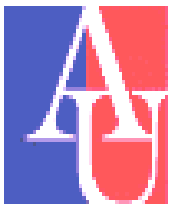

AMERICAN UNIVERSITY

WASHINGTON, DC

Automorphisms of Models of Arithmetic

Michael H. Cassel

Advisor: Ali Enayat

May 2013

Technical Report No. 2013-4

https://doi.org/10.17606/w460-2520

AUTOMORPHISMS OF MODELS OF ARITHMETIC

MICHAEL H. CASSEL

Written in Partial Fulfillment of the Requirements for the Degree of Master of Arts in Mathematics at American University.

Date: 05/09/2013.

CONTENTS

1. INTRODUCTION

Mathematics has a way of creating bizarre connections between seemingly disparate subjects. One of those bizarre connections is in the study of automorphisms of models of arithmetic, which links ideas from arithmetic, mathematical logic, abstract algebra, permutation group theory, and even some topology. The fact that there even can be automorphisms of models of arithmetic is somewhat surprising, but under nice conditions they turn out to not only exist in abundance, but to have a metrizable topological group structure.

The theory of arithmetic is motivated by trying to express the behavior of the natural numbers as a set of logical axioms. Arithmetic being a rather fundamental aspect of mathematics, it has been well-studied by logicians. The reader is probably familiar with Gödel's Incompleteness Theorems, which are really results in the theory of arithmetic. And while those theorems state that any theory that can effectively perform arithmetic is too strong to be both complete and consistent, it turns out that any such theory is also too weak in a certain sense as well. It turns out that other objects that are not the natural numbers also satisfy the theory of arithmetic. This is the starting point for the study of what exactly these other objects are - the study of nonstandard models of arithmetic.

The goal of this thesis is to exposit the key results of the subject, with an eye towards presenting two open problems related to the structure of the groups of automorphisms of a model of arithmetic. Section 2 will present preliminary results and definitions, discussing the axioms of Peano Arithmetic (PA), and deriving key theorems in the model theory of arithmetic. Section 3 will discuss recursive saturation, which is the key to building automorphisms of models of arithmetic. Essentially, recursive saturation is all about building models "just rich enough" to have many elements that are free to move under an automorphism. Finally, Section 4

will cover results at the cutting edge[1] of the subject, and present two open problems.

2. Preliminaries

2.1. **Definitions.** For the purposes of this paper, we adopt the following conventions:

- Caligraphic letters like $\mathcal{M}$ denote structures and models where the normal font equivalent, M denotes the underlying set. $\mathcal{L}$ with various subscripts denotes a language. $\mathcal{L}_{\mathrm{A}}$ refers to the language of arithmetic. When needed to be made explicit, we superscript an element with the model or set it belongs to.
- The letter $\mathcal{N}$ refers to the standard model of arithmetic, $(\mathbb{N}, +, \times, <, 0, 1)$ all being interpreted in the usual way.
- The notation $\bar{x}$ is an abbreviation for a tuple of elements $(x_0, x_1, ...x_{n-1})$, with the length of the tuple being clear by context.
- The symbols $\prec$ and $\succ$ mean that a structure is either an elementary extension or an elementary substructure of another.
- The complexity or hierarchy of a formula is related to the level of quantifier alternation. A formula is Δ_0 if the only quantifiers that occur in the formula are bounded, meaning that the quantifier is of the form $\exists x \leq t$ or $\forall x \leq t$, where t is a term that does not depend on x. For $n = 0$, $\Delta_0 = \Sigma_0 = \Pi_0$. A formula is of the form Σ_{n+1} if it is of the form $\exists \bar{y} \phi(x, \bar{y})$ where $\phi(x, \bar{y})$ is Π_n. A formula is of the form Π_{n+1} if it is of the form $\forall \bar{y} \phi(x, \bar{y})$ where $\phi(x, \bar{y})$ is Σ_n. By way of example, the formula $\forall x \exists y (x > y)$ would be a Π_2 formula. Of course, any formula can be expanded by meaningless quantifiers, so the really important classification of a formula is the lowest level of the hierarchy which

[1] As in, the author was alive when they were published.

contains a formula logically equivalent to the one in question.

- Unless explicitly stated otherwise, all models are countable. While many of the results do go through in higher cardinalities, we do not examine those here.
- We take the meta-theory to be ZFC, Zermelo-Fraenkel Set Theory with the Axiom of Choice, although this is significantly more powerful than strictly needed for most results.
- For each countable model $\mathcal{M} \vDash T$, $\mathrm{Type}(\mathcal{M})$ is the set of complete 1-types realized in $\mathcal{M}$, while $\mathrm{Type}(T)$ is the collection of complete 1-types realized in some model of T. In other words,

$$\mathrm{Type}(T) = \cup\{\mathrm{Type}(\mathcal{M}) | \mathcal{M} \vDash T\}$$

- The sequence coded by an element x is denoted as (x), and the n^{th} member of that sequence is denoted as $(x)_n$.

This thesis focuses on models of Peano Arithmetic (abbreviated PA), so we begin with that.

Definition 1. We define $\mathcal{L}_{\mathrm{A}}$ as the language of arithmetic, which consists of the function symbols $+, \times$, the relation $<$, and the constant symbols $0, 1$. The most common structure for $\mathcal{L}_{\mathrm{A}}$ is the natural numbers $\mathbb{N}$.

Definition 2. [12] PA refers to Peano Arithmetic. Peano Arithmetic is the axiom schema for arithmetic. There are many equivalent axiomatizations of PA, so the particular form the axioms take is not particularly important. We give one of them here, but by no means is this axiomatization canonical.

$$\begin{aligned}
PA1: &\quad \forall x, y, z[(x + y) + z = x + (y + z)] \\
PA2: &\quad \forall x, y[x + y = y + x] \\
PA3: &\quad \forall x, y, z[x \cdot y = y \cdot x] \\
PA4: &\quad \forall x, y, z, [x \cdot y = y \cdot x] \\
PA5: &\quad \forall x, y, z[x \cdot (y + z) = (x \cdot y) + (x \cdot z)]
\end{aligned}$$

$PA6: \quad \forall x[x + 0 = x]$
$PA7: \quad \forall x[x \cdot 0 = 0]$
$PA8: \quad \forall x[x \cdot 1 = x]$
$PA9: \quad \forall x \neg [x < x]$
$PA10: \ \forall x, y[x < y \vee x = y \vee y < x]$
$PA11: \ \forall x, y, z[x < y \wedge y < z \rightarrow x < z]$
$PA12: \ \forall x, y, z, [x < y \rightarrow x + z < y + z]$
$PA13: \ \forall x, y, z, [0 < z \wedge x < y \rightarrow x \cdot z < y \cdot z]$
$PA14: \ \forall x, y[x < y \rightarrow \exists z(x + z) = y]$
$PA15: \ \forall x[x = 0 \vee 0 < x]$
$PA16: \ \forall x[0 < x \rightarrow x = 1 \vee 1 < x]$

These axioms form the theory PA^-. The last "axiom" of PA is not really an axiom - it is an axiom schema. For each formula $\varphi(x, \bar{y})$, the axiom of induction on x in $\varphi(x, \bar{y})$, $I_x\varphi$ is the sentence:

$$\forall \bar{y}(\varphi(0, \bar{y}) \wedge \forall x(\varphi(x, \bar{y}) \rightarrow \varphi(x + 1, \bar{y})) \rightarrow \forall x \varphi(x, \bar{y}))$$

$I_x\varphi$ states that if φ is a formula (potentially with parameters $\bar{y}$), such that φ holds for 0 and if for every x, if φ holds for x, then φ holds for $x+1$, then φ holds for all x. The last "axiom" is to include $I_x\varphi$ for every formula φ in $\mathcal{L}_{\mathrm{A}}$. This cannot be written as a single axiom because there are infinitely many formulas of $\mathcal{L}_{\mathrm{A}}$.[3][2]

PA^- is best thought of as the theory of the non-negative parts of discretely ordered rings. By discrete ordering, we mean that there is a first element, and every element has an immediate successor,

[2]This induction axiom schema is extremely powerful, as well as somewhat unnatural, and much research has been done on weaker theories than full PA as a result. Some of the most common ones, in addition to PA^-, are $I\Delta_0$, induction for formulas with at most bounded quantifiers, as well as $I\Sigma_1$ and $I\Pi_1$, induction on formulas with an unbounded existential quantifier or unbounded universal quantifier, respectively. $I\Delta_0$ has a special name called "bounded arithmetic," which is of particular interest as a so called "weak fragment" of PA. It is also provable that there is no finite axiomatization of PA - in other words, this infinite axiomatization is no "worse" than any other axiomatization of PA.

and if nonzero, also an immediate predecessor. Likewise, the ring axioms as applied to the positive parts also hold - for instance $\forall x, y, z(x \leq y \rightarrow zx \leq zy)$, and $\forall x, y, z(x \leq y \rightarrow z + x \leq z + y)$. In fact there are models of PA^- that do not outwardly resemble arithmetic.[3]

An obvious question is: Just how weak is PA^-? It would be nice if PA^- proved enough of arithmetic such that we would not have to bother with full PA. As it turns out, PA^- fails to prove many basic arithmetical truths. The easiest way to demonstrate this fact is to create a model of PA^- that fails to satisfy a very basic property in arithmetic: that every number is either even or odd.

Consider the ring $\mathbb{Z}[X]$, the ring of polynomials with coefficients from $\mathbb{Z}$. $\mathbb{Z}[X]$ can be represented in $\mathcal{L}_{\mathrm{A}}$ by defining the order $<$ such that for $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ with $a_n \neq 0$, then we define $a_0 + a_1X + \cdots + a_nX^n > 0$ iff $a_n > 0$. Given any two polynomials $p, q \in \mathbb{Z}[X]$, we define $p > q$ iff $p - q > 0$, subtraction here being the usual polynomial subtraction. Then we can define $\mathbb{Z}^+[X]$ to be the ring of non-negative polynomials in $\mathbb{Z}[X]$, in other words all the polynomials greater than or equal to 0 under the ordering just defined. It turns out that this ring can be verified to satisfy PA^- since the axioms are either satisfied by the order just defined or by the fact that $\mathbb{Z}[X]$ is a ring. However,[3]

$$\mathbb{N} \vDash \forall x \exists y(2y = x \vee 2y + 1 = x)$$

This is demonstrably false in $\mathbb{Z}^+[X]$ by the simple example of the polynomials $X + 0$ and $X - 1$ being indivisible by anything except themselves. Therefore PA^- fails to prove the basic fact that every number is either even or odd. Full PA by contrast has more than enough strength to prove this statement - for any $m \in M$, M being a structure satisfying PA, $2 \times 0 = 0$, and if m satisfies the "even-odd property", then either $2 \times y = m$, or $2 \times y + 1 = m$.

[3]The pedantic reader may note that 2, or more generally any n are not defined symbols in our language, but we can treat them as abbreviations for the term (expressible in $\mathcal{L}_{\mathrm{A}}$) $\overbrace{1 + 1 + 1 + \ldots}^{n-times}$, and sometimes denoted as $\underline{2}$, or $\underline{n}$.

Thus either $m + 1 = 2 \times y + 1$, or $m + 1 = 2 \times y + 2$. However, by $PA5$, the latter statement is equivalent to $m + 1 = 2 \times (y + 1)$. Either way, the "even-odd" property holds in every model of PA, and thus $\mathbb{Z}^+[X]$ is not a model of PA. Heuristically, PA proves everything that it is supposed to - basic arithmetical truths are satisfied in all models of PA.

Definition 3. A model of arithmetic is a mathematical structure that interprets the formal language of arithmetic, and satisfies the axioms of PA. We also deal with models of PA^- and certain other variants of PA as well. The set $\mathbb{N}$, along with interpreting $<, +, \times, 0,$ and 1 in the usual way is a model of PA, and we refer to it as $\mathcal{N}$. [3]

We now begin by stating the two fundamental theorems of mathematical logic. While Gödel's *incompleteness* results get most of the attention, the completeness theorem is the practically important one. While there are many different equivalent formulations of these theorems, they all express extremely deep facts about mathematical logic, and provide a partial justification for the primacy of first order logic. In fact, first order logic is the strongest logic where completeness and compactness hold, and thus the primary reason why higher order logics are problematic. Compactness is especially useful as a tool in this thesis because it lets us exploit the weaknesses of first order logic to create new models with desirable properties.

Theorem 4. *(Compactness) A set of first order sentences has a model if and only if every finite subset of those sentences has a model.*[3]

Theorem 5. *(Gödel Completeness) Every consistent, countable theory has a finite or countable model.*[4]

[4]In general, both of these theorems are equivalent to each other and to weak versions of the axiom of choice. For countable languages, there are actually no choice requirements, and both theorems are provable from ZF alone. For uncountable languages, both theorems hold with a weak form of the axiom of choice, the most famous of the equivalent formulations being the Boolean

The next result is one of the key theorems of model theory, albeit one with some disturbing consequences. Essentially, it states that logical theories T cannot specify the cardinality of their models, and that while there are countable models of arithmetic, there are also uncountable models of arithmetic. Even more disturbingly, theories such as $\mathrm{Th}(\mathbb{R})$, the theory of the real numbers, in a countable language have a countable model according to this theorem. In other words, from a first order perspective there are countable sets that satisfy the exact same sentences as the real numbers.

Theorem 6. *(Löwenheim-Skolem) For every infinite model $\mathcal{M}$ in a language $\mathcal{L}$ with cardinality σ, and every cardinal $\kappa \geq \sigma$, there is a model $\mathcal{R}$ of cardinality κ such that if $|\mathcal{M}| \leq \kappa$, then $\mathcal{M}$ is an elementary submodel of $\mathcal{R}$, and if $|\mathcal{M}| \geq \kappa$, then $\mathcal{R}$ is an elementary submodel of $\mathcal{M}$. (Alternately, $\mathcal{M}$ is an elementary extension of*

---

prime ideal theorem, which states that every Boolean algebra contains a prime ideal.

The prettiest proof of compactness, which hides most of the topology needed in the other proofs, involves ultraproducts, at the expense of using the full axiom of choice instead of its weak variants. The statement that if a theory has a model, then any finite subset of it has a model is trivial - we prove the other direction.
That proof proceeds by considering a language $\mathcal{L}$, and letting Σ be the set of sentences of $\mathcal{L}$. We let $I = [\Sigma]^{\aleph_0}$, the collection of all countable subsets of Σ, and for each $i \in I$, let $\mathcal{M}_i$ be a model of i. (Note here that the $i's$ are themselves sets of sentences.) For each $\sigma \in \Sigma$, we let $\hat{\sigma}$ be the set of all $i \in I$ such that $\sigma \in I$. Then the set

$$E = \{\hat{\sigma} : \sigma \in \Sigma\}$$

has the finite intersection property (the intersection of any finite collection of sets of E being non-empty) because $\{\sigma_1, \ldots, \sigma_n\} \in \hat{\sigma}_1 \cap \ldots \cap \hat{\sigma}_n$. Therefore E is a filter over I. By the ultrafilter theorem, E is extendable to an ultrafilter D over I. If $i \in \hat{\sigma}$, $\sigma \in i$, therefore $\mathcal{M}_i \vDash \sigma$. Therefore, for each $\sigma \in \Sigma$,

$$\{i \in I : \mathcal{M}_i \vDash \sigma\} \supseteq \hat{\sigma}$$

And since $\hat{\sigma} \in D$,

$$\{i \in I : \mathcal{M}_i \vDash \sigma\} \in D$$

since D being an ultrafilter must contain any set X for which $\hat{\sigma} \subseteq X \subseteq I$. Therefore by the fundamental theorem of ultraproducts (which is choice dependent),

$$\prod_{i \in I} \mathcal{M}_i / D \vDash \Sigma$$

as desired. [11, 1]

$\mathcal{R}$.) If the language $\mathcal{L}$ is countable, then every infinite model $\mathcal{M}$ in the language $\mathcal{L}$ has elementarily equivalent[5] models in every cardinality.

This is a key result for us since it allows us to strengthen the compactness theorem slightly, by permitting us to treat the model created by compactness as countable.

2.2. **Existence of nonstandard models.** This section discusses how to justify the existence of nonstandard models of arithmetic. We begin by constructing one nonstandard (i.e. not $\mathcal{N}$) model of arithmetic, and then discuss how to construct many such models. The key tools we use in these constructions are the compactness theorem, and Gödel's Incompleteness Theorem. We end by proving that while there are continuum many distinct models of PA that do not satisfy all of the same sentences as $\mathbb{N}$, there are also continuum many distinct models of $\mathrm{Th}(\mathbb{N})$, or of any other completion of PA.

2.2.1. *Existence of nonstandard models via compactness.*

Theorem 7. *There is a countable model of arithmetic that is not $\mathcal{N}$, and is thus "nonstandard."*

Proof. From theorem 4, we see that if we can exhibit a set of first order sentences such that every finite subset of those sentences is satisfiable, then a model exists that has to satisfy all of the sentences.

[5]Whenever we use the word "elementary", we don't mean something is easy! Elementary equivalence means that two models satisfy the same first order sentences, and so whenever the word "elementary" appears as a descriptor we mean it in this sense. This is a strictly weaker condition than two models being isomorphic. One way to see this is as an immediate consequence from Lowenheim-Skolem Theorem, which states that theories have elementarily equivalent models in different cardinalities, which can't possibly be isomorphic because of the absence of a bijective map between them. Another way to understand the difference is that isomorphisms require that an element and its image under isomorphism must satisfy the exact same formulas - elementary equivalence only requires that some element satisfy those formulas. Formally, isomorphisms preserve types (we'll define those in a bit), while elementary equivalence provides no such guarantee.

Therefore, we can create a model by starting with $\mathrm{Th}(\mathbb{N})$, the theory of the natural numbers. In addition, we expand the language of arithmetic by adding a constant symbol c. This is all first-order sentences that are true about $\mathbb{N}$, and add the following additional sentences.

$$\phi_1 : c > 1$$

$$\phi_2 : c > 2$$

$$\vdots$$

$$\phi_n : c > n$$

$$\vdots$$

Every finite subset of these sentences is satisfiable by the standard model $\mathcal{N}$ itself, because $\mathcal{N}$ satisfies $\mathrm{Th}(\mathbb{N})$, and for any finite set of the additional ϕ sentences, c can be interpreted so as to satisfy all of them - if the last ϕ sentence included is ϕ_m, then the element $c = \underline{m+1}$ satisfies all the included ϕ sentences. Therefore, by compactness there has to be a countable model that satisfies all the ϕ sentences as well as $\mathrm{Th}(\mathbb{N})$. This model cannot be the standard model, as $\mathbb{N}$ does not have an element larger than everything in itself.

Therefore, we have created a model $\mathcal{M}$ that satisfies $\mathrm{Th}(\mathbb{N})$ (and thus PA), but is not $\mathcal{N}$. While this model is in the expanded language, the reduct of the model it by omitting explicit reference to c in the language is still a model of PA and is not $\mathcal{N}$. However, compactness is just an existence result - it tells us nothing about the underlying structure of the model, although some structure can be gleaned from the proof in footnote 5. □

Theorem 8. *There are continuum-many countable models of* $\mathrm{Th}(\mathbb{N})$.

Proof. We can repeat a similar compactness argument as above, but in a slightly different form. We define the formulas

$$\varphi_n = \text{"The } n^{th} \text{ prime divides } c\text{"}$$

Each of these formulas can be implemented in $\mathcal{L}_{\mathrm{A}} \cup \{c\}$. A set of formulas in n free variables is called an n-type. A complete $n-$type is a type that is maximal with respect to inclusion, i.e every formula or its negation is included in the type, and we recall that we denote the set of all the complete 1-types of a model by $\mathrm{Type}(\mathcal{M})$, and all the complete 1-types of all models of a theory by $\mathrm{Type}(T)$. An sequence of elements (or in a 1-type, just an element) realizes a type, if when that sequence of elements is substituted for the free variables in the type, then all the formulas in the type are satisfied.

We show that there are uncountably many 1-types expressible from the $\varphi_n's$. Consider that for a given 1-type Σ, Σ can either include φ_n, or include the negation of φ_n. Therefore Σ can be seen as a map from the set of $\varphi_n's$ to 0 or 1 - 1 if the formula is included in the type and 0 if it is not. Therefore we have precisely $2^{\aleph_0}$ distinct types. Each of these types is finitely satisfiable because for any finite combination of these sentences, there are many elements of $\mathbb{N}$ that could have the desired property.[6]

Therefore by compactness, there exist models of $\mathrm{Th}(\mathbb{N})$ that realize each distinct 1-type. Moreover, each countable model created in this way could realize at most countably many of the 1-types, because to realize each different type requires a different element (no element could be both divided and not divided by the n^{th} prime). Yet we had stated that $\mathrm{Type}(T) = 2^{\aleph_0}$.

We define an equivalence relation on all of these models by $\mathcal{M} \sim \mathcal{M}'$ iff $\mathrm{Type}(\mathcal{M}) = \mathrm{Type}(\mathcal{M}')$, and moreover see that if two models don't realize the same types, they can't be isomorphic[7].

[6]For instance, an element that satisfies the first 4 $\varphi_n's$ would be $2 \cdot 3 \cdot 5 \cdot 7$.

[7]For two models to be isomorphic, an element and its image under isomorphism must satisfy the same formulas. Therefore if some type Γ is realized in $\mathcal{M}$ but not in $\mathcal{M}'$, then some element c must realize Γ in $\mathcal{M}$, and there is no element $f(c)$ that realizes Γ in $\mathcal{M}'$.

And since each of the different models created via the compactness argument can realize only countably many types, each model could share the same types with only countably many others. Therefore, the size of each $[\mathcal{M}]$ is countable.

It is a theorem of ZFC that if $\mathscr{A}$ is a family of countable subsets of a set X such that $\cup\mathscr{A} = X$, where X is of size continuum, then $\mathscr{A}$ is also of size continuum[8]. That is precisely the situation here - each $[\mathcal{M}]$ is countable, and therefore there must be continuum many equivalence classes $[\mathcal{M}]$. Therefore we have established that there are continuum-many non-isomorphic models of $\mathrm{Th}(\mathbb{N})$. □

2.2.2. *Existence via Gödel Incompleteness.* Another method of demonstrating the existence of nonstandard models of Arithmetic is to utilize perhaps the best known result in Mathematical Logic - the theorem of Gödel that PA is incomplete.[9]

Theorem 9. *(Gödel Incompleteness) If PA is consistent, then there is a sentence σ such that neither $PA \vdash \sigma$ nor $PA \vdash \neg\sigma$. Moreover, any finite extension T of PA also has a sentence τ such that neither $T \vdash \tau$ nor $T \vdash \neg\tau$.* [10]

[8]To see this result, consider that $|\cup\mathscr{A}| \leq |\mathscr{A}| \cdot \aleph_0$ because each member of the union is a countable set. Therefore $2^{\aleph_0} \leq |\mathscr{A}| \cdot \aleph_0$, which by cardinal arithmetic forces $|\mathscr{A}| \geq 2^{\aleph_0}$. Let $[X]^{\aleph_0}$ be the full collection of countable subsets of X, then $|[X]^{\aleph_0}| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. Since $\mathscr{A} \subseteq [X]^{\aleph_0}$, $|\mathscr{A}| = 2^{\aleph_0}$.

[9]The result presented in this section also goes through for PA^- and many other theories weaker than PA. Gödel's Incompleteness Theorems are sometimes erroneously thought to rest on the induction axiom schema of PA. They actually hinge on the ability of the theory to prove "enough" of the theory of the natural numbers, along with having the axioms of the theory be "effectively generated", or "recursively enumerable." Both PA^- and Robinson arithmetic (also known as Q) satisfy these conditions. (In fact it should not be surprising that PA^- and Q are incomplete since they are in the same language as PA but are much weaker.) An example of a theory that is sufficiently weak to avoid incompleteness is Presburger arithmetic, which essentially removes multiplication and the ordering relation from $\mathcal{L}_{\mathrm{A}}$ and the corresponding axioms from PA, but retains induction - this theory is provably consistent, complete, and decidable.

[10]We explicitly avoid presenting a proof of this theorem, even though it is not terribly far afield, because this thesis is not about Gödel's Theorems, their philosophical implications, or the countless other conundrums generated by

Corollary 10. *Let $T \supseteq PA$ be at most a finite extension of PA. Then T has $2^{\aleph_0}$ complete countable extensions.*

Proof. Because T is incomplete, there are sentences σ such that $T \cup \{\sigma\}$ and $T \cup \{\neg\sigma\}$ are both consistent, such that models exist for both. We create the following tree of theories, where s is some sequence of 0s and 1s:

$$T_\emptyset = T$$

$$T_{s0} = T_s + \sigma_{T_s}$$

$$T_{s1} = T_s + \neg\sigma_{T_s}$$

For each function $f : \mathbb{N} \to \{0, 1\}$, let T_f be $\cup_{n\in\mathbb{N}} T_{f\restriction n}$, where $f \restriction n$ is the finite sequence $f(0)$, $f(1)$, $f(2)$, ..., $f(n-1)$, of 0s and 1s. Each T_f is consistent by construction, and therefore each T_f can be extended to a complete consistent theory T'_f. Then, we'd like to demonstrate that if $f \neq g$, then $T'_f \neq T'_g$. Since there are $2^{\aleph_0}$ distinct functions from $\mathbb{N} \to \{0, 1\}$, this suffices. Again the nature of our construction comes into play here - if $f \neq g$, then there is a first n where they disagree - in other words $f \restriction n = g \restriction n$ but $f(n) \neq g(n)$, and therefore T_f and T_g disagree on $\sigma_{T_{f\restriction n}}$, thus requiring $T'_f \neq T'_g$, as desired.[3]

Each of these theories has a countable model by completeness, thus producing $2^{\aleph_0}$ non-elementarily equivalent (and thus non-isomorphic) countable models of PA. Only one of these theories could be $\mathrm{Th}(\mathbb{N})$, so the rest of the countable models produced in this way cannot be isomorphic to $\mathcal{N}$ and are thus nonstandard. □

them. There are other interesting subjects in models of arithmetic besides Gödel. This section is really meant to be a minor digression into proving existence of nonstandard models of arithmetic, and not an investigation into the rather laborious machinery used to prove these theorems.

Remark 11. By Corollaries 8 and 10, we achieve the satisfying result that there $2^{\aleph_0}$ pairwise non-elementarily equivalent countable models of arithmetic, with each of those having $2^{\aleph_0}$ elementarily equivalent but pairwise non-isomorphic models.

2.2.3. *An explicit construction of a nonstandard model of arithmetic using definable ultrapowers.* This section is a slight digression in that it relies on tools that are not used in automorphisms of models of arithmetic. That said, it provides a useful look at the notion of definability, a subject which is of critical importance for automorphisms.

From above we have the notion of a definable set, and thus definable functions. Because the number of formulas in $\mathcal{L}_{\mathrm{A}}$ is countable, and every definable function is equivalent to a formula of $\mathcal{L}_{\mathrm{A}}$, the number of definable functions and definable sets in every model of arithmetic is countable.

We let $\mathfrak{B}$ be the Boolean Algebra of Sets of definable sets of $\mathbb{N}$, and let U be an ultrafilter over $\mathfrak{B}$. We let $\mathfrak{F}$ be the family of functions from $\mathbb{N} \to \mathbb{N}$ that are definable from $\mathcal{N}$. Then we form the ultrapower:

$$\mathcal{M}^* = \prod_{\mathfrak{F},U} \mathcal{N}$$

We see that the universe of M^* is

$$\{[f] : f \in \mathfrak{F}\}$$

where

$$f \sim g \iff \{n \in \mathbb{N} : f(n) = g(n)\} \in U$$

We make two remarks at this point. First, without the restriction to definable functions, this ultrapower would be uncountable. The universe would be all functions from $\mathbb{N} \to \mathbb{N}$, which is uncountable. Although it is not a trivial argument, the equivalence relation formed by a non-trivial ultrafilter will not change the uncountability.[11] Secondly, while in general with ultrapowers U is

[11]Suppose the set of all equivalence classes $E := \{[f]_U | f \in \mathbb{N}^{\mathbb{N}}\}$, the set of equivalence classes of functions from $\mathbb{N}$ to $\mathbb{N}$ under a non-trivial ultrafilter U,

left inexplicit, on $\mathbb{N}$ any ultrafilter contains the Frechet filter, or all co-finite sets. All cofinite sets are definable in $\mathbb{N}$ by a formula expressing that x is not equal to a finite list of things, so therefore these sets are in $\mathfrak{B}$. And this U can be made into an ultrafilter.[12]

$\mathcal{M}^*$ is a model of arithmetic, and we can see that it is non-isomorphic to $\mathcal{N}$ because of the presence of the id function, which sends the first copy of $\mathcal{N}$ to 1, the second copy of $\mathcal{N}$ to 2, and so on. $\mathcal{M}^*$ contains an initial segment isomorphic to $\mathcal{N}$ since the functions $[0]$, $[1]$, $[2]$ (which assign $0, 1, 2$ to each copy of $\mathcal{N}$) are easily shown to be isomorphic to $\mathbb{N}$. However, $\mathcal{M}^*$ contains the function id, which assigns 0 to the first copy of $\mathcal{N}$, 1 to the second copy of $\mathcal{N}$, and so on. This function is larger than everything in the initial segment. It is easy to prove $[id] > [n]$ since from the set of places where $[id] > n$ is cofinite, and thus in U. [2]

In fact, very little of our discussion depended on $\mathcal{M}$. If we modify the hypotheses of this discussion to require that, if $\mathcal{M}$ is a model of arithmetic, if we let $\mathfrak{B}$ be the algebra of sets definable

---

was countable. Then we could form an enumeration of them, $[f_1], [f_2], [f_3], \ldots$ with representative members f_1, f_2, f_3, $\ldots$, and create a new function g by a diagonalization type argument:

$$g(1) = f_1(1) + 1$$

$$g(2) = f_1(2) + f_2(2) + 1$$

$$g(n) = f_1(n) + f_2(n) + \ldots + f_n(n) + 1$$

By construction g is guaranteed to disagree with f_k for all $n \geq k$. This is the key use of non-trivial ultrafilters: since g and f_k disagree on a co-finite set, $[g] \neq [f_k]$ since an non-trivial ultrafilter on $\mathbb{N}$ must contain all co-finite sets. Therefore we have created a $[g]$ not listed in the enumeration, and thus the set of equivalence classes E could not have been countable.

[12]Consider we can show that the set of all cofinite sets is a filter F. First, the empty set is not a member of F, if A and B are definable sets, A is cofinite, and a subset of B, then B clearly is cofinite itself and thus in U. If A and B are cofinite, then their intersection must also be cofinite. Only the last condition on ultrafilters poses difficulty - there are definable sets that are neither finite nor cofinite - an obvious example is the even numbers. However, we can use the classic result of ultrafilters that every filter is extendable to an ultrafilter. Although there are also explicit constructions for U, we don't need anything nearly as powerful here. We can be satisfied with making sure U contains F, and thus contains all cofinite sets.

with parameters, and $\mathfrak{F}$ be set of definable functions with parameters, then we can prove the MacDowell-Specker Theorem, a result we reach later via more standard techniques.

Theorem 12. *(Countable MacDowell-Specker Theorem via Ultraproducts) Every countable model of PA has an elementary end extension.*

Proof. The key is the in the construction of the ultrafilter. In the $\mathcal{N}$ case, every definable function with bounded range ended up equivalent to some constant function, since it had to be below some $[n]$ function, and we had already stated that the $[n]$ functions formed an initial segment isomorphic to $\mathbb{N}$. That concept can be extended for an arbitrary model $\mathcal{M}$, to construct a U such that every definable map with a bounded range is constant on a member of U. Then by precisely the argument that $[id]$ was greater than all the constant functions, that once again is the case here. $\mathcal{M}$ forms an initial segment of the new $\mathcal{M}^*$ by the constant functions, and the new $[id]$ function must be greater than all such constant functions. Therefore $\mathcal{M}^*$ is an elementary end extension not isomorphic to $\mathcal{M}$. [2] □

2.3. **What happens in non-standard models.**

2.3.1. *Basic results of nonstandard models.* One of the key early results of nonstandard models is to look at the order type of all such models. We can prove that all models of arithmetic take the form $\mathbb{N} + \mathbb{Z}\mathbb{Q}$, or a copy of the natural numbers, then a dense copy of the integers.

Definition 13. If $\mathcal{M}$ and $\mathcal{R}$ are two $\mathcal{L}_{\mathrm{A}}$ structures with $\mathcal{R}$ a substructure of $\mathcal{M}$, and every element of $\mathcal{M} \backslash \mathcal{R}$ is greater than every element of $\mathcal{R}$, then $\mathcal{R}$ is an initial segment of $\mathcal{M}$ and $\mathcal{M}$ is an end-extension of $\mathcal{R}$. If $\mathcal{R} \neq \mathcal{M}$, then $\mathcal{R}$ is a proper initial segment of $\mathcal{M}$. If $\mathcal{R}$ is cofinal in $\mathcal{M}$, then $\mathcal{M}$ is a cofinal extension of $\mathcal{R}$. [3]

Definition 14. A cut of a model of arithmetic is a subset of the model that is closed under the successor operation. A proper cut is a proper subset of the model that is a cut. [3]

Definition 15. A injective map between two models $\mathcal{M}$ and $\mathcal{R}$ that preserves functions, relations, and formulas is called an elementary embedding. [1]

Definition 16. A set $A \subseteq M$ is definable in $\mathcal{M}$ if there is some formula $\varphi(x)$ such that $a \in A \iff \mathcal{M} \vDash \varphi(a)$. A set A is definable *with parameters from* B if there is a formula $\varphi(x, \bar{y})$ such that $a \in A \iff \mathcal{M} \vDash \varphi(a, \bar{b})$. [3]

Theorem 17. *All models of arithmetic have an initial segment isomorphic to* $\mathcal{N}$.

Proof. The axioms of PA^- show that the map $n \to \underline{n}^M$ respects addition, multiplication, and ordering[13]. Because it respects ordering, the map must also be an embedding (one-to-one) since $\mathcal{N}$ is discretely ordered. Finally, to show that this map actually creates an initial segment, consider that we can show that for all $k \in \mathbb{N}$, $PA^- \vdash \forall x(x \leq k \to x = \underline{0} \vee x = \underline{1} \vee \cdots \vee x = \underline{k})$ because the base case ($k = 0$) is trivial, and since $PA^- \vdash \forall x, y(y > x \to y \geq x + 1)$, which makes the induction case hold. Therefore the image of this map, $N = \{\underline{n}^M | n \in \mathbb{N}\}$ is an initial segment of $\mathcal{M}$. [3] □

The upshot of this theorem is that we can talk about the natural numbers in any nonstandard model of arithmetic, or even models of weaker theories like PA^- without ambiguity - even though they may be called something else when interpreted in that particular model, they are isomorphic to $\mathcal{N}$.

Theorem 18. *All countable nonstandard models of* PA *take the form* $\mathbb{N} + \mathbb{Z}\mathbb{Q}$.

[13]Formally, consider that if $n, l, k \in \mathbb{N}$ and $n = l + k$, then $PA^- \vdash \underline{n} = \underline{l} + \underline{k}$ since if $k = 0$, $PA6$ achieves the desired result, and the rest follows by simple induction and $PA1$ (only needed to stage $\underline{n}$ at most, as opposed to infinite induction, which requires full PA). Likewise, if $n = l \cdot k$, then $PA^- \vdash \underline{n} = \underline{l} \cdot \underline{k}$ by the fact that if $k = 0$, $PA6$ carries the day. Then if PA^- proves that $\underline{n} = \underline{l} \cdot \underline{k}$, then for $k' = k + 1$ and $n' = n + l$, then $PA^- \vdash \underline{l} \cdot (\underline{k} + 1) = \underline{l} \cdot \underline{k} + \underline{l}$ by $PA5$ and $PA7$, and thus $PA^- \vDash \underline{l} \cdot \underline{k}' = \underline{n} + \underline{l}$, and thus $PA^- \vdash \underline{l} \cdot \underline{k}' = n'$. And if $n < k$, then PA^- proves $\underline{n} < \underline{k}$ again by induction on k and $PA14$, $PA11$, and $PA8$.

Proof. Let $\mathcal{M}$ be a nonstandard model of PA. The elements $0, 1, 2, ..$ are an initial segment of $\mathcal{M}$ with order type isomorphic to $\mathbb{N}$. Therefore M is of the form $\mathbb{N} + X$, where X is some linear order. If we take some nonstandard element a, we can let the set $[a]$ as "the set of points finitely far from a", or formally,

$$\{x | \exists n \in \mathbb{N}(x + \underline{n} = a \vee a + \underline{n} = x\}$$

This is called a $\mathbb{Z}$ block of a, since a is at the center of two copies of $\mathbb{N}$, one above a and one below a. If we have another nonstandard element $b > a$, such that $b - a$ is nonstandard, then consider that $[a] \cap [b] = \emptyset$, and thus that if $x \in [a]$ and $y \in [b]$, then $x < y$. Let A be the set of all $\mathbb{Z}$ blocks. We've now shown A is linear ordered, defined as:

$$[a] < [b] \iff a \notin [b] \wedge a < b$$

This relation is reflexive, transitive, and anti-symmetrical. Likewise, A has no least element, since either $\frac{a}{2}$ or $\frac{a+1}{2}$ exists[14], is nonstandard, and is not in $[a]$ since the distance between them is either $\frac{a}{2}$ or $\frac{a-1}{2}$, both nonstandard. A has no greatest element since $[2a] > [a]$ (the distance between a and $2a$ is nonstandard.) Therefore A is a linear order without endpoints. Finally, consider that for any $[a]$, $[b]$, either $\frac{a+b}{2}$ or $\frac{a+b+1}{2}$ exists, and $[\frac{a+b}{2}]$ or $[\frac{a+b+1}{2}]$ is not $[a]$ or $[b]$ by the same distance argument. Therefore A is a dense linear order without endpoints, which is the order type of $\mathbb{Q}$. [3, 1] □

Corollary 19. *Let $\mathcal{M} \vDash PA$ be countable and nonstandard. Then M has $2^{\aleph_0}$ proper cuts I.*

Proof. Consider that by the previous result M has the order type $\mathbb{N} + \mathbb{Z}\mathbb{Q}$. Therefore if S is a cut of $\mathbb{Q}$ (in the sense that $\forall x \in S \forall y \in$

[14]To see this, we wish to prove that $PA \vDash \forall x \geq 1(2|x \vee 2|(x+1))$, where $|$ means divides as usual. While $|$ is an abbreviation it is not hard to write it as a formal statement of PA. The proof is inductive - consider that $2|2$, which is the base case. So, we assume that the result holds to n, and consider $n+1$. Suppose $2|n$. Then $2 \cdot q = n$, and $2 \cdot 1 = 2$ Therefore $2 \cdot (q+1) = n+2$ and thus $2|(n+1)+1$. Otherwise $2|(n+1)$ and we are done. Perhaps unexpectedly, this theorem actually requires more than PA^- to prove - the previously mentioned example of a model PA^- as $Z^+[x]$ fails this theorem.

$\mathbb{Q}(y < x \to y \in S)$[15], then the set $\mathbb{N} + \mathbb{Z}S$ must be a proper cut of M since $S \neq \mathbb{Q}$ and yet each $\mathbb{Z}$ block is closed under successor. In other words, each of these cuts of $\mathbb{Q}$ simply removes $\mathbb{Z}$ blocks from the end of the model. Moreover each distinct S generates a distinct cut. Finally, we see that there are uncountably many such cuts because the reals are in fact defined by each distinct cut of $\mathbb{Q}$, i.e.

$$r \to \{q \in \mathbb{Q} | q < r\}$$

□

The next results we give are related to how nonstandard models of arithmetic behave in the sense of mathematical properties transferring from initial segments to later ones, and from later ones to initial ones. These results matter a great deal because they give us some insight as to what has to be happening in these segments. Like other famous "lemmas", we adhere to convention in referring to them as lemmas although in terms of importance they should probably be Theorems.

Lemma 20. *(Overspill) Let $\mathcal{M} \vDash PA$ be non-standard and let I be a proper cut of M. Suppose $\bar{a} \in M$ and $\varphi(x, \bar{a})$ is an $\mathcal{L}_{\mathrm{A}}$ formula such that*

$$\mathcal{M} \vDash \varphi(b, \bar{a}) \textit{ for all } b \in I$$

Then there is a $c > I$ such that

$$\mathcal{M} \vDash \forall x \leq c[\varphi(x, \bar{a})]$$

Proof. The key is in the detail that I is a proper cut. Recall that a proper cut is an initial segment that also happens to be closed under successor. Any proper cut necessarily cannot be defined by a formula. Suppose it was - then

$$I = \{b \in M | \mathcal{M} \vDash \psi(b, \bar{a})\}$$

[15]The concept of cut in these remarks is intentionally used in two different senses. In fact, it is less ambiguous than it seems at first - while a cut of a model M outwardly does not look anything like the Dedekind Cut and its variants from set theory, this result actually proves that they are very alike, so the terminology is well chosen.

Then

$$\mathcal{M} \vDash \psi(0, \bar{a}) \wedge \forall x(\psi(x, \bar{a}) \rightarrow \psi(x+1, \bar{a}))$$

By the induction axiom in PA, and since I is closed under successor,

$$\mathcal{M} \vDash \forall x \psi(x, \bar{a})$$

Which contradicts the fact that I was a *proper* cut. This gives us the insight to prove overspill - suppose that the conclusion of overspill was false. Then

$$\mathcal{M} \vDash \forall y < x[\varphi(y, \bar{a})]$$

would be a definition of the proper cut. [3] □

Corollary 21. *Let $M \vDash PA$ be nonstandard and I a proper cut of M. Suppose $\varphi(x, \bar{a})$ is an $\mathcal{L}_{\mathrm{A}}$ formula with $\bar{a} \in M$, and that for all $x \in I$ there exists $y \in I$ such that*

$$\mathcal{M} \vDash y \geq x \wedge \varphi(y, \bar{a})$$

(there are unboundedly many $y \in I$ satisfying $\varphi(y, \bar{a})$. Then for each $c > I$ in M there exists $b \in M$ with $I < b < c$ and

$$\mathcal{M} \vDash \varphi(b, \bar{a})$$

(i.e. there are arbitrarily small $b > I$ satisfying $\varphi(b, \bar{a})$.

This is especially useful when $I = \mathbb{N}$, since (for instance) this gives us the ability to see results like "there are arbitrarily small nonstandard prime numbers" when I is taken to be $\mathbb{N}$ and φ a formula expressing the primality of b. More importantly though, overspill provides the key tool to ensure that logical properties holding in initial segments can be transferred to segments later in the model.

We now return briefly to the subject of proper cuts and closure properties. We have previously proven that there are $2^{\aleph_0}$ proper cuts of any countable nonstandard model M. It turns out with overspill we can prove much more. The cuts that we have previously exhibited were weak in the sense that they were closed only under successor. The proof of the order type of PA used the fact

that we could merely add to get out of each cut and get into the next one. For our purposes, it will be very useful to have cuts that are much harder to get out of - cuts that are not only closed under successor, but also addition, multiplication, and exponentiation.

Theorem 22. *Let $\mathcal{M} \vDash PA$ be countable and nonstandard. Then M has $2^{\aleph_0}$ proper cuts that are closed under $+, \cdot$, and exponentiation.*

Proof. Recall the tetration, or iterated exponentiation function, as ${}^n a = a^{\overbrace{a^{\cdot^{\cdot}}}^{n-times}}$. Instead of our equivalence relation being the finitely away relation, we now use the "finite tetration away" equivalence relation[16]

$$a \sim b \text{ iff } M \vDash b < {}^n(a+2) \vee a < {}^n(b+2) \text{ for some } n \in \mathbb{N}$$

We see that this is in fact an equivalence relation - reflexivity and symmetry come for free by our definition. The only difficulty is transitivity. We need the statement that if ${}^n(a+2) > b$, and ${}^{n'}(b+2) > c$, then there is some $m \in \mathbb{N}$ such that ${}^m(a+2) > c$. While intuitively this seems clear - it requires a bit of subtlety in the proof because exponentiation is not associative. We first need a short lemma.

Consider

$$({}^n x)^{{}^n x}$$

We would like to show that

$$({}^n x)^{{}^n x} \leq^{2n} x$$

Consider that

$$(x^{x^{x^x}})^{x^{x^{x^x}}} = x^{x^{x^x} \cdot x^{x^{x^x}}} = x^{x^{x^x} + x^{x^x}}$$

In fact, there was nothing special about our choice of $n = 4$ - a similar pattern would result for any choice of n. That similar pattern is:

[16] We use the $+2$'s to avoid pathological situations that can result from a, b, or n being 0. In the normal case that a or b is nonstandard, the $2's$ should not matter.

$$({}^{n}x)^{{}^{n}x} = x^{x^{{}^{m+1}x+{}^{m}x}}$$

where $m = n - 2$.

Consider that in general,

$${}^{m}x +^{m+1} x \leq^{2m+1} x$$

for obvious reasons. Therefore we have

$$\leq x^{x^{{}^{2m+1}x}} = x^{x^{{}^{2n-3}x}} \leq^{2n-1} x \leq^{2n} x$$

This gives us the insight to prove the result - consider that if ${}^{n'}(b+2) > c$, then

$${}^{n'}(b+2) = (b+2)^{\overbrace{(b+2)^{(b+2)^{\cdot^{\cdot^{\cdot}}}}}^{n'-times}} > c.$$

Since $b >^{n} (a+2)$

$${}^{n'}(b+2) \leq^{n} (a+2)^{{}^{n}\overbrace{(a+2)^{{}^{n}(a+2)^{\cdot^{\cdot^{\cdot}}}}}^{n'-times}} > c.$$

Consider the last two entries in this power tower are identical to the result first proved. Therefore

$$\leq^{n} (a+2)^{{}^{n}\overbrace{(a+2)^{{}^{n}(a+2)^{\cdot^{\cdot^{\cdot^{\cdot^{2n}(a+2)}}}}}}^{n'-1-times}}$$

Since n and n' are finite, this process can be iterated using a very similar argument to the original one.

$${}^{n' \cdot n}(a+2) > c$$

Therefore this is an equivalence relation, and so we can look at $A = (M \backslash [0])/\sim$. We see that A is a linearly ordered set, for largely the same reason that the finitely away relation was a linear order - if $a < b$ and $[a] \neq [b]$, then $[a] <_A [b]$.

We now set out to prove that this linear order is dense. Suppose that $[a] <_A [b]$. Then $\mathbb{N} < a < b$ (recall that we removed the first

equivalence class, which can be easily verified to correspond to $\mathbb{N}$, since finite tetrations of natural numbers are natural.) Therefore

$$M \vDash \exists x({}^{n}(a+2) < x < {}^{n}(x+2) < b$$

for each $n \in \mathbb{N}$. This heavily relies on the fact that tetration (and exponentiation) actually can be defined as formulas in PA - a subject that we will turn to in a moment. For now we can take it on faith that ${}^{n}a$ is a valid abbreviation for an actual formula of PA. As for the statement, it merely states that since a and b are more than a finite tetration away, once we fix a particular $n \in \mathbb{N}$ there must be an x between a and b such that x is more than ${}^{n}(a+2)$ and ${}^{n}(x+2) < b$. Therefore by overspill, there must be some c,$d > \mathbb{N}$ such that

$$M \vDash {}^{c}(a+2) < d < {}^{c}(d+2) < b$$

Therefore

$$[a] <_A [d] <_A [b]$$

And thus this linear order is dense. Moreover by a similar construction it is quite clear that there can be no first nor last element of this linear order - thus we have a dense linear order, which once again is the order type of $\mathbb{Q}$. Therefore each cut of $\mathbb{Q}$ induces a cut of M, and there are $2^{\aleph_0}$ such cuts.

Moreover, each of these cuts is closed under exponentiation. Take any element e in some initial segment $I = [a]$ created in this way, and without loss of generality take e. Then consider that since

$$e < {}^{n}a$$

for some n, e is in the equivalence class of a, and therefore $[a] = [e]$. Then we see that ${}^{1}e = e^e$ must be contained in $[a]$ as well.

Thus $e^e \in I$, and therefore I is closed under exponentiation. Closure under multiplication, addition, and successor is obvious from here. Therefore M has $2^{\aleph_0}$ proper cuts closed under addition, multiplication, and exponentiation, as desired. $\square$

Our next few results discuss the ability of models of arithmetic to be extended. It turns out that models of arithmetic can be extended both cofinally (that is, with every new element being below some old element), as well as end (that is, with every new element above every old element.) These results are somewhat surprising if one considers the standard model, since $\mathbb{N}$ certainly cannot be extended cofinally. The first result appears to have nothing to with extensions at all, but it turns out to be of critical importance in proving these results.

Theorem 23. *(MacDowell-Specker via standard means) Every model of arithmetic has a proper elementary end extension.*

The proof of this seminal result in nonstandard models of arithmetic requires the use of very small models. The broad idea is that if $M \prec K$ with K an end extension of M and $c \in K \backslash M$ then K satisfies the theory:

$$\{\varphi(\bar{a}) | \bar{a} \in M \vDash \varphi(\bar{a})\} \cup \{c > a | a \in M\}$$

To even state this theory requires a massive language expansion - here we add a constant that names each $a \in M$ and an additional constant c. Since K is an end extension, it has to omit at least these types:

$$p_a(x) = \{x < a\} \cup \{x \neq b | b \in M \vDash b \leq a\}$$

K fails to realize these types because there is no choice of $x \in M$ such that $x > a$ and $x < a$. Because we are omitting lots of types - at least countably many, and possibly more if our original model was uncountable, we know that at least K can't be "huge", or saturated. The goal is to define $K = K(N; M \cup \{c\})$ for some $c \in N \backslash M$. The work is in constructing N and c.

If we do find an extension $K \succ M$ with $K \supseteq_e M$, and $c \in K \backslash M$, then if we have a formula $\varphi(x, \bar{y})$ and every $\bar{b} \in M$, $K \vDash \varphi(c, \bar{b})$ means that

$$\mathcal{M} \vDash \forall z \exists x (x > z \wedge \varphi(x, \bar{b}))$$

Essentially, this is stating that if one element in the extended model K satisfies a formula, then there must be unboundedly many things that also satisfy it in the original model M. This is so because of the fact that the extension is elementary. We denote this property - that unboundedly many things satisfy a formula, as $\mathrm{Q}x\varphi(x, \bar{b})$. The needed expansion of the language we denote as $\mathcal{L}_{\mathrm{A}}(M)$, the Language of Arithmetic supplemented by constant symbols for each element of M. [3]

Proof. While a proof for the general case is given in [3], we present a proof of the countable case. Consider that since M is countable, we can enumerate all the $\mathcal{L}_{\mathrm{A}}(M)$ formulas in one free variable as $\theta_0(x), \theta_1(x), ...$ We construct a sequence of formulas $\varphi_0, \varphi_1, ...$ such that $M \vDash \mathrm{Q}x\varphi_i(x)$ for all i.

We let $\varphi_0(x)$ be

$$x = x$$

Next, for each $i \geq 0$, if $\theta_i(x)$ is $\exists y < b(\psi(x, y))$ for some ψ and some $b \in M$, then we let

$$\varphi_{i+1}(x) = \varphi_i(x) \wedge \psi(x, c) \wedge c < b$$

for some $c \in M$, or:

$$\varphi_{i+1}(x) = \varphi_i(x) \wedge \neg\theta_i(x)$$

If $\theta_i(x)$ is any other $\mathcal{L}_{\mathrm{A}}(M)$ formula,

$$\varphi_{i+1}(x) = \varphi_i(x) \wedge \theta_i(x)$$

We first show that this construction in fact means that for all φ_i, $\mathrm{Q}x\varphi_i(x)$. Consider the unbounded formula φ and the arbitrary formula θ. If θ is a bounded formula (in the sense all elements that satisfy the formula are less than some $d \in M$), then $\neg\theta$ is satisfied by all elements greater than y. Therefore $\varphi \wedge \neg\theta$ would be unbounded. Likewise if $\neg\theta$ is bounded, then $\varphi \wedge \theta$ would be unbounded. Finally, if θ and $\neg\theta$ are both unbounded, then if $\varphi \wedge \theta$ was bounded, then $\varphi \wedge \neg\theta$ is necessarily unbounded.

This leaves the case where $\theta_i(x) = \exists y < b(\psi(x,y))$. By collection[17] $\mathrm{Q}x\exists y < b(\psi(x,y)) \to \exists y < b\mathrm{Q}\mathrm{x}(\psi(x,y))$. This latter formula says that there is a *fixed* $y < b$ such that unboundedly many x satisfy ψ. Therefore, if $\theta_i(x)$ is unbounded, then $\varphi_i \wedge \psi(x,c) \wedge c < b$ must also be unbounded by the previous combinatorial argument and replacing the fixed y by c. If $\theta_i(x)$ is not unbounded, then we can conjoin its negation as usual and retain an unbounded formula.

Therefore, the $\varphi_n' s$ are a sequence of unbounded formulas. We can thus see that:

$$\mathcal{M}^* \vDash \mathrm{Th}(\mathcal{M}, m)_{m\in M} + \{\varphi_i(d) : i \in \mathbb{N}\} + \{d > m : m \in M\}$$

where $(\mathcal{M}, m)$ is $\mathcal{M}$ with constant symbols added for each element exists by compactness. (The theory is consistent since for any finite combination of formulas, d can be made large by the unboundedness of each of the $\varphi' s$). Moreover $\mathcal{M}^*$ is not $\mathcal{M}$ because it contains $d > m$ for all $m \in M$. However, this is not necessarily an end-extension.

Instead, we examine $\mathcal{M}_0$, which we define as the submodel of $\mathcal{M}^*$ generated by $M \cup \{d\}$. We claim that this $\mathcal{M}_0$ is in fact an elementary end-extension. $\mathcal{M}_0$ is an elementary extension since it is a submodel of $\mathcal{M}^*$ and $d > M$. To show it is an end extension, we need to show that no new elements are added to $\mathcal{M}$. Suppose one was, that is,

$$\mathcal{M}_0 \vDash \tau(m,d) < b$$

for some $b \in M$. We'd like to show that $\tau(m,d)$ is already defined by $\mathcal{M}$. Consider that by elementarity,

$$\mathcal{M}^* \vDash \tau(m,d) < b$$

Therefore -

$$\mathcal{M} \vDash \mathrm{Q}x\tau(m,x) < b$$

[17]Collection is a property of PA, and the traditional statement of it is that a function f with finite domain has a finite range. The way it is used here is a variant of collection that allows us to interchange the order of quantifiers.

Thus

$$\mathcal{M} \vDash \mathrm{Q}x\exists y < b(y = \tau(m, x))$$

But now this must be one of the θ_i's, and thus by construction $\exists y_0 < b \in M$ such that

$$\mathcal{M} \vDash \mathrm{Q}xy_0 = \tau(m, x)$$

□

Essentially, the work involved in the proof is not in constructing a model that contains the original model. There are many constructions of such models via compactness. The hard part is to prove that we can come up with a model that is also an end extension - that it preserves the original model in its entirety, without adding any new elements under any old elements. That requires the more careful construction we exhibited in this proof.

2.3.2. *The relationship between recursion and arithmetic.* There is a deep and rich connection between recursion theory and arithmetic, which we do not examine in great detail. The key results we need are that:

Proposition 24. *$A \subseteq \mathbb{N}^k$ is recursively enumerable iff there is a Σ_1 formula $\psi(x_1, x_2...x_k)$ such that for all $\bar{x} \in \mathbb{N}$, $\bar{x} \in A$ iff $\mathbb{N} \vDash \psi(\bar{x})$.* [3]

Proposition 25. *$A \subseteq \mathbb{N}^k$ is recursive iff there is a Π_1 formula $\psi(x_1, x_2, ...x_k)$ such that for all $\bar{x} \in \mathbb{N}$, $\bar{x} \in A$ iff $\mathbb{N} \vDash \psi(\bar{x})$.* [3]

Informally, the notion is that a recursively enumerable set is "semi-decidable" - to determine if a number is in a set, there is an algorithm that will eventually terminate if the number is in the set, but is not guaranteed to terminate if the number is not in the set. A recursive set is completely decidable, in that there is an algorithm that will terminate in a finite length of time and give an answer as to whether or not the number is in the set.

We focus primarily on recursive sets and their properties.

Proposition 26. *(Church's Thesis) Every function whose values can be found by some purely mechanical algorithm is a recursive function.* [3]

This statement can't be proven as it is a heuristic statement rather than a formal mathematical one, but it is essentially accepted. It takes real work to come up with non-computable functions, somewhat like creating a non-measurable set. While provably the vast majority of functions in arithmetic are non-recursive, (there are only countably many recursive functions because each recursive function can be defined by a formula of $\mathcal{L}_{\mathrm{A}}$), all the usual functions that we would be interested in, such as addition, modified subtraction, multiplication, exponentiation, tetration, and essentially anything else we can name is computable, and thus by Church's Thesis is computable. While Church's Thesis is a helpful guide to which functions are recursive, and helps to avoid long, drawn out proofs, proofs do exist for any function we use.

Proposition 27. *Gödel Numbering: There is a computable (and thus recursive) function that assigns a natural number to every well formed formula in the Language of Arithmetic.*

One of the key aspects of arithmetic is that it has immense ability to formalize mathematics within the theory, rather than outside. Nowhere is that more evident than in the ability to represent statements of mathematical logic as natural numbers. This means that proofs, sentences, and other traditional constructs of mathematical logic can be represented as statements about natural numbers. This is the key technique used in the proofs of incompleteness and other results. While there are many different numbering systems available, for our purposes the key result is that we can represent formulas as a natural number. The notation we use is that the Gödel number of a formula φ is $\ulcorner\varphi\urcorner$.

Proposition 28. *A nonstandard element c can be seen as coding a sequence of numbers through a computable function.*

Perhaps the easiest way of coding a sequence is to use the fact that every number has a unique binary expansion. This property is just as true of nonstandard integers as it is of standard ones. Consider that for any integer c,

$$c = \sum_{i=0} n \cdot 2^i$$

A particular integer i is included in the sequence if the value of n for that i is 1, and is not if the value of n is 0. The sequence coded by a particular integer is denoted as $(c)_n$. With this coding, numerous benefits accrue. For instance, exponentiation can be defined as $\chi(x, y, z) = \exists w[(w)_0 = 1 \wedge \forall i < y((w_{i+1}) = x \cdot (w)_i \wedge z = (w)_y$. There are many other coding mechanisms that also work just as well - a more formalistic argument involves a result called Gödel's Lemma and is detailed in [3].

3. Recursive Saturation and Its Consequences

3.1. **Introduction.** The intuitive picture of a model of arithmetic is a rigid structure. And in fact it is quite clear that the standard model $\mathcal{N}$ has no non-trivial automorphisms. Therefore the obvious question is: what is so different in nonstandard models that they can have non-trivial automorphisms?

It turns out that while rigid nonstandard models exist (in fact, in abundance) - we can also construct models of arithmetic with uncountably many automorphisms. We begin this section by considering a weaker theory than arithmetic, then develop the theory and existence of recursively saturated models of arithmetic. Finally, we show how recursively saturated models are rich enough to have non-trivial automorphisms.

3.2. **Automorphisms of $\mathbb{N} + \mathbb{ZQ}$.** By weakening the theory to just considering the theory of the set $\mathbb{N} + \mathbb{ZQ}$ as a linear order (formally, the theory of Discrete Linear Orders with a first element), we see that it is intuitively plausible that this set at least has automorphisms. $Aut(\mathbb{Q})$ (where $\mathbb{Q}$ is considered as an order)

is of size continuum, and each of these naturally induces an automorphism of $\mathbb{N} + \mathbb{Z}\mathbb{Q}$.

We can even consider the case of the theory of the set $\mathbb{N} + \mathbb{Z}$ as a linear order, and see that each automorphism of $\mathbb{Z}$ ($\mathbb{Z}$ here considered solely as a linear order), which are "shifts", also induces an automorphism on $\mathbb{N} + \mathbb{Z}$.

One interesting thing to note here is that in neither of these theories is any element outside of $\mathbb{N}$ definable by a formula. In the language consisting just of equality and $<$ we can uniquely define 0 $[\exists x \forall y (y > x)]$, and thus we can define each member of $\mathbb{N}$. But that's as far as it goes - it is hopeless to uniquely define any element in $\mathbb{Z}$ or $\mathbb{Z}\mathbb{Q}$, since our language is not strong enough to distinguish among them. This makes intuitive sense: because adding 1 or n to each element results in an identical set as an ordering, and we know that automorphisms preserve types, all elements of $\mathbb{Z}$ as an order must have the exact same type. Therefore each member of $\mathbb{Z}$ cannot be uniquely defined by a formula, and therefore each member of $\mathbb{Z}$ is what we call "undefinable". Each undefinable appears to be able to be mapped to another undefinable that shares the same complete type by an automorphism. In fact here, all of the undefinable share the same complete type, although this is by no means a requirement for more general models. The existence (and in fact, abundance) of undefinable elements and their relative freedom to move in automorphisms plays a key role in the creation of automorphisms of models of arithmetic.

3.3. **Recursive Saturation.** One of the key objects of study in Model Theory are the consequences of types being realized or omitted. Some theories are extremely rigid, or "categorical", meaning that there is no flexibility in what types can or can't be included in a model of a theory. But many other theories, including PA, have far more freedom with types. The extreme cases of types being included or excluded are saturated models and prime models, respectively. In short, a prime model realizes as few complete

types as possible, while a saturated model realizes as many as possible.

The best way to think about a saturated model is as a model that is extremely "rich." In a saturated model, informally, "as many things that can happen do happen." Formally, that translates into as many complete types as possible being realized. From the fact that there are uncountably many distinct models of PA, the total number of types in $\mathcal{L}_{\mathrm{A}}$ is uncountable, which would be problematic for a study of saturated countable models of PA.

However, in arithmetic, it turns out to be helpful to look at recursive saturation. Recursive saturation means that every recursive type is realized by some element in the model. While these structures are slightly less rich than full saturation, in that instead of all types, we are commuted to realizing just all recursive types, their chief benefit is that recursive types also are definable in the language of arithmetic, which is not guaranteed with full saturation. One immediate benefit is that this limits us only to countably many recursive types (since there are only countably many formulas). Therefore we can modify the statement above about saturated models to "everything (recursive) that can happen, does happen." This fertile intersection between definability and saturation properties leads to the results that follow.

3.3.1. *Existence.* We begin by formalizing the definition of a recursive type.

Definition 29. A recursive type is a type $p(\bar{x})$ whose set of Gödel numbers $\{\ulcorner\varphi(x)\urcorner|\varphi(\bar{x}) \in p(\bar{x})\}$ is recursive. [3]

Definition 30. A *type over* M is a set $p(\bar{x})$ of formulas $\varphi(\bar{x}, \bar{a})$ of $\mathcal{L}_{\mathrm{A}} \cup \{\bar{a}\}$, where $\bar{x}$ is a fixed finite tuple of free variables and $\bar{a}$ is a fixed finite tuple of parameters such that $p(\bar{x})$ is finitely satisfied in M, i.e

$$M \vDash \exists \bar{x} \bigwedge_{i=1}^{k} \varphi_i(\bar{x}, \bar{a})$$

for each finite subset $\varphi_1(\bar{x}, \bar{a}), \ldots \varphi_k(\bar{x}, \bar{a})$. $p(\bar{x})$ is a recursive type over M if the set of Gödel numbers of these formulas is recursive, or formally if the set,

$$\{\ulcorner\varphi(\bar{x}, \bar{y})\urcorner | \varphi(\bar{x}, \bar{a}) \in p(\bar{x})\} \subseteq \mathbb{N}$$

is a recursive set, where $\bar{y}$ is a tuple of variables disjoint from $\bar{x}$ (this caveat is necessary because of the way Gödel numbering functions are defined.) As usual, a type is complete iff for all formulas $\varphi(\bar{x}, \bar{a})$ involving the same free-variables $\bar{x}$ as $p(\bar{x})$ and the same parameters $\bar{a}$ as $p(\bar{x})$, then either φ or $\neg\varphi$ is in the type.[3]

Definition 31. A model $M \vDash PA$ is recursively saturated iff every recursive type over M is realized in M.

We have seen before that an element can be seen as coding a set - we formalize this as "the set coded by a in M" is the set

$$S = \{n \in \mathbb{N} | M \vDash (a)_n \neq 0\}$$

The precise definition of $(a)_n$ here is not important as long as it is consistent - perhaps the nicest one is the binary expansion function, although others work just as easily.

We then define the "standard system" of a model M, denoted $SSy(M)$ as the collection of all subsets of $\mathbb{N}$ coded in M, or

$$SSy(M) = \{S \subseteq \mathbb{N} | S = \{n \in \mathbb{N} | M \vDash (a)_n \neq 0\} \text{ for some } a \in M\}$$

Two results that illuminate the behavior of $SSy(M)$ are that every recursive subset of the natural numbers is coded in all nonstandard models of PA, and the converse that for every non-recursive set, there is a nonstandard model that does not code that set. [3]

Lemma 32. *If $S \subseteq \mathbb{N}$ is recursive than S is coded in all nonstandard models of PA.*

Proof. We define the type

$$p(x) := \{(x)_i \neq 0 | i \in S\} \cup \{(x)_i = 0 | i \notin S\}$$

These formulas state that "x codes the i^{th}" element of S for each i. Therefore if $p(x)$ is realized, that all of these formulas are realized - in other words some element codes S. And if S is coded, then some element x has to be doing the coding - therefore $p(x)$ is realized.

Now we use the recursion hypothesis: since S is recursive, it is definable by a formula φ - therefore

$$n \in S \Rightarrow PA \vdash \varphi(n)$$

$$n \notin S \Rightarrow PA \vdash \neg\varphi(n)$$

Therefore $p(x)$ is realized if the type:

$$q(x) = \{(x)_i \neq 0 \leftrightarrow \varphi(i) | i \in \mathbb{N}\}$$

is also realized in M.

At this point, we make an overspill argument: for $k \in \mathbb{N}$

$$M \vDash \exists x \forall i < k[(x)_i \neq 0 \leftrightarrow \varphi(i)]$$

since x is just the binary expansion of a sequence. Therefore

$$M \vDash \exists x \forall i < b[(x)_i \neq 0 \leftrightarrow \varphi(i)]$$

for b nonstandard. Because b is nonstandard, some a nonstandard realizes $q(a)$, and therefore a codes the set S. [3] □

We also observe that the proof of this statement gives us additional detail about $SSy(M)$ - the interaction between a set being coded and a type being realized tells us that the sets in $SSy(M)$ correspond to which types are realized in M. [3]

We turn back to the problem of actually constructing a recursively saturated model.

Proposition 33. *Let M be an countably infinite model of $\mathcal{L}_{\mathrm{A}}$. Then there exists an $\mathcal{L}_{\mathrm{A}}$ structure M' that elementarily extends with M' recursively saturated and countable.*[18]

[18]The theorem as proved in Kaye is actually stronger than this - it states that there are recursively saturated extensions of any infinite model of any

Proof. For each $m, n \in \mathbb{N}$ there are countably many sets

$$p(x_0, \ldots x_m, y_0, \ldots y_n)$$

of formulas

$$\varphi(x_0, \ldots x_m, y_0, \ldots y_n)$$

with at most $m+n$ free variables and whose set of Gödel numbers

$$\{\ulcorner \varphi(\bar{x}, \bar{y}) \urcorner | \varphi \in p(\bar{x}, \bar{y})\}$$

is recursive. Over $n, m \in \mathbb{N}$, the collection of all of these is a countable union of countable sets, and thus countable. We can therefore enumerate this as $p_0(\bar{x}, \bar{y}), p_1(\bar{x}, \bar{y}), \ldots, p_i(\bar{x}, \bar{y}) \ldots$ such that the free variables in $p_i(\bar{x}, \bar{y})$ are $x_0, \ldots x_{m_i}, y_0 \ldots y_{n_i}$.

We now set up an elementary chains argument. In the first stage, we let $M_0 = M$. The cardinality of the set of all finite length sequences in M is the same as the cardinality of M, again because they are a countable union of countable sets, and denote that set as $M^{<\omega}$. A representative element of $M^{<\omega}$ is $\bar{a} = (a_0, a_1, \ldots a_m) \in M$ of length $m+1$.

At this point, we consider each pair of $p_i(\bar{x}, \bar{y})$ and tuples $\bar{a}$. The goal will be to define new constant symbols for each of the free variables $\bar{x}$ such that $p_i(\bar{x}, \bar{a})$ can be expressed using constant symbols for each member of $\bar{x}$. This is easy enough to do - we add the constant symbols $c_{i,\bar{a},0}, c_{i,\bar{a},1}, \ldots c_{i,\bar{a},m_i}$, and while the triple indexing is abhorrent, it merely means that each constant symbol depends on which of the i types it is coming from, the choice of $\bar{a}$, and its position in $\bar{x}$. We also expand the language to name each element $a \in M_0$. While this is a massive language expansion, it is still countable.

---

recursive language, not just $\mathcal{L}_{\mathrm{A}}$, a recursive language meaning that there is a Gödel Numbering that assigns numbers to each constant, relation, function, and variable such that the set of all constants, the set of all relations, the set of all functions, and the set of all variables as numbered are recursive. This is rather trivial for $\mathcal{L}_{\mathrm{A}}$ since there are only finitely many constants, relations, and functions, and no variables. We also only prove the countable case although the general case requires a slight modification.

Then, we consider the theory T in this expanded language $\mathcal{L}$, with axioms:

(a) $\theta(\bar{a})$ for every $\mathcal{L}$-formula $\theta(\bar{x})$ and every $\bar{a} \in M_0$ for which $M_0 \vDash \theta(\bar{a})$

(b) $\varphi(c_{i,\bar{a},0}, \ldots c_{i,\bar{a},m}, \bar{a})$ for every $\varphi(\bar{x}, \bar{y}) \in p_i$, every $i \in \mathbb{N}$, and every $a_0, a_1, \ldots a_{n_i} \in M$ such that $p(\bar{x}, a_0, a_1, \ldots, a_{n_i})$ is a type over M_0.

This argument has a very definition-chasing flavor to it: the definition of type over M_0 requires that each type be finitely satisfiable, and the axioms including true statements are necessarily consistent. Therefore by compactness there is countable model M_1 satisfying T. Moreover, because M_1 must have an element that realizes the constant for each $a \in M_0$, $M_1 \succ M_0$, and moreover M_1 must realize every recursive type over M_0.

We can continue to proceed in this way, such that we have a chain of models $M_0 \prec M_1 \prec \ldots$ of models all of countable cardinality such that M_{j+1} realizes every recursive type of M_j. Then consider the model

$$M' = \bigcup_{j \in \mathbb{N}} M_j$$

By the fact that this is an elementary chain, it is an elementary extension of M_0, and M' is countable as a union of countable sets. Finally, if $q(\bar{x})$ is a recursive type over M' that involves a finite number of parameters $\bar{b}$, then this recursive type must have been contained in M_j for some j since $\bar{b} \in M_j$ for some j. Therefore this type would have been realized in M_{j+1}, and therefore in M' since $M' \succ M_{j+1}$. The reduct of M' to $\mathcal{L}_{\mathrm{A}}$ must still be recursively saturated since we are only removing constant symbols. [3] $\square$

3.4. **Automorphisms of recursively saturated models.** The key aspect of recursively saturated models is that they realize so many types, while having the vast majority of elements remain undefinable, even with finitely parameters. This gives fertile grounds for creating non-trivial automorphisms by moving elements. The result we trace here is due to Smorynski, and proves

rather more than just creating one automorphism. Instead, we prove that there are continuum many automorphisms that pointwise fix any initial segment closed under exponentiation.

A new bit of notation we need is that we consider $a_0, \ldots, a_{n-1} \equiv b_0, \ldots b_{n-1} \bmod c$ iff the n-tuples have the same types relative to parameters less than or equal to c.[19] The idea is that c represents how much of the model that can be preserved.

Lemma 34. *Smorynski's Basic Back-and-Forth Lemma: Let $\mathcal{M}$ be recursively saturated. Let $c, a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}, a_n \in |M|$ be given with c nonstandard and $a_0, \ldots a_{n-1} \equiv b_0, \ldots b_{n-1} \bmod c$. Then there is an element $b_n \in M$ such that $a_0, \ldots, a_{n-1}, a_n \equiv b_0, \ldots, b_{n-1}, b_n \bmod d$ where $2^{2^d} \leq c$.*

Proof. Suppose for all θ,

$$\mathcal{M} \vDash \forall v_0, \ldots v_{m-1} \leq \bar{c}[\theta(v_0, \ldots, v_{m-1}, a_0 \ldots a_{n-1}) \leftrightarrow \theta(v_0, \ldots, v_{m-1}, b_0, \ldots, b_{n-1})]$$

Then consider the set $\tau(v, a_0, \ldots a_{n-1}, a_n, b_0, \ldots b_{n-1}, d)$, which we denote as τ_v, defined as

$$\forall v_0, \ldots v_{m-1} \leq \bar{d}[\theta(v_0, \ldots v_{m-1}, a_0, \ldots a_{n-1}, a_n) \leftrightarrow \theta(v_0, \ldots v_{m-1}, b_0, \ldots b_{n-1}, v)]$$

We try and show that if d is sufficiently small, then τ_v is a type.

We now create the set of code numbers that satisfy each θ_i. We define

$$D_{e_i}^{\theta_i} = \{\langle c_0, c_1, \ldots, c_{m-1}\rangle | c_0, \ldots c_{m-1} \leq d \wedge \mathcal{M} \vDash \theta_i(c_0, \ldots c_{m-1}, a_0, \ldots a_{n-1}, a_n)\}$$

D_x is the set that contains each member of its binary expansion. $D_{e_i}^{\theta_i}$ contains the tuples of all substitutions for the free variables $v_0, \ldots v_{m-1}$ that satisfy θ_i. e_i is the number that results from the binary expansions of the result of the Cantor Pairing function. We can show that each of these $e_i < c$, if $c \geq 2^{2^d}$. Consider that for

[19] Formally, this is stated as $a_0, \ldots a_{n-1} \equiv b_0, \ldots b_{n-1} \bmod c$ if and only if for all formulas θ with no parameters and $m + n$ free variables, $\mathcal{M} \vDash \forall v_0 \ldots v_{m-1} \leq \bar{c}[\theta(v_0 \ldots v_{m-1}, a_0 \ldots a_{n-1}) \leftrightarrow \theta(v_0 \ldots v_{m-1}, b_0 \ldots b_{n-1})$.

any $\theta_1, \dots \theta_k$, k finite,

$$\mathcal{M} \vDash \exists v \forall v_0, \dots v_{m-1} \leq d \bigwedge_i^k [\theta_i(v_0, \dots v_{m-1}, a_0, \dots, a_{n-1}, v) \leftrightarrow \langle v_0, \dots v_{m-1} \rangle \in D_{e_i}^{\theta_i}]$$

This is simply definition chasing - here v is simply a_n, and the rest follows by the way $D_{e_i}^{\theta_i}$ was created. But since $a_0, \dots a_{n-1} \equiv b_0, \dots b_{n-1} \bmod c$, and $d, e_1, \dots e_k < c$,

$$\mathcal{M} \vDash \exists v \forall v_0, \dots v_{m-1} \leq d \bigwedge_i^k [\theta_i(v_0, \dots v_{m-1}, b_0, \dots b_{n-1}, v) \leftrightarrow \langle v_0, \dots v_{m-1} \rangle \in D_{e_i}^{\theta_i}]$$

Therefore

$$\mathcal{M} \vDash \exists v \forall v_0, \dots v_{m-1} \leq d \bigwedge_i^k [\theta_i(v_0, \dots, v_{m-1}, b_0, \dots b_{n-1}, v) \leftrightarrow \theta_i(v_0, \dots, v_{m-1}, a_0, \dots a_{n-1}, a_n)]$$

Therefore τ_v is a type. Since this is a recursive type, and $\mathcal{M}$ is recursively saturated, $\mathcal{M}$ is realized by some element $b_n \in M$, and thus $a_0, \dots a_n \equiv b_0, \dots b_n \bmod d$. [7] □

Lemma 35. *Smorynski's Combinatorial Lemma: Let $\mathcal{M}$ be recursively saturated, $I \subset_e \mathcal{M}$ an initial segment closed under exponentiation. Let $I < a$ and $I < b$ be given. Then there are c, d with $I < c < d < a$ and d not definable from b together with any parameters less than or equal to c.*

Proof. We select c such that $2^{2^c} \leq a$ and count the number of possible definitions. The number of definitions using a finite number k parameters, each parameter less than or equal to c, together with b must have an upper bound of the number of formulas times the number of k-tuples with each parameter less than c.

In other words, $\#(definitions) \leq \#(formulas) \times \#(k-tuples)$

However, the number of formulas of $\mathcal{L}_{\mathrm{A}}$ must be contained within I [20], and thus

$$\leq c \cdot \binom{c+1}{k}$$

[20] More specifically - the set of Gödel Numbers of each formula of $\mathcal{L}_{\mathrm{A}}$ is an embedding into $\mathbb{N}$, and therefore must be lower than any nonstandard element.

Therefore

$$\leq \sum_{i=0}^{\omega} c \cdot \binom{c+1}{k} \leq c(\sum_{i=0}^{c+1} \binom{c+1}{i} \leq c \cdot 2^{c+1} \leq 2^{2c+1}$$

The first inequality follows by taking k over all finite numbers, the second by pulling c out and summing over more terms than originally used, the third by the fact that the sum of the $(c+1)^{st}$ row of Pascal's Triangle is $(c+1)^2 \leq 2^{(c+1)}$, and the last by the fact that $c \leq 2^c$.

But since $2^{2^c} \leq a$, there are more elements between c and a than there are definitions. Therefore we can select a d not definable as desired.[7] □

Lemma 36. *Let M be recursively saturated. Let $a_0, \ldots a_{n-1}, c \in M$ with a_n undefinable from $a_0, \ldots a_{n-1}$ and $e_0, \ldots, e_{k-1}$ for any $e_i \leq c$. In $\mathcal{M}$ there is an $a'_n \neq a_n$ such that:*

$$a_0, \ldots, a_{n-1}, a_n \equiv a_0, \ldots a_{n-1}, a_n \bmod d$$

where $2^{2^d} \leq c$.

Proof. Consider that $\tau(v, a_0, \ldots a_{n-1}, a_n, d)$:

$$\exists v \neq a_n \forall v_0, \ldots v_{m-1} \leq d[\theta(v_0, \ldots v_{m-1}, a_0, \ldots, a_{n-1}, a_n) \leftrightarrow \theta(v_0, \ldots, v_{m-1}, a_0, \ldots, a_{n-1}, v)]$$

Then consider that if this set of formulas is inconsistent, then for some finite set of formulas $\theta_0, \ldots, \theta_k$

$$M \vDash \forall v_0, \ldots, v_{m-1} \leq d \bigwedge_{i=0}^{k} [\theta_i(v_0, \ldots, v_{m-1}, a_0, \ldots, a_{n-1}, v) \leftrightarrow \langle v_0, \ldots, v_{m-1} \rangle \in D_{e_i}^{\theta_i}] \rightarrow v = a_n$$

But then we have precisely a definition of a_n from $a_0, \ldots, a_{n-1}$ and the $e'_i s$, and we had stated that a_n was undefinable. [7] □

Theorem 37. *Let M be a countable recursively saturated model of arithmetic, $I \subset_e \mathcal{M}$ an initial segment closed under exponentiation. There is a continuum of automorphisms which pointwise fix I.*

Proof. By $\omega - step \bmod 3$ back and forth argument. We enumerate M, and require that $c_0, c_1, \ldots$ be a sequence of elements in M such that $2^{2^{c_{n+1}}} < c_n$, and that the $c_n's$ are downward cofinal in $M \backslash I$, in other words that they are arbitrarily close to I.

Then at stages where $k \equiv 0 \bmod 3$,

$$a_0, \ldots, a_{k-1} \equiv b_0, \ldots, b_{k-1} \bmod c_{n_k}$$

Then we let a_k be the first element in the enumeration of M not among $a_0, \ldots, a_{k-1}$ and use lemma 34 to find a b_k such that

$$a_0, \ldots, a_k \equiv b_0, \ldots, b_k \bmod c_{n_k+1}$$

and we can therefore set $n_{k+1} = n_k + 1$.

At stages where $k \equiv 1 \bmod 3$, we do the same thing except we map b_k to a_k.

At stages where $k \equiv 2 \bmod 3$, we have that

$$a_0, \ldots, a_{k-1} \equiv b_0, \ldots b_{k-1} \bmod c_{n_k}$$

We can apply lemma 35 to find c, a such that

$$c < a < c_{n_k}$$

with a undefinable from $\langle a_0, \ldots, a_{k-1} \rangle$ with any parameters less than or equal to c. Therefore we can choose $c_m \leq c$, and letting $a_k = a$, find via lemma 34 and lemma 36 distinct elements b, b'such that $a_0, \ldots, a_k \equiv b_0, \ldots, b_{k-1}, b \equiv b_0, \ldots, b_{k-1}, b' \bmod (c_{m+3})$. We can choose one of b and b' to be b_k and let $n_{k+1} = m + 3$.

Then after ω steps, every element of M will have been treated at some point by the steps congruent to 0 and 1, thus forcing us to have an automorphism by mapping the a tuple to the b tuple, which after all necessarily have the same types relative to I. Because in the steps where $k \equiv 2 \bmod 3$, we had two choices, after ω steps we now have a continuum of of automorphisms. Furthermore, elements arbitrarily low above I are moved by virtue of the $k \equiv 2$ step because the $c_n's$ are downward cofinal. Finally, every member of I is fixed because for $a \in I$, $a < c_n$ for every n, and therefore can be defined using parameters from below c_n - namely

itself. Because it is definable in this way it has to be mapped to itself. [7] □

Therefore, we have proved rather more than just that recursively models of arithmetic have automorphisms. Indeed, we achieve the satisfying statement that:

Theorem 38. *In a recursively saturated model of arithmetic, there are continuum many initial segments I that are closed under exponentiation, each of which has continuum many distinct automorphisms for which I is the largest initial segment fixed pointwise.*

We can also prove an interesting converse to this result. What we had previously shown was that initial segments closed under exponentiation were maximal segments fixed by some automorphism. They also turn out to be the minimal fixed segment of an automorphism as well. We denote the largest initial segment pointwise fixed by an automorphism g as $I_{\text{fix}}(g)$. [4]

Proposition 39. *If $g \in G$ and $I = I_{fix}(g)$ then I is closed under exponentiation.*

Proof. This is proof that exploits the use of even infinite (from outside the model) binary expansions of elements being able to be reduced to a formula, and thus being preserved under automorphism . Recall that g is an automorphism, so suppose g fixes $\{x \in M : M \vDash x < a\}$ and $y < 2^a$. Then we define the formula $u \in v$ to be "the uth digit of the binary expansion of v is 1"[21]. Then, for all $x \in M$, if $M \vDash x \in y$, we have $x < a$ so that

$$M \vDash x \in y$$

Because g is an automorphism, all formulas satisfied by the old elements must also be satisfied by the new one:

$$\iff M \vDash g(x) \in g(y)$$

[21]This poses no definability issues since INSIDE the model u is just a natural number - even though from outside it appears to be infinite.

But since $x < a$,

$$\iff M \vDash x \in g(y)$$

Therefore x is in the binary expansion of $g(y)$, and since y and $g(y)$ must now have the same binary expansion, $y = g(y)$. □

The key use of the fact that $y < 2^a$ is that all the elements of the binary expansion are under a, since if there was an element b in the binary expansion of y that was larger than a, that would imply that $2^b < y$, which is impossible since $y > 2^a$.[4]

4. A Bit About the Open Problems

A very interesting connection between automorphisms of PA and the rest of mathematics are in the fact that they have a topological group structure. In fact, the general structure of automorphisms of any countable structure $\mathcal{M}$ have similar topological and algebraic properties to PA. In this section, we merely trace out some of the results in this area, mostly without proofs, and state two problems that remain open in the subject.

Fact 40. *The automorphisms of a countable recursively saturated models $\mathcal{M}$, or $\mathrm{Aut}(\mathcal{M})$ have a mertrizable topological permutation group structure.*

The permutation group here G turns out to have cardinality $2^{\aleph_0}$. The topology is metrizable; enumerate the model as $\{x_n : n < \omega\}$ [22], and then define $d(f, g) = \frac{1}{2^{n+1}}$, where n is the least such n for which $x_n^f \neq x_n^g$ or $(x_n)^{f^{-1}} \neq (x_n)^{g^{-1}}$. Moreover, this group has some other interesting properties: G has to be Hausdorff, complete, the index of all open subgroups can be at most countable. We can also describe the basic open subgroups: they take the form

$$G_a = \{g \in G : g(a) = a\} \text{ over all } a \in M$$

[4]

[22]This exploits yet another strange feature of models of arithmetic: while they are not the natural numbers, they remain countable, and thus in bijection with them! We can therefore enumerate a nonstandard model of arithmetic using the natural numbers.

Fact 41. *Types correspond to orbits.*

We recalled earlier the notion of types as the set of formulas realized by a particular element. It turns out that because the automorphism group of a recursively saturated model is "strongly $\aleph_0$ homogenous", each type corresponds to an orbit of the automorphism group. This actually should not be terribly surprising: if a complete type can be realized by more than one element (and thus realized by infinitely many such elements), then by 34 an automorphism can be constructed mapping these elements to each other in a non-trivial way. Therefore each complete type corresponds to an orbit of the permutation group.[4]

Remark 42. The open problems relate to the closed normal subgroups of $\mathrm{Aut}(\mathcal{M})$. In order to phrase the problem, we need a few more notions and notations. $G_{(A)}$ is the subgroup of the automorphism group that fixes the set A pointwise; $G_{\{A\}}$ is the subgroup that fixes A setwise. $G(_{>I})$ is the set of all automorphisms such that $\mathrm{I}_{\mathrm{fix}}(\mathrm{g}) \supsetneq I$. An initial segment I is "invariant" if every automorphism in G fixes I setwise, that is, $G_{\{I\}} = G$. It turns out that for an initial segment I closed under exponentiation, $G_{(I)}$ and $G_{(>I)}$ are normal iff I is invariant. Moreover, $G_{(I)}$ is always necessarily closed. The key result of [4] is that:

Theorem 43. *For $\mathcal{M}$ recursively saturated, and G a topological group with the usual topology*

(a) For initial segments I, J of $\mathcal{M}$: $G_{(I)}$ and $G_{(J)}$ are closed; $G_{(I)} = G_{(J)}$ iff they have the same closure under exponentiation, and $G_{(I)}$ is normal iff $\exp(I)$ is invariant. Also, for $N \lhd G$, $\mathrm{I}_{\mathrm{fix}}(N)$[23] is invariant and closed under exponentiation.

(b) The operations

$$I \to G(I)$$

and

$$N \to \mathrm{I}_{\mathrm{fix}}(N)$$

[23]A slight abuse of notation - this means the largest initial segment pointwise fixed by the group of automorphisms N

defined on invariant initial segments I of $\mathcal{M}$ closed under exponentiation, and closed normal subgroups N of G are inverse to each other. [4]

As Kaye points out, this leads to some interesting remarks; first, due to another result, this means that there are nontrivial normal closed subgroups for a model of PA if and only if there are nonstandard definable elements. But the really interesting questions are:

Problem 44. Classify all normal subgroups, showing that they are all $G_{(I)}$ or $G_{(>I)}$ for invariant I. [4]

Problem 45. Give a group-theoretic characterization of the closed subgroups that occur as $G_{(I)}$for some initial segment I of M. Given such a characterization, extend the Galois correspondence in Theorem 43 to all such groups. [4]

We end on that note - Kaye offers some suggestions on how to solve the first, but the second remains completely open.

A short note on references is worth making here. I cite numerous references that aren't used in the paper; these references were helpful to me although not directly used in the paper. Of course, I have been studying this subject for nearly two years, and have been reading both for general knowledge as well as this paper. Inevitably some sources will be left out. Everything I use directly in the paper should be cited. I also benefited greatly from conversations with Dr. Ali Enayat; his influence is throughout this paper as well and nearly everything should also have a citation to him.

REFERENCES

[1] C.C. Chang and H.J. Keisler. *Model Theory*. North Holland, 1990.

[2] Ali Enayat. Automorphisms of models of arithmetic, May 2007.

[3] Richard Kaye. *Models of Peano Arithmetic*. Oxford Science Publications, 1991.

[4] Richard Kaye. *Automorphisms of First-Order Structures*. Oxford Science Publications, 1994.

[5] Roman Kossak and Jim Schmerl. *The Structure of Models of Peano Arithmetic*. Oxford University Press, 2006.

[6] J.H. Schmerl. Closed normal subgroups. *Mathematical Logic Quarterly*, 47:489–492, 2001.

[7] C. Smorynski. Back-and-forth inside a recursively saturated model of ariihmetic. *Logic Colloquium '80*, pages 273–278, 1982.

[8] C. Smorynski. Recursively saturated nonstandard mmodel of arithmetic. *The Journal of Symbolic Logic*, 46:259–286, Jun. 1981.

[9] Terry Tao. The completeness and compactness theorems of first-order logic, April 2009.

[10] Wikipedia. Booolean prime ideal theorem, 2013.

[11] Wikipedia. Compactness theorem, 2013.

[12] Gideon Wormeester. Arithmetic, models & automorphisms. Master's thesis, Utrecht University., 2008.