal systems and their relationships, beginning, most notably, with [Pr29] and [Go31].

These formal investigations generally give rise to formal problems in classes Π^0_1 , Σ^0_1 , Π^0_2 , and Σ^0_2 , and theorems in classes Π^0_1 , Π^0_2 .

For instance, consistency of an effectively presented formal system is a Π^0_1 sentence; interpretability of one finitely axiomatized system in another is a Σ^0_1 sentence; 1-consistency of an effectively presented formal system is a Π^0_2 sentence; interpretability of one effectively presented formal system in another is a Σ^0_3 sentence. In each specific example, the relevant theorems witness the outermost existential quantifiers with particular interpretations.

H3. The equality of two volumes of two tetrahedra of equal bases and equal altitudes

Hilbert asks whether there exists

two tetrahedra of equal bases and equal altitudes which can in no way be split up into congruent tetrahedra, and which cannot be combined with congruent tetrahedra to form two

polyhedra which themselves could be split up into congruent tetrahedral.

The dissections are normally required to be polyhedra, in the sense of a 3 dimensional solid consisting of a collection of polygons, joined at their edges.

The problem is literally Σ^1_2 as stated. This is a rather high complexity class, given that so much mathematics is Π^0_∞ .

Suppose two tetrahedra are given, as well as an integer bound on the number of complementary tetrahedra allowed, the number of pieces in the dissections allowed, and the number of points in the polyhedra allowed. Then the statement of impossibility can be expressed as a first order formula in the ordered field of reals. Thus the formula is subject to Tarski's elimination of quantifiers for real closed fields, [Ta51], and is quantifier free in the language of ordered fields.

These considerations show that H3 is essentially Σ^1_1 . The outermost second order existential quantifiers correspond to the tetrahedral, which are followed by a universal quantifier(s) over integers, corresponding to the bound.

Can further uses of Tarski's elimination and some general principles further reduce the essentially complexity? E.g., from Σ^1_1 to Π^0_2 or even Π^0_1 ?

As is widely known, the problem was solved negatively in [Dehn01] using Dehn invariants. The counterexample given by Dehn provides many specific natural examples α, β .

For any of these specific natural examples (using algebraic points), the Tarski elimination yields a Π^0_1 sentence, since the outermost second order quantifiers are replaced by specific algebraic numbers.

Thus H3 is immediately implied by a Π^0_1 sentence. The proof of this implication does not involve [Dehn01].

H4. Problem of the straight line as the shortest distance between two points

It would be very interesting to have clear formulations of this problem, and subject them to logical analysis.

H5. Lie's concept of a continuous group of transformations without the assumption of the differentiability of the functions defining the group

The modern formulation of this problem is:

Are continuous groups automatically differentiable groups?

A topological group (continuous group) G is a topological space and group such that the group operations of product and inverse are continuous.

A continuous group is a topological group where the topological space is locally Euclidean.

The problem asks whether it follows that the group operations of product and inverse are (continuously) differentiable.

It is clear that we can assume without loss of generality that the space is separable.

Additional considerations show that the problem is essentially in class Π^1_1 . Do the positive solutions by Gleason, Montgomery, Zippin provide a stronger assertion that is essentially Π^0_2 , or even essentially Π^0_1 ?

H6. Mathematical Treatment of the Axioms of Physics

The investigations on the foundations of geometry suggest the problem: To treat in the same manner, by means of axioms, those physical sciences in which already today mathematics plays an important part; in the first rank are the theory of probabilities and mechanics.

Although very substantial mathematics is needed to begin seriously treating this problem, the problem itself is not a mathematical problem in the sense meant here.

H7. Irrationality and transcendence of certain numbers

Hilbert's seventh problem is answered by the Gelfond-Schneider theorem, which states that

If α and β are algebraic numbers with $\alpha \neq 0, 1$ and if β is not a rational number, then any value of $\alpha^\beta = \exp(\beta \log \alpha)$ is a transcendental number.

There are three main types of such problems. The first is where we present a particular interesting number, and ask if it is irrational or if it is transcendental. In this case, invariably we have an effective means of approximating the number, α .

It follows that " α is irrational" is a Π^0_2 sentence, and that " α is transcendental" is also a Π^0_2 sentence.

A particularly famous example is $e + \pi$. It is not known if $e + \pi$ is rational or if $e + \pi$ is transcendental. The transcendence, or irrationality, is in Π^0_2 .

Many expect that not only is $e + \pi$ irrational, but there is a reasonable function f such that

$$(\forall a, b \geq 1) (|e + \pi - a/b| > 1/f(a, b))$$

thereby creating a stronger form of the assertion, that is Π^0_1 .

The second is statements that all interesting combinations of a countable family of numbers - typically algebraic numbers - are irrational, or transcendental. Such statements are also generally Π^0_2 . The Gelfond-Schneider theorem is obviously of this second type.

Does the proof of the Gelfond-Schneider theorem give a stronger theorem that is much more concrete? E.g., Π^0_2 or even Π^0_1 ?

The third type concerns relationships between interesting combinations of arbitrary real or complex numbers. Such statements are generally Π^1_1 . We expect that they are generally implied by interesting statements of far lower complexity - e.g., Π^0_2 or even Π^0_1 .

Schanuel's Conjecture is in the third type, and is wide open. So Schanuel's Conjecture is literally Π^1_1 . Is there a reasonable stronger conjecture that is much more concrete? E.g., Π^0_2 , or even Π^0_1 ?

H8. Problems of prime numbers

Here Hilbert poses the following problems.

The Riemann hypothesis (the real part of any non-trivial zero of the Riemann zeta function is $1/2$), Goldbach's

conjecture (every even number greater than 2 can be written as the sum of two prime numbers), and the Twin Prime conjecture (there are infinitely many primes p such that $p+2$ is prime).

Let

$$\delta(x) = \prod_{n < x} \prod_{j \leq n} \eta(j)$$

where $\eta(j) = 1$ unless j is a prime power, and $\eta(p^k) = p$.

LEMMA. RH is equivalent to the following. For all integers $n \geq 1$, $(\sum_{k \leq \delta(n)} 1/k - n^2/2)^2 < 36 n^3$.

Proof: See [DMR76]], p. 335. QED

The above equivalence to RH can be straightforwardly expressed in Π_1^0 form, and so RH is essentially Π_1^0 .

It is obvious that Goldbach's conjecture and Fermat's Last Theorem are Π_1^0 . The latter was proved by Wiles.

The Twin Prime conjecture asserts that for all $n \geq 0$ there exists $p > n$ such that p and $p+2$ are prime. Hence the Twin Prime conjecture is Π_2^0 .

It is expected that the Twin Prime conjecture is true and a stronger result will be obtained in the form

$$(\forall n) (\exists p) (p, p+2 \text{ are prime and } p \leq f(n))$$

for some reasonable function f . This strong form will obviously be Π_1^0 .

Mordell's conjecture (proved by Faltings) is Π_3^0 . It asserts that certain Diophantine equations have at most finitely many solutions. I.e., this takes the form

$$(\forall n) (\exists m) (\forall r) (h(n, m, r) \text{ is not a solution})$$

which is Π_3^0 . (Here h is a specific primitive recursive function required in the classification scheme.)

Many expect this result to be improved with an upper bound for m as a reasonable function of n :

$$(\forall n) (\exists m \leq f(n)) (\forall r) (h(n, m, r) \text{ is not a solution})$$

which is Π_1^0 (after some quantifier manipulation).

H9. Proof of the most general law of reciprocity in any number field

A number field is a finite degree field extension of the field of rational numbers. The residue fields are all finite, and so these kinds of problems about solving equations mod primes are all Π_1^0 .

This problem led to far reaching developments in algebraic number theory, and ultimately to the Langlands program. It would be interesting to see what these developments mean from the point of view of Mathematical Statement Theory.

H10. Determination of the solvability of a diophantine equation

The most commonly cited interpretation of Hilbert's tenth problem is the following.

Is there an algorithm for determining whether a given polynomial of several variables with integer coefficients has a zero in the integers?

This has the form

$$(\exists \text{ algorithm } \alpha) (\forall \text{ integral polynomials } P) (P \text{ has a zero} \rightarrow \alpha(P) = 1 \wedge P \text{ does not have a zero} \rightarrow \alpha(P) = 0)$$

which is Σ_3^0 (after some quantifier manipulation). The negation

$$(\forall \text{ algorithm } \alpha) (\exists \text{ integral polynomial } P) (\neg(P \text{ has a zero} \wedge \alpha(P) = 1 \wedge P \text{ does not have a zero} \rightarrow \alpha(P) = 0))$$

is therefore Π_3^0 , and was proved in [Mat70] building on earlier work of M. Davis, H. Putnam, and J. Robinson. See [Da73], [DMR76], [Mat93].

Actually, what is proved is stronger, and results in a Σ_2^0 sentence. A rather complicated algorithm γ is provided with the following Π_1^0 property.

Given any algorithm α , $\gamma(\alpha)$ quickly produces
 an integral polynomial P
 and an integral vector x such that either
 $P(x) = 0$ and $\alpha(x)$ does not compute 1, or

$P(x)$ has no integral zero and $\alpha(x)$ does not compute 0.

If we ask for real or complex zeros, then there is an algorithm by [Ta51]. The problem is open for rational zeros.

There has been considerable interest in this problem over number fields. It is known that if the Shafarevich-Tate conjecture holds, then Hilbert's Tenth Problem has a negative answer over the ring of integers of every number field. See [MR10].

We use the solution to H10 in section 5.6 as a technical tool.

H11. Quadratic forms with any algebraic numerical coefficients

A quadratic form over a number field F is a quadratic in several variables over F , all of whose terms have degree 2. Two quadratic forms over F are considered equivalent over F if and only if one form can be transformed to the other by a linear transformation with coefficients from F .

The Hasse Minkowski theorem is most often cited in connection with H11. It asserts that two quadratic forms over a number field are equivalent if and only if they are equivalent over every completion of the field (which may be real, complex, or p -adic).

This theorem takes the form

$$(\forall \text{ number fields } F) (\forall \text{ quadratic forms } \alpha, \beta \text{ over } F) \\ (\alpha, \beta \text{ are equivalent over } F \leftrightarrow (\forall \text{ completions } F' \text{ of } F) \\ (\alpha, \beta \text{ are equivalent over } F')).$$

It would appear that using standard techniques, this can be put into Π_{∞}^0 form. Can it be put into Π_2^0 or even Π_1^0 ? If there a stronger theorem that is in Π_1^0 ?

H12. Extension of Kronecker's theorem on Abelian fields to any algebraic realm of rationality

The modern interpretation of this problem is to extend the Kronecker-Weber theorem on Abelian extensions of the rational numbers to any base number field.

The Kronecker-Weber theorem states that every finite extension of \mathbb{Q} whose Galois group over \mathbb{Q} is Abelian, is a subfield of a cyclotomic field; i.e., a field obtained by adjoining a root of unity to \mathbb{Q} . This takes the form

$$(\forall \text{ finite extensions } F \text{ of } \mathbb{Q}) (\text{Gal}(F/\mathbb{Q}) \text{ is Abelian} \rightarrow \\ (\exists \text{ cyclotomic } G \text{ over } \mathbb{Q}) (F \text{ is a subfield of } G))$$

which is Π_3^0 . It would appear that this can be put into Π_2^0 form. Is there a stronger form that is Π_1^0 ?

The same issues occur with related statements over any base number field.

H13. Impossibility of the solution of the general equation of the 7-th degree by means of functions of only two arguments

In modern terms, Hilbert considered the general seventh-degree equation

$$x^7 + ax^3 + bx^2 + cx + 1 = 0$$

and asked whether its solution, x , a function of the three coefficients a, b, c , can be expressed using a finite number of two variable functions.

A more general question is: can every continuous function of three variables be expressed as a composition of finitely many continuous functions of two variables?

V.I. Arnold proved a much stronger statement: every continuous function of three variables be expressed as a composition of finitely many continuous functions of two variables? See [Ar59, 62].

Arnold's statement is in Π_2^1 form, using standard coding techniques from mathematical logic. Is there a yet stronger version that is much more concrete? E.g., Π_2^0 or Π_1^0 ?

H14. Proof of the finiteness of certain complete systems of functions

In modern terms, Hilbert asks the following question.

Let F be a field, and K be a subfield of $F(x_1, \dots, x_n)$. Is the ring $K \cap F[x_1, \dots, x_n]$ finitely generated over F ?

Here $F(x_1, \dots, x_n)$ and $F[x_1, \dots, x_n]$ are the ring of rational functions over F and the ring of polynomial functions over F , in n variables.

On the face of it, this question is even less concrete than H1, the continuum hypothesis! This is because the question involves absolutely all fields F .

Is there a way of separating the abstract set theory from the intended mathematical content? More specifically, is there a way of showing, e.g., that if the statement holds for all countable fields, then it holds for all fields?

The answer is yes by a simple construction. Let F, K be a counterexample. Build an appropriate infinite sequence from F and from K , and use the subfield of F generated by the infinite sequence from F .

Consequently, we consider the following statement.

Let F be a countable field, and K be a subfield of $F(x_1, \dots, x_n)$. Is the ring $K \cap F[x_1, \dots, x_n]$ finitely generated over F ?

This is a Π_1^1 sentence. Can we put it in Π_∞^0 form using basic algebraic principles? What about Π_2^0 or even Π_1^0 ?

Nagata gave a negative answer to H14 in [Na59].

[CT06] gives the following formulation of Hilbert's 14th problem:

If an algebraic group G acts linearly on a polynomial algebra S , is the algebra of invariants S^G finitely generated?

According to [CT06], this has been proved for reductive G in [Hil1890], and for certain nonreductive groups in [Wei32]. Can this theorems, and related open questions, be put into Π_∞^0 , or even Π_2^0 or Π_1^0 form? Are they implied by Π_1^0 statements?

H15. Rigorous foundation of Schubert's enumerative calculus

Hermann Schubert claimed some spectacular counts on the number of geometric objects satisfying certain conditions, using methods that were not rigorous even by 1900

standards. Many of his claims have not been confirmed or denied.

Hilbert asked for a rigorous foundation for Schubert's enumerative calculus. Independently of the search for foundations here, many, if not all, of his counts, when given rigorous treatments, fit into the framework of Tarski's decision procedure for the field of real numbers, [Ta51].

As an example, it follows (based on work subsequent to Tarski), that there is an algorithm that takes any $S \subseteq \mathcal{R}^n \times \mathcal{R}^m$ presented with rational coefficients, and produces a number $0, 1, \dots, \infty$, which counts the number of distinct cross sections of S (obtained by fixing the first argument, from \mathcal{R}^n). This can be applied in the many situations where one wants to count the number of nice objects satisfying some nice condition.

This can be used to put various statements in Π^0_1 form, or even in quantifier free form.

H16. Problem of the topology of algebraic curves and surfaces

In modern terms: describe relative positions of ovals originating from a real algebraic curve and as limit cycles of a polynomial vector field on the plane.

Here a limit cycle of a polynomial vector field in the plane is a periodic orbit which can be separated from all other periodic orbits by placing a tube around it. Here it is understood that periodic orbits consist of more than one point.

It has been shown in [Il91] and [Ec92] (or at least claimed) that every polynomial vector field in the plane has at most finitely many limit cycles.

We can put this in the form

$$(\forall P) (\exists n) (\forall x_1, \dots, x_n) (x_1, \dots, x_n \text{ do not generate different limit cycles})$$

which, unless some interesting mathematics comes to bear, is going to be Π^1_3 and maybe a lot higher. Can we use perhaps even some elementary mathematics to reduce this

very sharply? Does the proof yield a stronger statement that is far more concrete? Perhaps Π_2^0 or even Π_1^0 ?

A principal open question is whether there is a uniform bound on the number of limit cycles of a polynomial vector field in the plane that depends only on the degree of the polynomial. This takes the form

$$(\forall d) (\exists n) (\forall P \text{ of degree } \leq d) (\exists x_1, \dots, x_n) \\ (\forall y) (\text{if } y \text{ is not on a limit cycle then } x_1, \dots, x_n \text{ are on it})$$

which also looks Π_3^1 and maybe a lot higher, unless some interesting (perhaps elementary) mathematics is used to reduce the complexity.

H17. Expression of definite forms by squares

In modern terms, is every polynomial of several variables over the reals that assumes no negative values a sum of squares of rational functions?

Emil Artin proved the assertion in [Art27]. The theorem takes the form

$$(\forall \text{ polynomials } P) (\text{if } P \text{ assumes no negative value then} \\ (\exists \text{ rational functions } R_1, \dots, R_k) (P = R_1^2 + \dots + R_k^2 \text{ holds} \\ \text{everywhere}))$$

which is Π_3^1 with no mathematical considerations. However, much sharper results have been proved which are much more concrete.

Specifically, it is known that for each d, n , there exists r such that

$$\text{for all polynomials of degree } \leq d \text{ in } n \text{ variables,} \\ \text{if } P \text{ assumes no negative value then} \\ P \text{ is the sum of at most } r \text{ rational functions} \\ \text{of degrees at most } r.$$

See [Day61], [Kre60], [Rob55], [Rob56], [DGL92]. In fact, a primitive recursive bound on r as a function of d, n is given in the first two references.

Note that the displayed statement above is a sentence in the language of the field of real numbers, primitive recursively obtained from d, n . Using Tarski's decision procedure for the field of real numbers, [Ta51], we now see

that this stronger result is Π_2^0 . In fact, given the above mentioned upper bound on r , we see that the strong form of this stronger result is in fact Π_1^0 .

H18. Building up of space from congruent polyhedra

In modern terms, there are three parts to the problem.

The first part asks whether there are only finitely many essentially different space groups in n -dimensional Euclidean space.

More formally, let $E(n)$ be the group of all isometries of \mathfrak{R}^n . We look for discrete subgroups $\Gamma \subseteq E(n)$ such that there is a compact region $D \subseteq \mathfrak{R}^n$ where the various congruent copies of D cover \mathfrak{R}^n and have only boundary points in common.

Ludwig Bieberbach answered this question affirmatively by showing that there are only finitely many such Γ up to isomorphism. See [Bi11], [Bi12].

The theorem takes the form: for some t , if

if G_1, \dots, G_t are discrete in $E(n)$, and
 $D_1, \dots, D_t \subseteq \mathfrak{R}^n$ are compact and congruent copies of D_i under
 G_i
 that cover \mathfrak{R}^n and have only boundary points in common,
 then there exists $i \neq j$ such that G_i and G_j are isomorphic.

Using quantifier manipulations and a small dose of mathematics, we see that this is Π_3^1 . We expect that with some additional mathematics, this can be reduced to Π_1^1 . We also expect that from Bieberbach's work, we can find a stronger statement which is considerably more concrete. Possibly Π_2^0 or even Π_1^0 .

The second part of the problem asks whether there exists a polyhedron which tiles 3-dimensional Euclidean space but is not the fundamental region of any space group. Such tiles are called anisohedral.

It is now known that there is an anisohedral tiling of even 2-dimensional Euclidean space. See Heinrich Heesch's Tiling, <http://www.spsu.edu/math/tiling/17.html>

The problem is in the form

(\exists polyhedron P) (P is not the fundamental region of any space group $\wedge P$ tiles the plane)

which appears to be around Σ^1_2 with only simple mathematical considerations. But consider the stronger statement

(\exists polyhedron P) (P is not the fundamental region of any space group $\wedge P$ tiles the plane periodically).

We can put this in the form: there exists r such that

\exists polyhedron P with r sides) (P is not the fundamental region of any space group $\wedge P$ tiles the plane periodically).

We expect that the displayed property of r can be viewed as a sentence in the theory of the field of reals, so that we can apply Tarski's decision procedure [Ta51]. This results in a Σ^0_1 sentence.

The third part of the problem asks for the best way to pack congruent solids of a given form. In particular, spheres of equal radius in \mathfrak{R}^3 .

The Kepler Conjecture is the case of sphere packing: the usual way of packing spheres of equal size in \mathfrak{R}^3 is the best.

Appropriate use of Tarski's decision procedure for the field of real numbers will show that the Kepler Conjecture - in various fully rigorous forms - is essentially Π^0_1 .

Of course, Hales has reduced Kepler's Conjecture to a specific large computation, which is Π^0_0 . But that involves deep insights into the problem itself, and is not a generic reduction in the sense of using the decision procedure for the real numbers.

H19. Are solutions of regular problems in the calculus of variations always necessarily analytic?

H20. The general problem of boundary values

H21. Proof of the existence of linear differential equations having a prescribed monodromic group

H22. Uniformization of analytic relations by means of automorphic functions

H23. Further development of the methods of the calculus of variations

H19-H23 involve statements of the following rough form (and sometimes simpler):

(\forall continuous objects α) (if there exist continuous objects β such that $P(\alpha, \beta)$, then there exist continuous objects γ such that $Q(\alpha, \gamma)$, which is unique with respect to some equivalence relation R).

Generally speaking, it is clear that statements of this kind are Π^1_2 . There is the opportunity for reduction from Π^1_2 using some significant mathematics not presupposing the proof or refutation, if any exist at this time. But far more likely is that if such a statement is proved or refuted, then an interesting stronger statement is really what is proved or refuted, and that the interesting stronger statement is considerably more concrete - perhaps even Π^0_2 or Π^0_1 .

We may encounter statements with an additional logical complication:

(\forall continuous objects α) (if there exist continuous objects β such that $P(\alpha, \beta)$, then there exist continuous objects γ such that $Q(\alpha, \gamma)$, which is related to all continuous objects γ' such that $Q(\alpha, \gamma)$ by some relation R).

Because R may not be an equivalence relation (it may, for example, be a maximality condition), such a statement may be only Π^1_3 or higher. Again, there are opportunities for reduction from Π^1_3 (or higher), and particularly so in terms of finding an interesting stronger statement that is far more concrete.

The many issues that arise in terms of a logical analysis of H19 - H23 are too varied and delicate to be appropriately dealt with here.