Arithmetic, Models & Automorphisms

by: Gideon Wormeester

Master Thesis
Supervised by: Jaap van Oosten
Co-supervised by: Ieke Moerdijk
Date: August 18, 2008

Contents

1 Introduction

Where most mathematicians seek to study (mathematical) objects, using theorems, proofs and logical reasoning, logicians typically study the theorems, proofs and reasoning themselves. Questions like "What is a proof?", "When is a statement true?", "If something is true, does it have to be provable?" seem very philosophical in nature, but logic gives them a clear, well-defined meaning and in this context, tries to answer these questions.

Most of mathematics can be reduced to two major areas: arithmetic and set theory. Arithmetic governs the behavior of the natural numbers, the properties of addition and multiplication. Set theory deals with sets, their unions and intersections. Because these two areas are so fundamental, they are an important area of study for logicians. Over time, people have come up with elegant, compact axiomatizations for arithmetic and set theory, in the form of Peano Arithmetic and Zermelo-Fraenkel Set Theory. There exist many variations on these axiomatizations and the strength (as determined by the statements that can be proven) of each of these variations has been studied extensively.

A question one can ask is if these axiomatizations are natural. That is, is our choice of axioms for these systems merely an arbitrary choice that happens to work well or do the theories emerge naturally from weaker systems? Work by Ali Enayat provides some insight into this question. In his papers [1], [2] and [3] he provides results that show that some foundational theories are characterized by weaker theories through automorphisms of models of these weaker theories. In this text, we will discuss these results. Our focus will mainly be on theories of arithmetic, but set theory will be briefly touched as well.

Section 2 will deal with the preliminary model theory of Peano Arithmetic and some of its fragments, some basic set theory implemented in arithmetic and the concept of ultrafilters, which is a recurring theme in the proofs of the three main theorems from Enayats papers. In section 3, a theorem from [1], a characterization of the fragment $I\Delta_0 + B\Sigma_1 + Exp$ of Peano Arithmetic in terms of the fragment $I\Delta_0$ will be discussed. Section 4 then gives similar theorems concerning second-order arithmetic ([2]) and set theory ([3]), which will be discussed with somewhat less detail.

2 Preliminaries

2.1 Definitions and notational conventions

- Caligraphic letters like $\mathscr{M}$, $\mathscr{N}$ denote structures and models where the normal font equivalents, M, N, denote the underlying set. So $\mathscr{M} = (M, -^{\mathscr{M}})$. $\mathscr{L}$ with various subscripts is used to denote a language.

- In inductive proofs on the structure of a formula, the only cases that will be evaluated are atomic formulas, $\neg\phi(\mathbf{x})$, $\phi(\mathbf{x}) \wedge \psi(\mathbf{x})$, $\exists y < t(\mathbf{x})[\phi(\mathbf{x}, y)]$ and $\exists y[\phi(\mathbf{x}, y)]$. All other logical connectives can be constructed using these four connectives.

- A formula is $\Delta_0(\mathscr{L})$ iff the only quantifiers that occur in the formula are bounded (e.g. of the form $\exists x < t(\mathbf{y})$, with $t(\mathbf{y})$ a term of the language $\mathscr{L}$ not containing x). Where there is no ambiguity about the language, the $(\mathscr{L})$-part will be omitted. We now define the formula-classes Δ_n, Σ_n, Π_n. For $n = 0$, $\Delta_0 = \Sigma_0 = \Pi_0$. A formula is Σ_{n+1} if it is of the form $\exists\mathbf{y}\phi(\mathbf{x}, \mathbf{y})$ where $\phi(\mathbf{x}, \mathbf{y})$ is Π_n. A formula is Π_{n+1} if it is of the form $\forall\mathbf{y}\phi(\mathbf{x}, \mathbf{y})$ where $\phi(\mathbf{x}, \mathbf{y})$ is Σ_n. A formula is Δ_n iff it is equivalent to both a Π_n formula and a Σ_n formula.

2.2 Models of Peano Arithmetic

The language of Peano Arithmetic (abbreviated by PA from this point on) is the default language that we use for everyday arithmetic. It consists of two symbols for constants, 0 and 1, one relation-symbol, $<$, and two function-symbols, $+$ and $*$. The most common structure for this language, $\mathscr{L}_{PA}$, is the structure of the natural numbers, $\mathbb{N}$. The domain of $\mathbb{N}$ are the non-negative integers $(0, 1, 2, 3, ...)$ and the constants, functions and relation are interpreted in the obvious way.

The natural numbers is the structure that we practise everyday arithmetic with. It is axiomatized by the set of axioms for Peano Arithmetic. This set contains axioms for the common properties of addition, multiplication, 0 and 1 together with for every formula ϕ the induction-axiom for ϕ. The complete set of axioms is as follows:

$$\begin{aligned}
PA1: &\quad \forall x,y,z[(x+y)+z=x+(y+z)]\\
PA2: &\quad \forall x,y[x+y=y+x]\\
PA3: &\quad \forall x,y,z[(x*y)*z=x*(y*z)]\\
PA4: &\quad \forall x,y[x*y=y*x]\\
PA5: &\quad \forall x,y,z[x*(y+z)=(x*y)+(x*z)]\\
PA6: &\quad \forall x[x+0=x]\\
PA7: &\quad \forall x[x*0=0]\\
PA8: &\quad \forall x[x*1=x]\\
PA9: &\quad \forall x\neg[x<x]\\
PA10: &\quad \forall x,y[x<y\vee x=y\vee y<x]\\
PA11: &\quad \forall x,y,z[x<y\wedge y<z\rightarrow x<z]\\
PA12: &\quad \forall x,y,z[x<y\rightarrow x+z<y+z]\\
PA13: &\quad \forall x,y,z[0<z\wedge x<y\rightarrow x*z<y*z]\\
PA14: &\quad \forall x,y[x<y\rightarrow \exists z(x+z=y)]\\
PA15: &\quad \forall x[x=0\vee 0<x]\\
PA16: &\quad \forall x[0<x\rightarrow x=1\vee 1<x]\\
PA17: &\quad \phi(0)\wedge\forall n(\phi(n)\rightarrow\phi(n+1)))\rightarrow\forall n\phi(n)
\end{aligned}$$

$PA17$ is not an axiom, but rather an axiom scheme. It gives an axiom for each formula ϕ stating the principle of induction for ϕ. Axioms $PA1$ through $PA17$ together form the theory PA, while leaving out the induction-scheme, $PA17$, yields the weaker theory PA^-. Note that there are many equivalent formulations of this set of axioms. The natural numbers, $\mathbb{N}$ are a model of PA (and consequently of PA^-). There are other models of PA that are not isomorphic to $\mathbb{N}$. It was Skolem who first proved in 1934 so-called "non-standard models" of PA exist. This proof makes use of the Compactness Theorem.

Theorem 2.1. *There exists a model $\mathscr{A}$ of PA such that $\mathbb{N} \ncong \mathscr{A}$.*

Proof. Extend the language $\mathscr{L}_{PA}$ with the constant c (Call the extended language $\mathscr{L}'_{PA}$). Consider the following set of sentences:

$$\Gamma = Th(\mathbb{N}) \cup \{\overline{n} < c | n \in \mathbb{N}\}$$

Clearly, every finite subset $\Gamma' \subset \Gamma$ contains only finitely many sentences ϕ_n of the form $\overline{n} < c$, so there exists an m such that for all $n > m$, $\phi_n \notin \Gamma'$.

Now, if we interpret c by any element of $\mathbb{N}$ greater than m, then $\mathbb{N}$, with this interpretation for the new constant c and the usual interpretations for the other symbols in the language, is a model of Γ'.

Since this holds for every finite $\Gamma' \subset \Gamma$, by the Compactness Theorem we have that there exists a model $\mathscr{A}$ of Γ. Clearly, $\mathscr{A} \models Th(\mathbb{N})$. If we reduce our extended language $\mathscr{L}'_{PA}$ by removing the new constant c, we obtain our initial language, $\mathscr{L}_{PA}$. So the $\mathscr{L}_{PA}$-structure $\mathscr{A}$ is a model of PA, but $\mathscr{A}$ is clearly not isomorphic to $\mathbb{N}$, since $\mathscr{A}$ contains an element that is greater than every element of $\mathbb{N}$ □

Since $\mathbb{N} \models \forall x(x = 0 \vee \exists y(x = y + 1))$ (for all x, x is either 0 or has a predecessor), this sentence also holds in our new model $\mathscr{A}$. Consequently, the non-standard element c has a predecessor, $c - 1$, which in turn has a predecessor $c - 2$, etc... On the other hand, there also exist $c + 1$, $c + 2$, etc... With this construction we find a copy of the integers as non-standard elements around the non-standard element c.

Because of the domain of the model $\mathscr{A}$ is closed under multiplication, we find another non-standard element, $2c$, which does not have a finite distance to c (For if the distance $2c - c$ would be equal to a finite n, then $c = n$, contradiction.). By the same construction as before, we also find a copy of the integers around the element $2c$.

The construction does not end here. We find an unbounded amount of new copies of the integers below our starting point c and between every pair of non-standard elements that are not a finite distance apart, we find a new element that does not lie at finite distance to either of the two. In fact, it can be shown that any non-standard model of PA consists of the natural numbers together with a dense linear order A without endpoints, with every element of A replaced by a copy of the integers.

Theorem 2.2. *Any model of PA not isomorphic to $\mathbb{N}$ has the ordertype of $\mathbb{N} + A\mathbb{Z}$, with A a dense linear order without endpoints.*

Proof. Let $\mathscr{M}$ be a non-standard model of PA. The elements 0, $0 + 1$, $0 + 1 + 1$, ... of $\mathscr{M}$ form a set isomorphic to $\mathbb{N}$. So $\mathscr{M}$ has order type $\mathbb{N} + X$ for a linear order X. Given a non-standard element a, let $[a]$ denote the set

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

In words, $[a]$ is the set of all elements with a finite distance to a, or the $\mathbb{Z}$-block of a. Clearly, if $|a - b|$ is non-standard then $[a] \cap [b] = \emptyset$. Also given $x \in [a]$ and $y \in [b]$, with $[a] \cap [b] = \emptyset$, then $x < y$ iff $a < b$. Let A be the set of $\mathbb{Z}$-blocks. Then A is a linear order, with the order relation defined as follows:

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

It's easy to see that this order on A satisfies the 3 axioms for a linear order (reflexivity, transitivity, anti-symmetry). A has no least element, because given a non-standard a, we can find a b such that $2b = a \vee 2b = a+1$ and we have that $[b] < [a]$. A has no greatest element, since for any $[a]$ we have $[2a] > [a]$. So A is a linear order without endpoints. Given a and b in different $\mathbb{Z}$-blocks, the rounded part of $\frac{a+b}{2}$ is in a $\mathbb{Z}$-block different from $[a]$ and $[b]$. So A is also a dense linear order. □

Definition 2.3. *Given a set I, a model $\mathscr{M}$ with domain M. I is called an* initial segment *of $\mathscr{M}$, notation $M \subset_e N$, if $I \subseteq M$ and*

$$\forall x \in I, y \in M[(\mathscr{M} \models y < x) \rightarrow y \in I]$$

Dually, $\mathscr{M} = (M, ...)$ is an end extension *of $\mathscr{N} = (N, ...)$ if N is an initial segment of $\mathscr{M}$.*

Given models $\mathscr{M}$, $\mathscr{N}$ of PA, $\mathscr{M}$ is confinal *in $\mathscr{N}$ (or $\mathscr{N}$ is a cofinal extension of $\mathscr{M}$), notation $M \subset_{cf} N$, iff*

$$\forall a \in N \exists b \in M[N \models b \geq a]$$

Theorem 2.4. *If $M \subset_e N$ are structures of $\mathscr{L}_{PA}$ then $\mathscr{M} \prec_{\Delta_0} \mathscr{N}$ ($\mathscr{M}$ is a Δ_0-elementary submodel of $\mathscr{N}$.), i.e. for all Δ_0-formulas $\phi(\mathbf{x})$ and all sequences of parameters $\mathbf{a} \in M$: $\mathscr{M} \models \phi(\mathbf{a}) \leftrightarrow \mathscr{N} \models \phi(\mathbf{a})$.*

Proof. To prove the theorem, we use induction on the structure of Δ_0-formulas. Recall that in Δ_0-formulas all quantifiers are bounded. Consider a Δ_0 formula $\phi(\mathbf{x})$. We need to show that for all $\mathbf{a}$ of elements of M,

$$\mathscr{M} \models \phi(\mathbf{a}) \Leftrightarrow \mathscr{N} \models \phi(\mathbf{a})$$

If $\phi(\mathbf{x})$ is atomic, then the equivalence clearly holds. Suppose $\phi(\mathbf{x})$ is of the form $\theta_1(\mathbf{x}) \wedge \theta_2(\mathbf{x})$ and the equivalence holds for $\theta_1(\mathbf{x})$ and $\theta_2(\mathbf{x})$. Take $\mathbf{a} \in M$

$$\begin{array}{cc} & M \models \phi(\mathbf{a}) \\ \Leftrightarrow & M \models \theta_1(\mathbf{a}) \wedge \theta_2(\mathbf{a}) \\ \Leftrightarrow & M \models \theta_1(\mathbf{a}) \text{ and } M \models \theta_2(\mathbf{a}) \\ \Leftrightarrow & N \models \theta_1(\mathbf{a}) \text{ and } N \models \theta_2(\mathbf{a}) \text{ (using the induction hypothesis)} \\ \Leftrightarrow & N \models \theta_1(\mathbf{a}) \wedge \theta_2(\mathbf{a}) \\ \Leftrightarrow & N \models \phi(\mathbf{a}) \end{array}$$

The induction steps for the other logical connectives are omitted, but are easy to do and follow a similar pattern, with the exception of bounded quantification, which makes use of the fact that $\mathscr{M}$ is an initial segment. Suppose $\phi(\mathbf{x}, y)$ is of the form $\exists y < t(\mathbf{x})\ \theta(\mathbf{x})$ and the equivalence holds for $\theta(\mathbf{x})$. For $\mathbf{a}$ a sequence of parameters from M, we have that

$$M \models \phi(\mathbf{a}, y) \Leftrightarrow \text{ there exists } b < t(\mathbf{a}), b \in M, M \models \theta(\mathbf{a}, b)$$

If $\mathbf{a} \in M$, then also $t(\mathbf{a}) \in M$, because M is closed under addition and multiplication. If $b < t(\mathbf{a})$ and $b \in M$, then we must have that $b \in N$, since M is an initial segment of N. So we find that:

$$\begin{array}{rc} & M \models \phi(\mathbf{a}, y) \\ \Leftrightarrow & \text{there exists } b < t(\mathbf{a}), b \in N, M \models \theta(\mathbf{a}, b) \\ \Leftrightarrow & \text{there exists } b < t(\mathbf{a}), b \in N, N \models \theta(\mathbf{a}, b) \\ \Leftrightarrow & N \models \phi(\mathbf{a}, y) \end{array}$$

Here the equivalence between the second and the third line follows from the induction hypothesis. □

We say that I is a *cut* of $\mathscr{M}$ if it is a non-empty proper initial segment of $\mathscr{M}$ that has no last element.

2.3 Fragments of PA

We will be considering models of theories that are strictly weaker than the full theory of Peano Arithmetic.

Definition 2.5. *Define the axiom of induction on x in a formula $\phi(\mathbf{y}, x)$, $I_x\phi$ by*

$$I_x\phi = \forall \mathbf{y}[\phi(\mathbf{y}, 0) \wedge \forall x(\phi(\mathbf{y}, x) \rightarrow \phi(\mathbf{y}, x + 1)) \rightarrow \forall x(\phi(\mathbf{y}, x))]$$

For a class Γ for formulas of $\mathscr{L}_{PA}$, define the theory $I\Gamma$ as $PA^{-} \cup \{I_x\phi | \phi \in \Gamma\}$.

This definition gives rise to an arithmetical theory that is weaker than PA, the theory $I\Delta_0$. This theory is similar to PA, but only includes the principle of induction for Δ_0-formulas. This theory is also called *bounded arithmetic*.

Definition 2.6. *For a language extending $\mathscr{L}_{PA}$, the formula-scheme $B\Sigma_1$ or Σ_1-collection consists of sentences of the form*

$$\forall x < a \exists y \phi(x, y)] \to [\exists z \forall x < a \exists y < z \phi(x, y)],$$

where $\phi(x, y)$ is a Δ_0-formula. Essentially, this scheme expresses that a bounded quantifier can be pushed inside an existential quantification.

Definition 2.7. *For every x, y the predicate $Exp(x, y)$ expresses that $y = 2^x$.*

Exp was first shown to be a Δ_0-predicate in [4]. This result can also be found in [5](Chapter 5). It makes heavy use of coding of sequences in order to construct a Δ_0-predicate $Exseq(s)$ which states that s is an *exponential sequence* (a sequence consisting of pairs $(2^x, x)$):

$$\begin{aligned} Exseq(s) := \quad & Seq(s) \wedge (1, 0) \in s \wedge \forall y \leq s \forall z \leq s \, [(z, y) \in s \to (z = 1 \wedge y = 0) \\ & \vee (y > 0 \wedge \exists v \leq s \exists w \leq s((y = 2v \wedge z = w^2 \wedge (w, v) \in s) \\ & \vee (y = 2v + 1 \wedge z = 2w^2 \wedge (w, v) \in s)))] \end{aligned}$$

Here $Seq(s)$ is the Δ_0-predicate that states that s codes a sequence. See [5] for details on this coding. It's easy to see that this predicate, in essence, consists of a recursive definition of the sequence $(1, 0), (2, 1), (4, 2), (8, 3), \ldots, (2^x, x)$. Using this, we can define the predicate $Exp(x, y)$:

$$\begin{aligned} Exp(x, y) := \quad & (y = 1 \wedge x = 0) \\ & \vee (\exists s \leq bound(y) \, (Exseq(s) \wedge (y, x) \in s) \end{aligned}$$

Here, $bound(y)$ is a function of y that bounds the existential quantifier. The precise form of this function is derived from the pairing function. Note that the original result yields a predicate $Exp'(x, b, y)$ stating $b^x = y$, we only need the restricted version $Exp(x, y) := Exp(x, 2, y)$ with base 2.

Paris later proved the following result [6]:

Lemma 2.8. *$I\Delta_0$ proves the following:*
(a) $\forall x \exists^{\leq 1} y Exp(x, y)$
(b) $\forall x [\exists y Exp(x, y) \to \forall z < x \exists y Exp(z, y)]$
(c) $\forall x, y [Exp(x, y) \to Exp(x + 1, 2y)]$

Here $\exists^{\leq 1}$ means "there exists at most one ...".

Lemma 2.8 expresses nothing more than that $I\Delta_0$ can prove the basic algebraic laws about exponentiation that we are familar with. We now definite the theory $I\Delta_0 + Exp$ by adding the following axiom to $I\Delta_0$:

$$Exp := \forall x \exists y Exp(x, y)$$

These various fragments of PA will come into play when we examine the main theorem of this thesis. For now, we look at some results concerning these fragments.

Theorem 2.9. *Let $\mathscr{M}$ be a model of $I\Delta_0$ and let S_ϕ be the solution set of a Δ_0-formula $\phi(x, \mathbf{y})$ in $\mathscr{M}$, in other words $S_\phi = \{x \in M | \phi(x, \mathbf{y})\}$, with $\mathbf{y}$ being a sequence of parameters from M. If $S_\phi \neq 0$:*
(a) [Δ_0-MIN] S_ϕ has a minimum element.
(b) I is not Δ_0-definable, i.e. there is no Δ_0-formula ϕ such that $I = S_\phi$.
(c) [Δ_0-OVERSPILL] If S_ϕ contains a cut I of $\mathscr{M}$, then there is a $b \in M \setminus I$ such that $\{x \in M | x < b\} \subset S_\phi$.
(d) [Δ_0-MAX] If S_ϕ is bounded in $\mathscr{M}$, then S_ϕ has a maximum element.

Proof. Take a Δ_0-formula $\phi(x)$, such that S_ϕ is not empty.
(a) Assume S_ϕ has no minimum element. Consider $\phi^*(v) := \forall x \leq v \neg\phi(x)$. Since ϕ is Δ_0, so is ϕ^*. Clearly $\phi^*(0)$ holds in $\mathscr{M}$, since if it wouldn't, $\phi(0)$ would hold and 0 would be the minimum element of S_ϕ. Now, assuming that for some x, $\phi^*(x)$ holds in $\mathscr{M}$, it immediately follows that $\phi^*(x+1)$ holds as well, since $\phi(y)$ does not hold for all $y < x + 1$ and $x + 1$ is by assumption not the minimum element of S_ϕ. By Δ_0-induction on ϕ^* we conclude that $\forall v[\forall x \leq v \neg\phi(x)]$ or $\forall x \neg\phi(x)$, which is in contradiction with S_ϕ being non-empty.

(b) Suppose ϕ is a Δ_0-formula that defines I: $S_\phi = I$. Since I is a cut of $\mathscr{M}$, we have that $\mathscr{M} \models \phi(0) \wedge \forall x\ (\phi(x) \rightarrow \phi(x + 1))$ and using induction, $I = M$. Which is a contradiction with the fact that I was a cut.

(c) Suppose S_ϕ contains a cut I. Define the following Δ_0-formula:

$$\psi(x) = \forall y < x\ \phi(y)$$

Since I is closed downwards, we have that $I \subset S_\psi$. Part (b) yields that there exists a $b \in S_\psi \setminus I$, for if no such b would exist, $S_\psi = I$. It is clear that this b has the required property: $\{x \in M | x < b\} \subset S_\phi$.

(d) Assume that S_ϕ is bounded by $b \in M$, but has no maximal element. Define the following Δ_0-formula stating that for a parameter x, there exists a y between x and b that satisfies ϕ:

$$\phi(x) = \exists y \leq b\ (x \leq y \wedge \phi(y))$$

The solution set S_ψ is an initial segment of M, for if, in $\mathscr{M}$, $\psi(x)$ and $y < x$, then also $\psi(y)$. Since we assumed that S_ϕ had no maximal element, we can conclude that S_ψ also does not have a maximal element. But then S_ψ is a proper (since S_ψ is bounded by b) initial segment with no maximal element, hence a cut. This cut is defined by the Δ_0-formula $\psi(x)$, a contradiction with part (b). □

Theorem 2.10. [7] *Every cut of a model of $I\Delta_0$ that is closed under multiplication satisfies $I\Delta_0 + B\Sigma_1$.*

Proof. We have to show that the cut I proves the induction axiom for every Δ_0-formula ϕ. This follows from the stronger claim that if $\phi(x, y)$ is Δ_0 with $y \in M$ and the following statements hold:
(1) $\mathscr{M} \models \phi(0, y)$
(2) For all $x \in I$, $\mathscr{M} \models \phi(x, y) \to \phi(x + 1, y)$
then for all $x \in I$, $\mathscr{M} \models \phi(x, y)$.

To prove this claim, define $\psi(x, y) = \forall w \leq x\ \phi(w, y)$. If for some $a \in I$ we have that $\mathscr{M} \not\models \phi(a, y)$, then S_ψ is bounded in I. From Lemma 2.9d we then find that S_ψ has a maximal element $b \in I$, so $\psi(b)$, but not $\psi(b + 1)$, which means that $\phi(b)$, but not $\phi(b + 1)$ which contradicts item (2) in the assumptions of the claim.

To prove that I satisfies $B\Sigma_1$, we assume that $I \models \forall x < a \exists y\ \phi(x, y)$ for some Δ_0-formula ϕ. Consider the formula $\psi(z) = \forall x < a \exists y < z\ \phi(x, y)$. We have to show that $I \models \exists z \forall x < a \exists y < z\ \phi(x, y)$, or $I \models \exists c\ \psi(c)$. Assume this is not true, so for no $z \in I$, $\psi(z)$. Since $\psi(z)$ trivially holds for every upper bound of I, we have that $z \in I \Leftrightarrow \neg\psi(z)$, or $I = S_{\neg\psi}$, but $\neg\psi$ is Δ_0 and we get a contradiction with Lemma 2.9b. □

Theorem 2.11. [7] *Every countable model of $I\Delta_0 + B\Sigma_1 + Exp$ has an end extension to a model of $I\Delta_0 + B\Sigma_1$.*

Theorem 2.12. [6] *Given a model $\mathscr{M}$ of $I\Delta_0 + B\Sigma_1$ and $\mathscr{F}$ the family of all M-valued functions $f(x_1, \ldots, x_n)$ on M^n ($n \in \mathbb{N}^+$) with a Σ_1 graph (i.e. there exists a Σ_1-formula $\delta(x_1, \ldots, x_n, y)$ that defines the graph of a given $f \in \mathscr{F}$) and for some term $t(x_1, \ldots, x_n)$, $f(a_1, \ldots, a_n) \leq t(a_1, \ldots, a_n)$ for all $a_i \in M$. Then the expanded structure*

$$\mathscr{M}_{\mathscr{F}} := (\mathscr{M}, f)_{f \in \mathscr{F}}$$

satisfies $I\Delta_0(\mathscr{L}_{\mathscr{F}}) + B\Sigma_1(\mathscr{L}_{\mathscr{F}})$ where $\mathscr{L}_{\mathscr{F}}$ is obtained by adding names for each $f \in \mathscr{F}$ to the language of arithmetic.

2.4 Filters and ultraproduct constructions

A filter on a set X is a subset of the powerset of X satisfying certain properties. Filters are used as a tool to construct large models from a sequence of smaller models. This section deals with some of the basics regarding filters and lead up to Ultraproduct Theorem by J. Łoš which specifies the truth in a model constructed using a filter in terms of the smaller models and the filter that was used. This result it is very similar in idea to elements of a proof that will be discussed. In fact, it served as an inspiration.

Given a set X, the powerset of X is denoted by $\mathscr{P}(X)$.

Definition 2.13. *Given a set X, a* filter *on $\mathscr{P}(X)$ is a subset $\mathscr{U} \subset \mathscr{P}(X)$ satisfying the following properties:*

- *$\mathscr{U}$ is closed under intersections: $\forall Y, Z \subset X[Y \in \mathscr{U} \wedge Z \in \mathscr{U} \to Y \cap Z \in \mathscr{U}]$.*
- *$\mathscr{U}$ is upwards closed: $\forall Y, Z \subset X[Y \in \mathscr{U} \wedge Y \subset Z \to Z \in \mathscr{U}]$.*

So any non-empty filter on $\mathscr{P}(X)$ contains X and if a filter $\mathscr{U}$ contains $\emptyset$ then $\mathscr{U} = \mathscr{P}(X)$. We call a filter *principal* if it contains at least one singleton set.

An *ultrafilter* $\mathscr{U}$ is a filter with the extra property that for every $Y \subset X$ either $Y \in \mathscr{U}$ or $X \setminus Y \in \mathscr{U}$. Ultrafilters are a tool used to create larger models from smaller ones using a construction called the *ultraproduct construction*. Consider a sequence of structures $(\mathscr{M}_i)_{i\in\mathbb{N}}$ of the same language and an ultrafilter $\mathscr{U} \subset \mathscr{P}(\mathbb{N})$. Let F be the set of all functions $f : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} M_n$ such that $f(n) \in M_n$ for all $n \in \mathbb{N}$.

The set F will be the domain of our new structure after being modded out by an equivalence relation. This equivalence relation $\sim_{\mathscr{U}}$ is defined as follows:

$$f \sim_{\mathscr{U}} g \leftrightarrow \{n \in \mathbb{N} | f(n) = g(n)\} \in \mathscr{U}$$

In words: two functions in F are equivalent if and only if the set of point on which they coincide is contained in the ultrafilter. It's easy to see that this relation is indeed an equivalence relation. Reflexivity follows from the fact that $\mathbb{N} \in \mathscr{U}$. Symmetry holds trivially and transitivity follows from the closure of the ultrafilter under intersections. The set $N := F/ \sim_{\mathscr{U}}$ will serve as the domain for our new structure.

Relations, functions and constants are defined in a similar way. Given a sequence of binary relations R_n we have:

$$R([f], [g]) \leftrightarrow \{n \in \mathbb{N} | R_n(f(n), g(n))\} \in \mathscr{U}$$

For a sequence of (unary) functions h_n we have:

$$h([f]) := [\lambda n \in \mathbb{N}.h_n(f(n))]$$

And for a sequence of constants c_n we have a constant c in the new structure as follows:

$$c := [\lambda n \in \mathbb{N}.c_n]$$

Theorem 2.14. (Ultraproduct Theorem, J. Łoš) *Given a sequence of structures $(\mathscr{M}_i)_{i\in\mathbb{N}}$ of the same language and an ultrafilter $\mathscr{U} \subset \mathscr{P}(\mathbb{N})$ we have for the structure $\mathscr{N}$, as defined above, that for every formula $\phi(x_0, \ldots, x_{m-1})$ and for every sequence $f_0, \ldots, f_{m-1}$ of elements of F:*

$$\mathscr{N} \models \phi([f_0], \ldots, [f_{m-1}]) \leftrightarrow \{n \in \mathbb{N} | \mathscr{M}_n \models \phi(f_0(n), \ldots, f_{m-1}(n))\} \in \mathscr{U}$$

Proof. [8] □

Note that it is possible for all $\mathscr{M}_n$ to be identical in the ultraproduct construction.

2.5 Set theory arithmetized

Due to division with remainder, one can see that for every x and y, there are unique $u \leq y$, $v \leq 1$ and $w < 2^x$ such that:

$$y = 2^{x+1} * u + 2^x * v + w$$

This allows us to define the Δ_0-predicate $E(x, y)$ which represents the statement "the x-th bit of the binary expansion of y is 1."

$$E(x, y) := \exists u \leq y \; \exists v \leq 1 \; \exists w < 2^x \; (y = 2^{x+1} * u + 2^x * v + w) \wedge (v = 1)$$

The symbol E behaves like the membership relation, $E(x, y)$ representing $x \in y$. This so-called *Ackermann coding* can be used to simulate finite set theory in $I\Delta_0$. From now on, we'll use the notation xEy to denote $E(x, y)$. For a model $\mathscr{M}$ of $I\Delta_0$, we say that a subset X of M is coded in $\mathscr{M}$ iff there exists a $c \in M$ that codes X in the aobve mentioned way and we have $\forall x \; (x \in M \leftrightarrow xEc)$.

For any model $\mathscr{M}$ of $I\Delta_0$, the structure (M, E) is a model of a decent fragment of set theory. In particular, $\mathscr{M}$ satisfies the following axioms of set theory:

- **Extensionality**:

$$\forall x, y \; [\forall z(zEx \leftrightarrow zEy) \rightarrow x = y]$$

- **Conditional Paring**:

$$\forall x, y \text{ [if } x < y \text{ and } 2^y \text{ exists, then } \{x, y\} \text{ exists}$$

- **Union**: The union of a set is also a set, or

$$\forall x \exists y \ [\forall z (zEy \leftrightarrow \exists u (zEu \wedge uEx))]$$

- **Power Set**: If x codes a set and 2^x exists then there exists a y coding the powerset of x

- **Δ_0-Comprehension**: If z codes a set and 2^z exists, then for any Δ_0-formula $\phi(x, \mathbf{y})$ and for any $\mathbf{y}$, the set $\{xEz : \phi(x, \mathbf{y})\}$ exists.

For details, see [5](Chapter 1)

It's obvious that in any model $\mathscr{M} \models I\Delta_0$ and $c \in M$, the set of predecessors of c, $\bar{c} := \{x \in M : x < c\}$ is coded in $\mathscr{M}$ iff 2^c exists in $\mathscr{M}$. We define the function $Card(x) = t$ as "the cardinality of the set coded by x is t". From [5](Theorem I.1.41) we learn that this function is definable within $I\Delta_0$

We will need the notion of iterated exponentiation, the so-called *superexponential* function, defined as follows:

$$\begin{aligned} Superexp(0, x) &:= x \\ Superexp(n+1, x) &:= 2^{Superexp(n,x)} \end{aligned}$$

It is clear that any structure that is closed under exponentiation is also closed under finite iteration of it and therefore closed under superexponentiation of the form $Superexp(n, x)$ with n a standard natural number.

For any function $f : [X]^n \to \overline{d}$ (where $[X]^n$ denotes the set of increasing n-tuples of X), we say that a subset $H \subseteq X$ is *f-monochromatic* iff f is constant on $[H]^n$. Also, we say that H is *f-canonical* iff there exists a set $S \subseteq \{1, \ldots, n\}$ such that for all increasing sequences $\mathbf{s}$ and $\mathbf{t}$ of elements from H, we have that:

$$f(\mathbf{s}) = f(\mathbf{t}) \Leftrightarrow \forall i \in S \ (s_i = t_i)$$

The following result by Ramsey, Erdös and Rado garantuees the existence of monochromatic and canonical sets once certain conditions are met.

Theorem 2.15. *Given some set X and some function f. For each $n \in \mathbb{N}_{>0}$, the following is provable in $I\Delta_0$:*
(a) [Ramsey] If $a = Superexp(2n, bc)$, $b \geq n^2$, $Card(X) = a$ and f :

$[X]^n \rightarrow \bar{c}$*, then there exists a* $H \subseteq X$ *with* $Card(H) = b$ *such that* H *is* f*-monochromatic.*
(b) [Erdös, Rado] If $a = Superexp(4n, b * 2^{2^{2n^2-n}})$*,* $b \geq 4n^2$*,* $Card(X) = a$ *and* $f : [X]^n \rightarrow Y$*, then there exists a* $H \subseteq X$ *with* $Card(H) = b$ *such that* H *is* f*-canonical.*

Proof. Ramsey's theorem [9] states that for sufficiently large a and a c-coloring f, the set $[X]^n$ (with $Card(X) = a$) has a f-monochromatic subset of cardinality b. The lower bound on the value of a is determined by the Ramsey-function and although the exact values of this function are unknown, [9] does provide us with an upper bound to this function, an upper bound that is less than $Superexp(2n, bc)$.

Part (b) uses the proof of the Erdös-Rado canonical partition theorem [10]. This proof states: Suppose we have a set X of cardinality a and a $p([\overline{2n}]^2)$-coloring f of $[X]^2n$, with $p(S)$ being the number of partitions of S, we have that $p([\overline{2n}]^2) = p(\{1, \ldots, 2n^2 - n\})$ (as there are $2n^2 - n$ pairs (a_1, a_2) with $a_1 < a_2$ and $a_1, a_2 \in \{0, \ldots, 2n - 1\}$). A simple induction argument shows that for an s-element set, $p(s) < 2^{2^s}$. So $p([\overline{2n}]^2) < 2^{2^{2n^2-n}}$. If we have that there exists an f-monochromatic H with cardinality b, then we also have that for some $f : [X]^n \rightarrow Y$ (for some set Y), there exists an f-canonical subset H of X with cardinality b.

Using the above result, part (a), the substitutions $c \rightarrow p([\overline{2n}]^2)$ and $n \rightarrow 2n$ and the upper bound for $p([\overline{2n}]^2)$, (b) follows directly. □

3 A model from fixed points of an automorphism

The main result of Enayats article [1] is a theorem that states that a model of $I\Delta_0$ gives rise to a model of a stronger theory, $I\Delta_0 + B\Sigma_1 + Exp$, through the fixed points of a non-trivial automorphism. And vice versa, any model of $I\Delta_0 + B\Sigma_1 + Exp$ can be obtained from the fixed points of a non-trivial automorphism of a model of a weaker theory. Such results inspire faith in our choice of axiomization of arithmetic as it allows a stronger theory to be characterized in terms of a much weaker theory. The main result of this section is the following theorem:

Theorem 3.1. *Given a countable model* $\mathscr{M}$ *of the language* $\mathscr{L}_{PA}$*. The following are equivalent:*
(a) $\mathscr{M} = I_{fix}(j)$*, with* j *a non-trivial automorphism of some model* $\mathscr{M}^*$ *of*

$I\Delta_0$.
(b) $\mathscr{M} \models I\Delta_0 + B\Sigma_1 + Exp$.

Definition 3.2. *Given a model* $\mathscr{M}$ *and an automorphism* j *of* $\mathscr{M}$, $I_{fix}(j)$ *will denote the largest initial segment of* $\mathscr{M}$ *that is fixed under* j.

Proof of Theorem 3.1, (a) $\Rightarrow$ *(b).* The proof of the first part of the equivalence is divided in three separate lemmas:

Lemma 3.3. $I_{fix}(j) \models I\Delta_0$

Lemma 3.4. $I_{fix}(j) \models B\Sigma_1$

Lemma 3.5. $I_{fix}(j) \models Exp$

Proof of Lemma 3.3. Our first goal is to verify that $I_{fix}(j)$ is closed under addition and multiplication. Take two elements x and y of $I_{fix}(j)$. We have that $j(x+y) = j(x) + j(y) = x + y$. So $x + y$ is a fixed point of j. To show that $x+y \in I_{fix}(j)$, we need to show that for every $v < x+y$, $j(v) = v$. Take an arbitrary $v < x + y$. Then we have that either $v \leq x$ or $v > x$. In the first case, $j(v) = v$ by virtue of x being in $I_{fix}(j)$. In the second case, there exists a $w < y$ such that $v = x + w$. Since $w < y$, we have that $j(w) = w$ and therefore $j(v) = j(x + w) = j(x) + j(w) = x + w = v$.

To show that $I_{fix}(j)$ is closed under multiplication, take two elements x and y of $I_{fix}(j)$. We have that $j(x * y) = x * y$. Take an arbitrary $v < x * y$. Using division with remainder, we find that $v = r * x + q$ with $r < y$ and $q < x$. Working this out, we get:

$$j(v) = j(r * x + q) = j(r) * j(x) + j(q) = r * x + q = v$$

as desired.

Since $I_{fix}(j)$ is a cut of a model of $I\Delta_0$, Lemma 2.10 yields that $I_{fix}(j) \models I\Delta_0$. □

Proof of Lemma 3.4. This proof also comes from Lemma 2.10. Since j is a non-trivial automorphism of $\mathscr{M}^*$, $I_{fix}(j)$ is a cut of $\mathscr{M}^*$ and we know that $I_{fix}(j)$ is closed under multiplication, so Lemma 2.10 is directly applicable. □

Proof of Lemma 3.5. The proof consists of three steps.
Step 1:
Claim: If $a \in I_{fix}(j)$ and 2^a is defined in $\mathscr{M}$, then $2^a \in I_{fix}(j)$.

Given a $y < 2^a$, we can find an element c that is the code for a subset of $\{0, 1, \ldots, a-1\}$ that corresponds to the binary representation of y:

$$y = \Sigma_{iEc} 2^i$$

This is possible because the base-2 expansion of a positive integer can be realized in $I\Delta_0$ provided some power of 2 exceeds the integer [5]. Now we have that iEc implies that $j(i) = i$, since iEc implies that $i < a$ and $a \in I_{fix}(j)$. From this it follows that for all i, $iEc \Leftrightarrow j(i)Ej(c) \Leftrightarrow iEj(c)$. Since (M, E) satisfies extensionality, this means that $j(c) = c$

So we have:

$$j(y) = j(\Sigma_{iEc}2^i) = \Sigma_{iEj(c)}2^i = \Sigma_{iEc}2^i = y$$

So for every $y < 2^a$ we have that $j(y) = y$ and therefore $j(2^a) = 2^a$ and $2^a \in I_{fix}(j)$.

Step 2:
Define the set $J := \{m \in M : 2^m \text{ is defined in } \mathscr{M}\}$. This is an initial segment of $\mathscr{M}$.
Claim: $K := \{2^x : x \in J\}$ is cofinal in M.
Note that K is the set of powers of 2 that is defined in $\mathscr{M}$. We prove the claim by contradiction: suppose some c in M is an upper bound of K. Then K can be written as the solution-set, $\{x|\phi(x, c)\}$, of the following Δ_0-predicate $\phi(x, c)$:

$$\phi(x, c) := x < c \wedge \exists y < cExp(x, y)$$

By $I\Delta_0$-MAX (Lemma 2.9b), the solution set, which was K, has a maximum element, but this would mean that there is a largest power of 2 defined in $\mathscr{M}$, which is absurd.

Step 3:
The goal is to prove that if $a \in I_{fix}(j)$, then 2^a is defined and is also an element of $I_{fix}(j)$. Because of the result of step 1, it suffices to show that for every $a \in I_{fix}(j)$, 2^a is defined as step 1 garantuees that is 2^a is defined, it automatically is a member of $I_{fix}(j)$. So we need to prove that $I_{fix}(j) \subsetneq J$. Assume the contrary, $J \subseteq I_{fix}(j)$. Since j is a non-trivial automorphism, we can find $a \in M \setminus I_{fix}(j)$.

Since the set of powers of 2 is cofinal in M, the result of stage 2, we can find $m \in J$ with $2^m > a$. By the assumption that $J \subseteq I_{fix}(j)$ we have that $m \in I_{fix}(j)$ and because of the result of step 1, we find that $2^m \in I_{fix}(j)$. Because $I_{fix}(j)$ is an initial segment, this means that also $a \in I_{fix}(j)$, a contradiction. Therefore: $I_{fix}(j) \subsetneq J$ and we find that for all $x \in I_{fix}(j)$, 2^x is defined, so $I_{fix}(j) \models Exp$. □

These three lemmas together prove the claim that $\mathscr{M}$ is a model of $I\Delta_0 + B\Sigma_1 + Exp$. □

Proof of Theorem 3.1, (b) $\Rightarrow$ (a). The proof of the (b) $\Rightarrow$ (a) part of Theorem 3.1 is more involved. Given a model $\mathscr{M}$ of $I\Delta_0 + B\Sigma_1 + Exp$, our goal is to construct a model of $I\Delta_0$ and a non-trivial automorphism j with the properties required by the theorem. We will construct such a model through the use of an appropriately chosen ultrafilter. In this part of the proof, the following conventions and definitions will be used:

- $\mathscr{M}$ is a model of $I\Delta_0 + B\Sigma_1$, I is a cut of $\mathscr{M}$ that satisfies Exp. c is an element of $M \setminus I$ such that 2^c exists in $\mathscr{M}$. Existence of such a c follows from the proof of Lemma 3.5 (step 2). This step shows that the set of powers of 2 is cofinal in M. So there exists an x such that $2^x \notin I$. But since I satisfies Exp, this means that this x must be in $M \setminus I$ and is the desired element c. Since for $1 < x \leq y$ we have $x+y \leq xy \leq 2^{x+y} \leq 2^{2y}$, I is also closed under addition and multiplication.

- $[X]^n$ ($n \in \mathbb{N}$) is the collection of all increasing n-tuples of elements of X. $[c]^n$ is the collection of all increasing n-tuples of elements of $0, 1, 2 \ldots c$.

- $\mathscr{F}$ and $\mathscr{L}_{\mathscr{F}}$ are as in Theorem 2.12. $\mathscr{F}_c$ is the family of functions $[c]^n \to M$ obtained by restricting the domains of all the n-ary functions in $\mathscr{F}$ to $[c]^n$.

- $\overline{c}$ is the set of predecessors of c.

- Let $\mathscr{U} \subseteq \mathscr{P}(\overline{c})$ be a filter. We say that $\mathscr{U}$ is *I-complete* if for every function $f \in \mathscr{F}_c$ and element $i \in I$, if $f : \overline{c} \to \overline{i}$, then there exists an $X \in \mathscr{U}$ on which f is constant. Suppose $\mathscr{U}$ is I-complete and take any $Y \in \mathscr{P}(\overline{c})$ and let χ_Y be the characteristic function of Y. We have that $\chi_Y : \overline{c} \to \overline{i}$ for $i = 2$. Since $\mathscr{U}$ is I-complete, there is an $X \in \mathscr{U}$ on which χ_Y is constant. Suppose $\chi_Y \rceil X = 1$, then $X \subseteq Y$ and therefore $Y \in \mathscr{U}$, by the property of upwards completion of a filter. Similarly, if $\chi_Y \rceil X = 0$, then $X \subseteq \overline{c} \setminus Y$ and $\overline{c} \setminus Y \in \mathscr{U}$. From this it follows that if a filter is I-complete then it is an ultrafilter.

- A filter $\mathscr{U} \subseteq \mathscr{P}(\overline{c})$ is *Ramsey* if for every $f \in \mathscr{F}_c$ and $n \in \mathbb{N}_{>0}$, if f is a function from $[\overline{c}]^n$ to $\{0, 1\}$, then there exists a $H \in \mathscr{U}$ on which f is constant (or, H is f-monochromatic).

- A filter $\mathscr{U} \subseteq \mathscr{P}(\overline{c})$ is *canonically Ramsey* if for $f \in \mathscr{F}_c$ and $n \in \mathbb{N}_{>0}$, if f is a function from $[\overline{c}]^n$ to M, then there exists a $H \in \mathscr{U}$ such that H is f-canonical. If $\mathscr{U}$ is a non-principal and canonically Ramsey ultrafilter, it is also Ramsey. To see this, assume that $\mathscr{U}$ is non-principal and canonically Ramsey and consider a function $f : [\overline{c}]^n \to \{0, 1\}$. We are given a set $H \in \mathscr{U}$ such there exists a set $S = \{1, \ldots, n\}$ such that for all sequences $s_1 < \ldots < s_n$ and $t_1 < \ldots < t_n$ from $[H]^n$:

$$f(\mathbf{s}) = f(\mathbf{t}) \Leftrightarrow \forall i \in S \ (s_i = t_i)$$

Suppose that S is empty, then f is constant on $[H]^n$ and we are done. Next, assume that S is nonempty and take $j \in S$. Fix $\mathbf{t} \in [H]^n$ such that $f(\mathbf{t}) = 0$ (If such a $\mathbf{t}$ would not exist, f would be constant with value 1 and we would be done. Now define $Y := H \setminus \{t_j\}$. Since $H \in \mathscr{U}$ and $\mathscr{U}$ is non-principal, we have that $Y \in \mathscr{U}$ (Since if $Y \notin \mathscr{U}$, then $Y^C \in \mathscr{U}$ and $\{t_j\} = H \cap Y^C \in \mathscr{U}$, contradiction).

We have that for all $\mathbf{s} \in [Y]^n$ that $s_j \neq t_j$ and therefore, $f(\mathbf{s}) \neq f(\mathbf{t})$. Which means that f is constant with value 1 on Y, a member of $\mathscr{U}$.

- A filter $\mathscr{U} \subseteq \mathscr{P}(\overline{c})$ is *I-tight* if for $f \in \mathscr{F}_c$ and $n \in \mathbb{N}_{>0}$, if f is a function from $[\overline{c}]^n$ to M, then there exists a $H \in \mathscr{U}$ such that either f is constant or is bounded from below by some element of $M \setminus I$.
- A set $X \in \mathscr{P}(\overline{c})$ is *I-large* if $Card(X) \notin I$.

The goal is now to construct an ultrafilter on $\mathscr{P}(\overline{c})$ with desirable properties that can be used to construct the model we need for the proof of Theorem 3.1. Leading up to the construction of this ultrafilter are 3 lemmas that deal with properties of I-large sets.

Lemma 3.6. *If X is I-large and for some $m \in I, m > 0$, $f \in \mathscr{F}_c$ is a function $\overline{c} \to \overline{m}$, then there exists an I-large subset of X on which f is constant.*

Proof. Define $\lfloor \frac{x}{y} \rfloor := \max\{t \leq x : ty \leq x\}$. If for some b, m we have that $b \notin I$ and $m \in I$, then $\lfloor \frac{b}{m} \rfloor \notin I$. To see this, suppose that $\lfloor \frac{b}{m} \rfloor \in I$. We then have that $\max\{t \leq b : tm \leq b\} \in I$ and therefore there exists a t such that $tm \in I$ and $t(m+1) \notin I$, but I is closed under addition and multiplication.

Let $b = Card(X)$. Since X is I-large, $b \in M \setminus I$. Let S_i be the sequence of levelsets of f:

$$S_i := \{x \in X : f(x) = i\}$$

Suppose that for all $i \leq m$ we have that $Card(S_i) < \lfloor \frac{b}{m} \rfloor - 1$. Since $X = \bigcup_{i<m} S_i$, the following holds:

$$b = Card(X) < m(\lfloor \frac{b}{m} \rfloor - 1) \leq b - m$$

Contradiction. So there is at least one i such that $Card(S_i) \geq \lfloor \frac{b}{m} \rfloor$ and therefore $Card(S_i) \notin I$. $\square$

Lemma 3.7. *Given an I-large set X, $f \in \mathscr{F}_c$, $n \in \mathbb{N}_{>0}$. If $f : [X]^n \to M$ then there exists an I-large, f-canonical subset of X.*

Proof. Since I is closed under Exp, we have that for every x in I and y in $\mathbb{N}_{>0}$, that $\exists z \in I\ \mathscr{M} \models Superexp(y, x)$. In particular:

$$\exists j \in I\ \mathscr{M} \models j = Superexp(4n, i * 2^{2^{2n^2-n}})$$

Using Theorem 2.15b, we see that this implies that for every $i \in I$, there exists an f-canonical subset of X with cardinality i. Using the overspill principle, this gives us a subset Y of X that is f-canonical and $Card(Y) \notin I$, so Y is I-large. $\square$

Lemma 3.8. *Let X and f be as in Lemma 3.7. There exists an I-large $Y \subseteq X$ such that one of the two following statements holds:*
(a) f is constant on $[Y]^n$.
(b) f is bounded from below by some element of $M \setminus I$.

Proof. For every $m \in M$, define $f_m : [X]^n \to \{0, 1\}$ as follows:

$$f_m(\mathbf{x}) = 0 \Leftrightarrow f(\mathbf{x}) \leq m$$

We claim that for each m, there exists an I-large set $Y_m \subseteq X$ such that f_m is constant on $[Y_m]^n$.

Proof of claim: Apply Lemma 3.7 to X, f_m. We get an I-large set $Z_m \subseteq X$ that is f_m-canonical. This means that there exists a set $S \subseteq \{1, \ldots, n\}$ such that:

$$\forall \mathbf{s}, \mathbf{t} \in [Z_m]^n\ [f_m(\mathbf{s}) = f_m(\mathbf{t}) \Leftrightarrow \forall i \in S(s_i = t_i)]$$

Consider the set S. If S is empty, we have that f_m is constant and we are done. Suppose that f_m is not constant, then we have that $S \neq \emptyset$, so take $i \in S$. Fix a $\mathbf{t} \in [Z_m]^n$ such that $f_m(\mathbf{t}) = 0$. This is possible since f_m only has 0 and 1 in its range and is assumed to not be constant. Now define $Y_m = Z_m \setminus \{t_i\}$.

We now have for all $\mathbf{s} \in [Y_m]^n$ that $s_i \neq t_i$ and by definition of Z_m being f_m-canonical, we have that $f_m(\mathbf{s}) \neq f_m(\mathbf{t})$, hence $f_m(\mathbf{s}) = 1$ for all $\mathbf{s} \in [Y_m]^n$ and f_m is constant on $[Y_m]^n$ (or: Y_m is f_m-monochromatic). This concludes the proof of the claim.

We will prove this lemma by making a distinction between two different cases:
(I) - There is an $i \in I$ such that $f_i(Y_i) = \{0\}$.
(II) - For all $i \in I$, $f_i(Y_i) = \{1\}$.

Case (I): Take $i \in I$ such that $f_i(Y_i) = \{0\}$. By definition of f_i, we have that $\forall \mathbf{x} \in [Y_i]^n\ f(\mathbf{x}) \leq i$. So $f : [Y_i]^n \to \bar{i}$. We can now apply 3.6 and find an I-large subset of Y_i on which f is constant and thus statement (a) holds.

Case (II): Consider the following $\mathscr{L}_{\mathscr{F}}$-formula:

$$\phi(v) := \exists Y \in \mathscr{P}(X)(Card(Y) > v \wedge \forall \mathbf{x} \in [Y]^n\ f_v(\mathbf{x}) = 1)$$

Since we can use the Ackermann coding to simulate set-theory in $I\Delta_0$, this is a Δ_0-formula. For every $i \in I$, $\phi(i)$ holds with $Y = Y_i$. Therefore, by Δ_0-OVERSPILL, there exists an $m_0 \in M \setminus I$ for which $\phi(m_0)$ holds. This means that there is an $Y \subseteq X$ with $Card(Y) > m_0$ (and therefore $Card(Y) \notin I$, making Y I-large) and for all $\mathbf{x} \in [Y]^n$, $f_{m_0}(\mathbf{x}) = 1$, so $f(\mathbf{x}) > m_0$ for all $\mathbf{x} \in [Y]^n$. We see that statement (b) holds in this case. □

With Lemmas 3.6, 3.7 and 3.8 we can prove that there exists an ultrafilter on $\mathscr{P}(\bar{c})$ which has certain properties that will prove useful later on.

Theorem 3.9. *There exists a non-principal ultrafilter $\mathscr{U} \subseteq \mathscr{P}(\bar{c})$ with the following properties:*
(a) $\mathscr{U}$ is I-complete.
(b) $\mathscr{U}$ is canonically Ramsey.
(c) $\mathscr{U}$ is I-tight.
(d) $\{Card(X) : X \in \mathscr{U}\}$ is downward cofinal in $M \setminus I$.

Proof. Let $\langle f_n : n < \omega \rangle$ enumerate all maps in $\mathscr{F}_c$ with $\bar{c}$ as domain and a range bounded in I. And let $\langle g_n : n < \omega \rangle$ enumerate all maps in $\mathscr{F}_c$ with $g_n : [\bar{c}]k_n \to M$. Let $\langle a_n : n \in \omega \rangle$ be a sequence of elements of M such that $a_0 \leq c$ and the sequence is downward cofinal in $M \setminus I$ (i.e. for all $n < \omega$, there exists $m \in M \setminus$ such that $m < a_n$).

With Lemmas 3.6, 3.7 and 3.8, we can inductively construct four sequences of I-large sets in $\mathscr{P}(\bar{c})$ such that these sets, $\langle W_n : n < \omega \rangle$, $\langle X_n : n < \omega \rangle$, $\langle Y_n : n < \omega \rangle$, $\langle Z_n : n < \omega \rangle$, satisfy the following properties for any $n < \omega$:
(1) $W_{n+1} \subseteq Z_n \subseteq Y_n \subseteq X_n \subseteq W_n$.
(2) f_n is constant on W_n.
(3) X_n is g_n-canonical.
(4) g_n is constant on $[Y_n]^{k_n}$ or g_n is bounded by an element of $M \setminus I$.
(5) $Card(Z_n) < a_n$.

This construction goes as follows:
First we construct W_0. Apply Lemma 3.6 with $X = \overline{c}$ and $f = f_0$. The lemma yields an I-large subset of $\overline{c}$ on which f_0 is constant. Define W_0 to be this subset.

For any $n < \omega$, suppose we have W_n satisfying the above properties. Apply 3.7 with $X = \overline{c}$ and $f = g_n$. We are given an I-large subset, call it G, of $\overline{c}$ which is g_n-canonical. Now let $X_n = W_n \cap G$. Similarly, Lemma 3.8 provides us with an I-large set, H with either g_n constant on $[H]^{k_n}$ or g_n is bounded from above in $[H]^{k_n}$ by an element from $M \backslash I$. Take $Y_n = X_n \cap H$. To obtain Z_n, simply reduce Y_n until an I-large set remains with $Card(Z_n) < a_n$. Finally, to construct W_{n+1}, apply Lemma 3.6 with $X = W_n$ and $f = f_{n+1}$ to obtain a set F on which f_{n+1} is constant. W_{n+1} is now $Z_n \cap F$.

We now define the set $\mathscr{U} := \{S \in \mathscr{P}(\overline{c}) : \exists n < \omega (W_n \subseteq S)\}$ and claim that this is an ultrafilter with the desired properties.

First we verify that $\mathscr{U}$ is a filter. $\mathscr{U}$ is obviously upwards closed, which leaves the matter of being closed under intersections. Suppose $S, T \in \mathscr{U}$. We can find sets W_{n_S} and W_{n_T} such that $W_{n_S} \subseteq S$ and $W_{n_T} \subseteq T$. Without loss of generality, assume that $n_S \geq n_T$, then by the inductive defintion of W_n, we have that $W_{n_S} \subseteq W_{n_T} \subseteq T$. So W_{n_S} is contained in both S and T, which means that $W_{n_S} \subseteq S \cap T$ and hence $S \cap T \in \mathscr{U}$.

(a) $\mathscr{U}$ is I-complete:
Given a function $f : \overline{c} \rightarrow \overline{i}$ for some $i \in I$ then there is a $k < \omega$ such that $f = f_k$. By property (2) of the inductive defintion of $\mathscr{U}$, f_k is constant on W_k. Clearly $W_k \in \mathscr{U}$ which proves that for every function in $\mathscr{F}_c$ with range bounded in I, there is a set $H \in \mathscr{U}$ on which this function is constant. Note that the I-completeness of $\mathscr{U}$ immediately implies that $\mathscr{U}$ is an ultrafilter.

(b) $\mathscr{U}$ is canonically Ramsey:
For any function $f \in \mathscr{F}_c$ with $f : [\overline{c}]^n$ there is a l such that $g_l = f$. Property (3) of the inductive definition yields that X_l is f-canonical and since $X_l \supseteq W_{l+1}$, we have that $X_l \in \mathscr{U}$.

(c) $\mathscr{U}$ is I-tight:
Like the previous two properties, this also follows fairly directly from the inductive defintion of $\mathscr{U}$, this time using property (4).

(d) $\{Card(X) : X \in \mathscr{U}\}$ is downward cofinal in $M \setminus I$:
We have to show that for every $m \in M \setminus I$ there is an $X \in \mathscr{U}$ such that $Card(X) < m$. Since every Z_n is in $\mathscr{U}$ (since $W_{n+1} \subseteq Z_n$), $Card(Z_n) < a_n$ and for every $m \in M \setminus I$ there is an $a_n < m$, we immediately see that the cofinality property holds. $\square$

The next step in our proof is to construct a suitable model using the newly found ultrafilter. We will make a family of models $\mathscr{N}_{\mathscr{U},\mathbb{L}}$ with $\mathbb{L}$ an arbitrary linear order. Later on, we will fix $\mathbb{L}$ to obtain a model with desirable properties.

Using the ultrafilter constructed in Theorem 3.9, we define the following family of partial n-types $\Gamma_n(x_1,\ldots,x_n)$ over $\mathscr{L}_{\mathscr{F}}$:

$$\phi(x_1,\ldots,x_n) \in \Gamma_n(x_1,\ldots,x_n)$$
$$\Leftrightarrow \exists S \in \mathscr{U} : \mathscr{M}_{\mathscr{F}} \models \phi(a_1,\ldots,a_n) \text{ for all sequences } a_1 < \ldots < a_n \text{ from } S$$

Define the set $T_{\mathscr{U}}$ simply as the union of the family of n-types:

$$T_{\mathscr{U}} := \bigcup_{n\in\mathbb{N}_{>0}} \Gamma_n(x_1,\ldots,x_n)$$

For any linear order, $\mathbb{L}$, the extended language $\mathscr{L}_{\mathscr{F},\mathbb{L}}$ is obtained by adding constant symbols l for each $l \in \mathbb{L}$ to the language $\mathscr{L}_{\mathscr{F}}$. In this extended language, the theory $T_{\mathscr{U},\mathbb{L}}$ is defined as follows:

$$T_{\mathscr{U},\mathbb{L}} := \{\phi(l_1,\ldots,l_n) : \phi \in T_{\mathscr{U}} \wedge l_1 <_{\mathbb{L}} \ldots <_{\mathbb{L}} l_n\}$$

Theorem 3.10. *$T_{\mathscr{U},\mathbb{L}}$ is consistent and $\Delta_0(\mathscr{L}_{\mathscr{F},\mathbb{L}})$-complete.*

Proof. Consider a finite subset T' of $T_{\mathscr{U},\mathbb{L}}$. Let n denote the maximum number of variables in the sentences of T'. Augment all $\phi \in T'$ with dummy-variables so that each $\phi \in T$ has n variables. For each $phi(l_1,\ldots,l_n) \in T'$, we have a $S \in \mathscr{U}$ such that $\mathscr{M}_{\mathscr{F}}$ satisfies $\phi(x_1,\ldots,x_n)$ for all increasing sequences of parameters from S.

Now take the intersection of all these sets. This intersection will be non-empty, since $\mathscr{U}$ is a non-principal ultrafilter, so it is possible to select an increasing sequence of parameters, $a_1 < \ldots < a_n$, from S such that for each $\phi(l_1,\ldots,l_n) \in T'$ we have that $\mathscr{M}_{\mathscr{F}} \models \phi(a_1,\ldots,a_n)$. Now augment $\mathscr{M}_{\mathscr{F}}$ with interpretations for each l_i: $l_i^{\mathscr{M}_{\mathscr{F}}} = a_i$.

This gives us a model for T'. Since T' was arbitrarily chosen, it follows that each finite subset of $T_{\mathscr{U},\mathbb{L}}$ has a model and therefore, by Compactness, $T_{\mathscr{U},\mathbb{L}}$ has a model.

To prove $\Delta_0(\mathscr{L}_{\mathscr{F},\mathbb{L}})$-completeness, we take an arbitrary Δ_0-formula $\phi(x_1,\ldots,x_n)$ and consider:

$$S := \{(x_1,\ldots,x_n) \in [\overline{c}]^n : \mathscr{M}_{\mathscr{F}} \models \phi(x_1,\ldots,x_n)\}$$

The characteristic function χ_S is a function from M^n to $\{0,1\}$, so in particular also to M. The graph of χ_S is defined by:

$$\begin{array}{rcl} \psi(x_1,\ldots,x_n,y) & := & (x_1 < \ldots < x_n < c \wedge \phi(x_1,\ldots,x_n) \wedge y = 1) \\ & \vee & (\neg(x_1 < \ldots < x_n < c \wedge \phi(x_1,\ldots,x_n)) \wedge y = 0) \end{array}$$

Since this is a Σ_1-graph and since χ_S is bounded by the term $t(a_1, \ldots, a_n) = 1$, we find that $\chi_S \in \mathscr{F}$ (see Theorem 1.12 for the definition of $\mathscr{F}$). Because $\mathscr{U}$ has the Ramsey-property, there exists a $H \in \mathscr{U}$ on which χ_S is constant. If $\chi_S(x_1, \ldots, x_n) = 1$ for all $x_i \in H$, then $\phi(x_1, \ldots, x_n) \in \Gamma_n(x_1, \ldots, x_n)$. If $\chi_S(x_1, \ldots, x_n) = 0$ for all $x_i \in H$, then $\neg\phi(x_1, \ldots, x_n) \in \Gamma_n(x_1, \ldots, x_n)$ □

We now construct a model of $T_{\mathscr{U},\mathbb{L}}$. Define the following equivalence relation $\sim$ on terms $\tau = f(l_1, \ldots, l_n)$ with $f \in \mathscr{F}$, $(l_1, \ldots, l_n) \in [\mathbb{L}]^n$:

$$f(l_1, \ldots, l_r) \sim g(l_1, \ldots, l_s) \Leftrightarrow (f(l_1, \ldots, l_r) = g(l_1, \ldots, l_s)) \in T_{\mathscr{U},\mathbb{L}}$$

So two terms are equivalent iff their equality is in the theory $T_{\mathscr{U},\mathbb{L}}$. We now verify that $\sim$ is indeed an equivalence relation. For any term $\tau(l_1, \ldots, l_n) = f(l_1, \ldots, l_n)$ with $(l_1, \ldots, l_n) \in [\mathbb{L}]^n$ and $f \in \mathscr{F}$ we have that $(\tau = \tau) \in T_{\mathscr{U},\mathbb{L}}$ precisely when

$\exists S \in \mathscr{U}$: $\mathscr{M}_{\mathscr{F}} \models (f(a_1, \ldots, a_n) = f(a_1, \ldots, a_n))$ for all sequences $a_1 < \ldots < a_n$ from S

This verifies reflexivity. Symmetry of $\sim$ follows from the symmetry of $=$ (if $\mathscr{M}_{\mathscr{F}} \models (f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n))$ then $\mathscr{M}_{\mathscr{F}} \models (g(a_1, \ldots, a_n) = f(a_1, \ldots, a_n))$. Transitivity requires the intersection-property of ultrafilters. Suppose $f(l_1, \ldots, l_r) \sim g(l_1, \ldots, l_s)$ and $g(l_1, \ldots, l_s) \sim h(l_1, \ldots, l_t)$. We have that $(f(l_1, \ldots, l_r) = g(l_1, \ldots, l_s)) \in T_{\mathscr{U},\mathbb{L}}$ and $(g(l_1, \ldots, l_s) = h(l_1, \ldots, l_t)) \in T_{\mathscr{U},\mathbb{L}}$. This means that

$\exists S_1 \in \mathscr{U}$:
$\mathscr{M}_{\mathscr{F}} \models (f(a_1, \ldots, a_{n_f}) = g(a_1, \ldots, a_{n_g}))$ for all increasing (a_i) from S_1
$\exists S_2 \in \mathscr{U}$:
$\mathscr{M}_{\mathscr{F}} \models (g(a_1, \ldots, a_{n_g}) = h(a_1, \ldots, a_{n_h}))$ for all increasing (a_i) from S_2

Now take $S_3 := S_1 \cup S_2$. From the definition of filters, it follows that $S_3 \in \mathscr{U}$. With this, and the transitivity of $=$, we have

$\mathscr{M}_{\mathscr{F}} \models (f(a_1, \ldots, a_{n_f}) = h(a_1, \ldots, a_{n_h}))$ for all increasing sequences (a_i) from S_3

So:

$$f(l_1, \ldots, l_r) \sim h(l_1, \ldots, l_t)$$

and transitivity is verified.

Having defined the universe for the new model, we now define the interpretations of $+$, $\times$ and $<$ in the model $\mathscr{N}_{\mathscr{U},\mathbb{L}}$:

$$\begin{array}{rcl}[f(l_1,\ldots,l_r)]\oplus[g(l'_1,\ldots,l'_s)] & = & [h(l''_1,\ldots,l''_t)] \\ & \Updownarrow & \\ (f(l_1,\ldots,l_r)+g(l'_1,\ldots,l'_s) & = & h(l''_1,\ldots,l''_t))\in T_{\mathscr{U},\mathbb{L}}\end{array}$$

Existence of h is easy to prove: Given f and g in $\mathscr{F}$, define $h=f+g$. That $h\in\mathscr{F}$ is straightforward. To see that this definition is independent of the representative, suppose $[f(\ldots)]\oplus[g(\ldots)]=h(\ldots)]$ and $[f(\ldots)]\oplus[g(\ldots)]=k(\ldots)]$. It follows that

$$\begin{array}{rcl}(f(l_1,\ldots,l_r)+g(l'_1,\ldots,l'_s) & = & h(l''_1,\ldots,l''_t))\in T_{\mathscr{U},\mathbb{L}} \\ (f(l_1,\ldots,l_r)+g(l'_1,\ldots,l'_s) & = & k(l''''_1,\ldots,l''''_v))\in T_{\mathscr{U},\mathbb{L}}\end{array}$$

Transitivity of $=$ coupled with Δ_0-completeness of $T_{\mathscr{U},\mathbb{L}}$ garantuees that

$$(h(l''_1,\ldots,l''_t)=k(l'''_1,\ldots,l'''_v))\in T_{\mathscr{U},\mathbb{L}}$$

and therefore $h(\ldots)\sim k(\ldots)$.

Multiplication is defined similarly and the proof of it being well-defined follows the same steps. The ordering relation is defined as follows:

$$[f(l_1,\ldots,l_r)]\lhd[g(l'_1,\ldots,l'_s)]\Leftrightarrow(f(l_1,\ldots,l_r)<g(l'_1,\ldots,l'_s))\in T_{\mathscr{U},\mathbb{L}}$$

Independence of the representative in this case follows directly from the definition of $\sim$ and the properties of $<$.

Recall that $c_m\in\mathscr{F}$ is the constant function with value m. We have an embedding $e_1:\mathscr{M}\to\mathscr{N}_{\mathscr{U},\mathbb{L}}$:

$$m\longmapsto_{e_1}[c_m(l)]$$

with $l\in\mathbb{L}$. With this embedding, we can identify each $m\in M$ with $[c_m(l)]\in N_{\mathscr{U},\mathbb{L}}$. Similarly, we use the identity function $id:M\to M$ to find the following embedding:

$$l\longmapsto_{e_2}[id(l)]$$

The embedding e_2 identifies each $[id(l)]$ with $l\in\mathbb{L}$.

Theorem 3.11. *For any Σ_1-formula $\phi(x_1,\ldots,x_k)$ of $\mathscr{L}_{PA}$ and $[\tau_1],\ldots[\tau_k]$, elements of $N_{\mathscr{U},\mathbb{L}}$, the following two conditions are equivalent:*
(a) $\mathscr{N}_{\mathscr{U},\mathbb{L}}\models\phi([\tau_1],\ldots,[\tau_k])$
(b) $\phi(\tau_1,\ldots,\tau_k)\in T_{\mathscr{U},\mathbb{L}}$

Proof. We prove this lemma by induction on the structure of the formula ϕ. First, assume that ϕ is atomic. Equivalence of (a) and (b) follows directly from the definition of the operations $\oplus$ and $\otimes$ and the definition of the ordering relation $\lhd$.

Next, assume that ϕ is of the form $\theta_1 \wedge \theta_2$. First we prove (a) $\Rightarrow$ (b) for this case. We have that $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta_1([\tau_1], \ldots, [\tau_k]) \wedge \theta_2([\tau_1], \ldots, [\tau_k])$ and therefore also that $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta_1([\tau_1], \ldots, [\tau_k]$ and $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta_2([\tau_1], \ldots, [\tau_k])$. From the induction hypothesis we get that $\theta_1 \in T_{\mathscr{U},\mathbb{L}}$ and $\theta_2 \in T_{\mathscr{U},\mathbb{L}}$. By the definition of $T_{\mathscr{U},\mathbb{L}}$, this means that there exist $S_i \in \mathscr{U}$ (with $i \in \{1, 2\}$) such that $\mathscr{M}_{\mathscr{F}} \models \theta_i(a_1, \ldots, a_k)$ for all sequences $a_1 < \ldots < a_k$ of elements from S_i. We now have that for all sequences $a_1 < \ldots < a_k$ of elements from $S_1 \cap S_2$, $\mathscr{M}_{\mathscr{F}} \models \theta_1(a_1, \ldots, a_k) \wedge \theta_2(a_1, \ldots, a_k)$. By the properties of a filter, $S_1 \cap S_2 \in \mathscr{U}$ and we find that $theta_1 \wedge \theta_2 \in T_{\mathscr{U},\mathbb{L}}$.

For (b) $\Rightarrow$ (a), consider that if $\theta_1 \wedge \theta_2 \in T_{\mathscr{U},\mathbb{L}}$ then $\theta_1 \in T_{\mathscr{U},\mathbb{L}}$ and $\theta_2 \in T_{\mathscr{U},\mathbb{L}}$ (this follows directly from the definition of $T_{\mathscr{U},\mathbb{L}}$). Therefore, by the induction hypothesis, $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta_1$ and $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta_2$ and consequently $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta_1 \wedge \theta_2$.

Suppose $\phi = \neg\theta$ and the equivalence of (a) and (b) is given for θ. We have that:

$$\begin{aligned}
\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \neg\theta([\tau_1], \ldots, [\tau_k]) \quad &\Leftrightarrow \quad \mathscr{N}_{\mathscr{U},\mathbb{L}} \not\models \theta([\tau_1], \ldots, [\tau_k]) \\
\text{(I.H.)} \quad &\Leftrightarrow \quad \theta(\tau_1, \ldots, \tau_k) \notin T_{\mathscr{U},\mathbb{L}} \\
(\Delta_0\text{-completeness of } T_{\mathscr{U},\mathbb{L}}) \quad &\Leftrightarrow \quad \neg\theta(\tau_1, \ldots, \tau_k) \in T_{\mathscr{U},\mathbb{L}}
\end{aligned}$$

Finally, assume that $\phi([\tau_1], \ldots, [\tau_k], [\sigma]) = \exists[\sigma]\theta([\tau_1], \ldots, [\tau_k], [\sigma])$ and that the equivalence of (a) and (b) is given for θ.

Assume that $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \exists[\sigma]\theta([\tau_1], \ldots, [\tau_k], [\sigma])$. We have that for some σ, $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta([\tau_1], \ldots, [\tau_k], [\sigma])$ and by the induction hypothesis it follows that for this σ, $\theta(\tau_1, \ldots, \tau_k, \sigma) \in T_{\mathscr{U},\mathbb{L}}$. This means that there exists a set $S \in \mathscr{U}$ such that $\mathscr{M}_{\mathscr{F}} \models \theta(a_1, \ldots, a_k, b)$ for all sequences $a_1 < \ldots < a_k$ with elements from S and some $b \in M$. Consequently, $\mathscr{M}_{\mathscr{F}} \models \exists y\theta(a_1, \ldots, a_k, y)$ for all sequences $a_1 < \ldots < a_k$ with elements from S and the proof (a) $\Rightarrow$ (b) is completed for the existential case.

The (b) $\Rightarrow$ (a) direction is more involved and makes use of a lemma concerning Δ_0-Skolem functions in $\mathscr{F}$:

Lemma 3.12. *If for some $\Delta_0(\mathscr{L}_{\mathscr{F}})$-formula $\psi(x_1, \ldots, x_n, y)$, we have that*

$$\mathscr{M}_{\mathscr{F}} \models \forall x_1 \ldots \forall x_n((x_1 < \ldots x_n < c) \rightarrow \exists y\ \psi(x_1, \ldots, x_n, y))$$

then there exists $g(x_1, \ldots, x_n) \in \mathscr{F}$ such that:

$$\mathscr{M}_{\mathscr{F}} \models \forall x_1 \ldots \forall x_n((x_1 < \ldots x_n < c) \rightarrow \psi(x_1, \ldots, x_n, g(x_1, \ldots, x_n)))$$

Proof. Given ψ for which the conditions of the lemma hold. First we define the following abbreviation for ease of notation:

$$\delta(x_1, \ldots, x_n, y) := (\psi(x_1, \ldots, x_n, y) \wedge \forall z < y \neg\psi(x_1, \ldots, x_n, z))$$

$\delta(x_1, \ldots, x_n, y)$ expresses that y is the smallest solution for $\psi(x_1, \ldots, x_n, y)$. Δ_0-MIN now yields that there is a unique least y such that:

$$\mathscr{M}_{\mathscr{F}} \models \forall x_1 \ldots \forall x_n((x_1 < \ldots < x_n < c) \rightarrow \delta(x_1, \ldots, x_n, y))$$

$\mathrm{B}\Sigma_1$ implies that there is some $b \in M$ such that:

$$\mathscr{M}_{\mathscr{F}} \models \forall x_1 \ldots \forall x_n((x_1 < \ldots < x_n < c) \rightarrow \exists! y < b\ \delta(x_1, \ldots, x_n, y))$$

Now, define a function g on M^n such that $g(a_1, \ldots, a_n) = a_{n+1}$ iff

$$\begin{aligned} \mathscr{M}_{\mathscr{F}} \models \quad & ((a_1 < \ldots < a_n < c) \wedge \delta(a_1, \ldots, a_n, a_{n+1})) \\ & \vee(\neg(a_1 < \ldots < a_n < c) \wedge (a_{n+1} = 0)) \end{aligned}$$

So for any sequence $a_1, \ldots, a_n$ we have that $g(a_1, \ldots, a_n)$ is equal to the least y such that $\psi(a_1, \ldots, a_n, y)$ if $a_1 < \ldots < a_n < c$ and $g(a_1, \ldots, a_n)$ is equal to 0 otherwise. Since δ is a $\Delta_0(\mathscr{L}_{\mathscr{F}})$-formula, the graph of g is certainly Σ_1. Because $g(a_1, \ldots, a_n)$ is bounded from above by the previously established b, we find that $g \in \mathscr{F}$. This shows that the function g we have constructed has the necessary properties. □

Having proven this lemma, we return to the (b) ⇒ (a) part of the existential case. Assume we have a formula $\exists y\ \theta(x_1, \ldots, x_k, y)$ for the equivalence of (a) and (b) holds for θ. Suppose (b) holds for $\exists y \theta$ for some selection $[\tau_1], \ldots, [\tau_k]$ of elements from $N_{\mathscr{U},\mathbb{L}}$. For each $\tau_i(l_1, \ldots, l_{n_i})$, add dummy-variables so that we have a sequence $(l_1, \ldots, l_n)$ from $[\mathbb{L}]^n$ and each τ_i can be written as $f_i(l_1, \ldots, l_n)$. Since (b) holds, the defintion of $T_{\mathscr{U},\mathbb{L}}$ yields that there exists an $S \in \mathscr{U}$ such that

$$\mathscr{M} \models \exists y\ \theta(f_1(a_1, \ldots, a_n), \ldots, f_k(a_1, \ldots, a_n), y)$$

for all sequences $(a_1, \ldots, a_n) \in [A]^n$. Let $d \in M$ be an element coding this set S. Define the formula $\alpha(x_1, \ldots, x_n)$:

$$\alpha(x_1, \ldots, x_n) := \bigwedge_{i=1}^{n}(x_i\ E\ d) \wedge \bigwedge_{i=1}^{n-1}(x_i < x_{i+1})$$

α states that $(x_1, \ldots, x_n)$ is an increasing sequence of elements from the set coded by d, which is S. Now, define the formula $\psi(x_1, \ldots, x_n, y)$:

$$\psi(\mathbf{x}, y) := [\alpha(\mathbf{x}) \rightarrow \theta(f_1(\mathbf{x}), \ldots, f_k(\mathbf{x}), y)] \wedge [\neg\alpha(\mathbf{x}) \rightarrow (y = 0)]$$

Since E has a Δ_0-definition, $\psi(x_1, \ldots, x_n, y)$ is a Δ_0-formula. We can therefore apply Lemma 2.9 to find a function $g(x_1, \ldots, x_n) \in \mathscr{F}$ such that

$$\mathscr{M}_{\mathscr{F}} \models \psi(a_1, \ldots, a_n, g(a_1, \ldots, a_n))$$

for all sequences $(a_1, \ldots, a_n) \in [A]^n$. Applying the induction hypothesis, we find:

$$\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \theta([\tau_1], \ldots, [\tau_k], [g(l_1, \ldots, l_n)])$$

And from this it follows that

$$\mathscr{N}_{\mathscr{U},\mathbb{L}} \models \exists y\ \theta([\tau_1], \ldots, [\tau_k], y)$$

which concludes the proof of (b) $\Rightarrow$ (a) of the existential case. □

The following lemmas will provide the pieces to complete the proof of Theorem 3.1.

Lemma 3.13. *$\mathscr{M}$ is cofinal in $\mathscr{N}_{\mathscr{U},\mathbb{L}}$.*

Proof. Given an element of $\mathscr{N}_{\mathscr{U},\mathbb{L}}$, an equivalence class of terms of the form $f(l)$ with $f \in \mathscr{F}$. This means that each such f has a Σ_1-graph. Denote this graph by $F(x, y) = \exists z\ G(x, y, z)$ with $G(x, y, z)$ a Δ_0-formula. Clearly we have that

$$\exists z\ G(x, y, z) \rightarrow \exists w \exists z < w\ G(x, y, z)$$

Because we're working with the graph of a function defined on all $x < c$, the following holds:

$$\mathscr{M} \models \forall x < c \exists y \exists z G(x, y, z)$$

And from this we get:

$$\mathscr{M} \models \forall x < c \exists w \exists y < w \exists z < w\ G(x, y, z)$$

Recall that $\mathscr{M}$ satisfied $B\Sigma_1$ and applying this, we find:

$$(\star)\ \mathscr{M} \models \exists m \forall x < c \exists w < m \exists y < w \exists z < w\ G(x, y, z)$$

Now, for $m \in M$ we have that c_m denotes the constant function with value m. This function is in $\mathscr{F}$. Consequently, the equivalence class $[c_m(l)]$ is an element of $N_{\mathscr{U},\mathbb{L}}$. From $(\star)$ we can conclude that the function is f is upwards bounded by m (Since all the function-values y are upwards bounded by w, which in turn is upwards bounded by m). We have that $f(l) < c_m(l)$ and consequently $[f] < [c_m]$. This shows that for every element $[f] \in N_{\mathscr{U},\mathbb{L}}$, there is an element from M that supercedes it. And therefore, $\mathscr{M} \subseteq_{cf} \mathscr{N}_{\mathscr{U},\mathbb{L}}$. □

Lemma 3.14. $\mathscr{N}_{\mathscr{U},\mathbb{L}} \models I\Delta_0$

Proof. Since $\mathscr{M}$ satisfies $I\Delta_0$, all axioms of $I\Delta_0$ are in $T_{\mathscr{U},\mathbb{L}}$ and by 3.11, this means that $\mathscr{N}_{\mathscr{U},\mathbb{L}}$ also satisfies $I\Delta_0$. □

Lemma 3.15. *$M \setminus I$ is downward cofinal in $N_{\mathscr{U},\mathbb{L}}$*

Proof. Take an arbitrary $[f(\mathbf{l})] \in N_{\mathscr{U},\mathbb{L}} \setminus I$. Since $\mathscr{U}$ is I-tight, there exists a set $H \in \mathscr{U}$ such that f is constant on H or f is bounded from below by some $m_0 \in M \setminus I$. In the first case, $f(\mathbf{x}) \notin I$ since we assumed that $[f(\mathbf{l})] \in N_{\mathscr{U},\mathbb{L}}$. And since f is M-valued, we have that $f(\mathbf{x}) = m_0$ for some $m_0 \in M \setminus I$. By Lemma 3.11, we see that there is an $m_0 \in M \setminus I$ such that $[c_{m_0}(\mathbf{l})] \trianglelefteq [f(\mathbf{l}]$.

In the second case, we have that there exists an $m_0 \in M \setminus I$ such that $m_0 < f(\mathbf{x})$ for all $\mathbf{x} \in [H]^n$. By Lemma 3.11, this yields that there exists an $m_0 \in M \setminus I$ such that $[c_{m_0}(\mathbf{l})] \trianglelefteq [f(\mathbf{l}]$. □

Lemma 3.16. *$\mathscr{N}_{\mathscr{U},\mathbb{L}}$ end extends I.*

Proof. Take $x \in I$ (identified with $[c_x(\mathbf{l})] \in N_{\mathscr{U},\mathbb{L}}$) and $[y(\mathbf{l})] \in N_{\mathscr{U},\mathbb{L}}$ such that $[c_x(\mathbf{l})] \triangleright [y(\mathbf{l})]$. Suppose $[y] \in N_{\mathscr{U},\mathbb{L}} \setminus I$, then by Lemma 2.13 there exists a $z \in M \setminus I$ such that $[c_z(\mathbf{l})] \trianglelefteq [y(\mathbf{l})]$. But since I is a cut of M, we must have that $[c_z(\mathbf{l})] \triangleright [c_x(\mathbf{l})]$, which is a contradiction. Therefore, $y \in I$. □

Next, we find that an automorphism of the linear order $\mathbb{L}$ induces an automorphism of the entire model $\mathscr{N}_{\mathscr{U},\mathbb{L}}$ with desirable properties.

Lemma 3.17. *Given an automorphism $j : \mathbb{L} \mapsto \mathbb{L}$, there exists an automorphism $\hat{j} : \mathscr{N}_{\mathscr{U},\mathbb{L}} \mapsto \mathscr{N}_{\mathscr{U},\mathbb{L}}$ such that $j \mapsto \hat{j}$ is a group-embedding of $Aut(\mathscr{L})$ into $Aut(\mathscr{N}_{\mathscr{U},\mathbb{L}})$. Additionally, for every nontrivial $j \in Aut(\mathbb{L})$, $I_{fix}(\hat{j}) = I$.*

Proof. Given an automorphism j of $\mathbb{L}$, define $\hat{j}$ as follows:

$$\hat{j}([f(l_1, \ldots, l_n)]) := [f(j(l_1), \ldots, j(l_n))]$$

It is easy to see that this map $j \mapsto \hat{j}$ conserves the group-operation, composition of functions. To verify the second part of the lemma, we need to show that for any nontrivial automorphism j, $\hat{j}$ fixes all elements of I, but that for every element x above I, there is a $y < x$ which is moved by $\hat{j}$. Since elements of M are identified with equivalence classes of constant functions $[c_m(\mathbf{l})]$, we have that:

$$\hat{j}([c_m(l_1, \ldots, l_n)]) = [c_m(j(l_1), \ldots, j(l_n))] = [c_m(l_1, \ldots, l_n)]$$

and therefore, each element of M is a fixed point of $\hat{j}$. Since I is a cut of M, the same holds for I.

Now, recall from Theorem 3.9 that there exists a sequence $\langle a_n : n \in \omega \rangle$ of elements of $M \setminus I$ that are downward cofinal in $M \setminus I$, and a sequence $\langle Z_n : n \in \omega \rangle$ of elements of $\mathscr{U}$ with $Card(Z_n) < a_n$. Using the Z_n, construct the following sequence of terms $\langle \tau_n : n \in \omega \rangle$ of $\mathscr{L}_{\mathscr{F}}$:

$$\tau_n(x) = y \Leftrightarrow x \text{ is the } y\text{-th element of } Z_n \text{ using the natural ordering.}$$

Clearly, $\tau_n(x) < a_n$ for all $n \in \omega$. Now consider the automorphism j of $\mathbb{L}$ and an element k that is not fixed by j. Say, $j(k) = l$ with $k \neq l$. We have that

$$\hat{j}([\tau_n(k)]) = [\tau_n(j(k))] = [\tau_n(l)]$$

Since τ_n is injective, these terms are clearly not equal. Since the sequence $\langle a_n : n \in \omega \rangle$ is downward cofinal in $M \setminus I$ and $M \setminus I$, $\langle a_n : n \in \omega \rangle$ is also downward cofinal in $N_{\mathscr{U},\mathbb{L}} \setminus I$. So we have now shown that $\hat{j}$ moves elements of $N_{\mathscr{U},\mathbb{L}} \setminus I$ that are arbitrarily close to I and therefore, $I_{fix}(\hat{j}) = I$. □

Now, we can combine the pieces of the puzzle and complete the proof of (b) ⇒ (a) of Theorem 3.1. Given a model $\mathscr{M}_0$ of $I\Delta_0 + B\Sigma_1 + Exp$, by Theorem 2.11, we can end extend this model to a model $\mathscr{M}$ of $I\Delta_0 + B\Sigma_1$. Using a cut I of $\mathscr{M}$ that satisfies Exp (we take the cut to be equal to our original model: $I = M_0$), we apply Theorem 3.9 to construct an ultrafilter $\mathscr{U}$. Using this ultrafilter, we construct a model $\mathscr{N}_{\mathscr{U},\mathbb{L}}$ for an arbitrary linear order $\mathbb{L}$ (3.11). This model satisfies $I\Delta_0$ (Lemma 3.14) and is an end extension of $\mathscr{M}$ (Lemma 3.16). Now, take $\mathbb{L} = \mathbb{Z}$ and consider the nontrivial automorphism $j(z) = z + 1$ of $\mathbb{Z}$. Lemma 3.17 now gives us an automorphism $\hat{j}$ of $\mathscr{N}_{\mathscr{U},\mathbb{Z}}$ with the property that $I_{fix}(\hat{j}) = I = M_0$. □

4 Similar results for other theories

Theorem 3.1 is an interesting result. Starting with a model of a weak theory ($I\Delta_0$), we can immediately obtain a model of a much stronger theory, $I\Delta_0 + B\Sigma_1 + Exp$. And conversely, every model of the stronger theory comes from a model of the weaker theory. In other words, $I\Delta_0 + B\Sigma_1 + Exp$ is completely characterized by models of $I\Delta_0$ and their automorphisms.

$I\Delta_0 + B\Sigma_1 + Exp$ is not the only theory that is characterized by a weaker theory in this way. Results found by Enayat show that a similar construction is also possible for second-order arithmetic [2] and set-theory [3], both of which will be discussed in this section.

4.1 Second-order arithmetic and automorphisms

Up until now, we have only used first-order arithmetic, in which reasoning is limited to individual elements, excluding things like quantifying over sets or functions. In second-order arithmetic, however, this restriction is lifted and formulas of the form

$$\forall n(n \in X \rightarrow (n+1) \in X)$$

or

$$\exists X(0 \notin X)$$

become valid formulas of the language. The language of second-order arithmetic is two-sorted, the first sort of terms and variables corresponding with individuals and the second with set-variables. A second-order formula is called *arithmetical* if it has no bounded set-variables. From the two examples given above, the first is arithmetical, the second is not.

The theory of second-order arithmetic, Z_2, is made up of all the axioms of PA, together with the second-order induction axiom:

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

and the axiom-scheme of *comprehension*, with for every formula $\phi(x)$:

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

The comprehension scheme basically allows us to define sets of the form $\{n|\phi(n)\}$. The comprehension-scheme restricted to this formulas that contain no bounded set-variables (i.e. the arithmetical formulas) is called *arithmetical comprehension*. The theory ACA_0 is a fragment of Z_2 where the comprehension-scheme is restricted to arithmetical comprehension.

Just like the language, models of second-order arithmetic are two-sorted: $(\mathscr{M}, \mathscr{A})$. Here $\mathscr{M}$ is a structure in the language of $\mathscr{L}_{PA}$ and $\mathscr{A}$ is a collection of subsets of M.

If $(\mathscr{M}, \mathscr{A}) \models ACA_0$ and $X \in \mathscr{A}$, then $(\mathscr{M}, X) \models PA(X)$, where $PA(X)$ is PA augmented with the induction scheme for the language consisting of $\mathscr{L}_{PA}$ together with a unary predicate X.

Definition 4.1. *Given a cut I of a model $\mathscr{M}$ of a strong enough fragment of arithmetic to allow for basic coding ($I\Delta_0$ already qualifies), we define the standard system of $\mathscr{M}$ with respect to I as the collection of sets coded by elements of $\mathscr{M}$, restricted to I:*

$$SSy_I(\mathscr{M}) := \{c_E \cap I : c \in M\}$$

where c_E is the set coded by c using the Ackermann coding described in section 2.5.

Theorem 4.2. *For any two-sorted structure $(\mathscr{M}, \mathscr{A})$, the following are equivalent:*
(a) M is a proper initial segment equal to the fixed-point set of some automorphism j of a model $\mathscr{N}$ of $I\Delta_0$ and $\mathscr{A} = SSy_M(\mathscr{N})$.
(b) $(\mathscr{M}, \mathscr{A}) \models ACA_0$

This theorem is in essence very similar to Theorem 3.1, with the exception that Theorem 3.1 considers a model formed by the largest initial segment that is fixed by the automorphism, where Theorem 4.2 requires the initial segment to be identical to the fixed-point set. Note that in the original theorem in [2], the (a) $\Rightarrow$ (b) part has the stronger conclusion that $\mathscr{N}$ is an elementary end extension of $\mathscr{M}$ and therefore a model of ACA_0.

The proof of Theorem 4.2 follows the same general idea as the proof of Theorem 3.1, one way is proven by using the properties of $\mathscr{N}$ and the automorphism to verify that $\mathscr{M}$ satisfies the required properties. The other way again uses ultrafilters to contruct a model with desirable properties.

Proof.]Proof of Theorem 3.2, (a) $\Rightarrow$ (b)] Theorem 3.1 immediately gives us that $\mathscr{M} \models I\Delta_0$ and $\mathscr{M} \models Exp$. We will need some set-theoretic reasoning power. Because of this, our next goal is to replace the end extension $\mathscr{N}$ by a more suitable model $\mathscr{N}^*$ which contains $\mathscr{M}$ and satisfies $I\Delta_0 + Exp$. For this we will need super-exponentiation.

Definition 4.3. *The predicate $SuperExp(x, y)$ expresses that*

$$y = Superexp(x, x)$$

Since $SuperExp(x, y)$ is Δ_0 and $Superexp(x, x)$ can be defined in $\mathscr{N}$ from x, we can apply the same reasoning as was used in stages 2 and 3 of the proof of Lemma 2.3C to find that $\mathscr{M} \models \forall x \exists y\ SuperExp(x, y)$.

Lemma 4.4. *There exists an initial segment $\mathscr{N}^*$ of $\mathscr{N}$ which contains $\mathscr{M}$ and is a model of $I\Delta_0 + Exp$. Furthermore, $j \restriction \mathscr{N}^*$ is an automorphism.*

Proof. Let $b \in N \setminus M$. By Lemma 4.4 and Δ_0-elementary equivalence of end extensions, we have that for every $m \in M$:

$$\mathscr{N} \models \exists y < b\ (Superexp(m, m) = y)$$

By Δ_0-OVERSPILL, there now is a $a \in N \setminus M$ such that $Superexp(a, a)$ is defined in $\mathscr{N}$. This means that elements $Superexp(n, a)$ with $n \in \omega$ are also defined. Assume that $j(a) > a$ (if it isn't, replace j by j^{-1}. Define N^* as follows:

$$N^* = \bigcup_{k\in\omega} \bigcup_{n\in\omega} [0, Superexp(n, j^k(a))]$$

where j^k denotes the k-times application of j. It's clear that $\mathscr{N}^*$ is an initial segment of $\mathscr{N}$ and that it contains $\mathscr{M}$. By Lemma 2.10, we find that $\mathscr{N}^* \models I\Delta_0$. For any $x \in N^*$, there are n and k such that $x < Superexp(n, j^k(a))$ and therefore $2^x < Superexp(n+1, j^k(a))$. So if 2^x is defined in $\mathscr{N}$, then it is in $\mathscr{N}*$. The proof that 2^x is defined mimics steps 2 and 3 of the proof of Lemma 3.5. So we also have that $\mathscr{N}^* \models Exp$. Since $\mathscr{N}^*$ is closed under j, the restriction $j \restriction \mathscr{N}^*$ is an automorphism. □

Definition 4.5. *Suppose $\mathscr{N} \models I\Delta_0$ and M is a cut of $\mathscr{N}$. M is a* strong cut *of $\mathscr{N}$ if for every function $f : X \to N$ (with $M \subseteq X$) for which the graph of f is coded in $\mathscr{N}$, there is an $s \in N$ such that for all $m \in M$:*

$$f(m) \notin M \Leftrightarrow s < f(m)$$

Lemma 4.6. *M is a strong cut of $\mathscr{N}$.*

Proof. Since $\mathscr{N}^* \subseteq_e \mathscr{N}$, it suffices to show that M is a strong cut of $\mathscr{N}^*$. Because $\mathscr{N}^* \models I\Delta_0 + Exp$, we can use some set-theory within $\mathscr{N}^*$. Take any function f satisfying the conditions of the lemma and let $\overline{f}$ denote the code of the graph of f in $\mathscr{N}^*$. Clearly $\overline{f} \notin M$. Take $\overline{g} = j(\overline{f})$, we have that $\overline{g} \notin M$ and $\overline{f} \neq \overline{g}$ since M is the fixed-point set of j. If g is the function coded by $\overline{g}$, then for all $m \in M$, if $f(m) = g(m)$, then $f(m) \in M$.

Assume that for some $m_0 \in M$, $f(m_0) \notin M$ (For if such an m_0 doesn't exist, then the proof is complete). Fix a set c_E containing $\overline{f}$, $\overline{g}$ and all $m \in M$, this set is coded by some $c \in \mathscr{N}^*$ with c_E being $\{x \in N^* : xEc\}$. Define the function $h(x)$ defined on the interval $[m_0, c]$ of $\mathscr{M}$:

$$h(x) = \mu y \leq c \, [\exists z \leq x \; (y = f(z) \neq g(z)]$$

Here $\mu y \leq c$ means "the least $y \leq c$ such that ...". If $m \in [m_0, c] \cap M$ then $h(m) \notin M$ because any y found by the least-search operator will not be in M and $f(m_0)$ (which is not in M) satisfies the requirements of this operator (though it may not be the least solution). Also, for $m, m' \in [m_0, c] \cap M$, if $m \leq m'$ then the set of solutions for m will be contained in the one for m', which means that $h(m') \leq h(m)$.

Since the Ackermann-coding is Δ_0-definable, the graph of $h(x)$ can be defined by a Δ_0-formula. Also, for all $m \in M$ with $m \geq m_0$, we have that $m < h(m)$. By Δ_0-OVERSPILL we find that there is a $s \in N^* \setminus M$ for which $s < h(s)$. Given any $m \in M$, suppose that $f(m) \notin M$. If $m < m_0$, replace m_0 by $m_0' = m$ and reapply the above reasoning. So without loss of generality, we can assume that $m_0 \leq m$. By definition of h, $h(m) \leq f(m)$.

Since $s \notin M$, $m < s$ and therefore $h(m) \geq h(s)$. So we have the following chain of inequalities:

$$s < h(s) \leq h(m) \leq f(m)$$

or $s < f(m)$, as desired. Now, suppose that for some $m \in M$, $s < f(m)$. If $f(m) \in M$, then $s \in M$, contradicton. This completes the proof that M is a strong cut of $\mathscr{N}^*$ and consequently of $\mathscr{N}$. $\square$

Lemma 4.7. *Let $\mathscr{A} := SSy_M(\mathscr{N})$. Define the language $\mathscr{L}$ by adding a unary relation symbol $\overline{S}$ for each set $S \in \mathscr{A}$ to $\mathscr{L}_{PA}$. For every $\mathscr{L}$-formula $\phi(x_1, \ldots, x_m)$ (where x_i are free variables) there is some Δ_0-formula $\theta_\phi(x_1, \ldots, x_m, b_1, \ldots, b_n)$ where $b_1, \ldots, b_n$ is a sequence of parameters from N, such that the following holds for all sequences $a_1, \ldots, a_m$ of elements from M:*

$$(\mathscr{M}, S)_{S \in \mathscr{A}} \models \phi(a_1, \ldots, a_m) \Leftrightarrow \mathscr{N} \models \theta_\phi(a_1, \ldots, a_m, b_1, \ldots, b_n)$$

Proof. The proof is done by constructing the desired formula θ_ϕ by recursion on the structure of ϕ. Two special cases merit our attention.

- ϕ is of the from $\overline{S_i}(t)$ with $\overline{S_i}$ a predicate generated by the set S_i in $\mathscr{A}$ and t a term. Choose the parameter $b \in N$ in such a way that the set coded by b, restricted to M, is S_i, so $b_E \cap M = S_i$. Now define $\theta_\phi = (vEb)$ (or $v \in b_E$).

- ϕ is of the form $\exists v \psi(v, x_1, \ldots, x_k)$. Fix some $c \in N \setminus M$ and define the following function on $[0, c]$:

  $$f(\langle x_1, \ldots, x_t \rangle) := \mu v \leq c(\theta_\psi(v, x_1, \ldots, x_k)$$

  Where $\mu v \leq c$ evaluates to 0 if no $v \leq c$ is found with the required property. f is coded in $\mathscr{N}$ and we can use the fact that M is a strong cut of $\mathscr{N}$ to find an $s \in \mathscr{N}$ such that for all $m \in M$, $f(m) \in M \Leftrightarrow f(m) \leq s$. Now define: $\theta_\phi := \exists v \leq s \theta_\psi(v, x_1, \ldots, x_n)$.

$\square$

Now we conclude the proof of (a) $\Rightarrow$ (b) of Theorem 4.2. Let $\mathscr{A}$ and $\mathscr{L}$ be as in Lemma 4.7. Because $\mathscr{M} \models I\Delta_0$, every non-empty element of $\mathscr{A}$ has a first element in $\mathscr{M}$. We need to show that $(\mathscr{M}, \mathscr{A})$ satisfies the arithmetical comprehension scheme. To do this, consider an arbitrary $\mathscr{L}$-formula $\phi(x)$ with one free variable, x. We need to show that $\{m \in M : (\mathscr{M}, \mathscr{A}) \models \phi(m)\} \in \mathscr{A}$.

Fix some $c \in N \setminus M$, we have that there is a $d \in N$ that codes $\{x < c : \mathscr{N} \models \theta_\phi(x)\}$ with θ_ϕ as in Lemma 4.7. Therefore:

$$\{m \in M : (\mathscr{M}, \mathscr{A}) \models \phi(m)\} = \{x < c : \mathscr{N} \models \theta_\phi(x)\} \cap M = d_E \cap M \in \mathscr{A}$$

$\square$

Proof of (b) ⇒ (a) of Theorem 4.2. The proof of the (b) ⇒ (a) part of Theorem 4.2 makes use of an ultrafilter-construction along a linear order, $\mathbb{Z}$, to create an end extension of $(\mathscr{M}, \mathscr{A})$. In a similar way as in Theorem 3.1, the automorphism $z \mapsto z+1$ of $\mathscr{Z}$ induces an automorphism of the entire model with the desired properties.

To start, we define a partially ordered set $\mathbb{P}$ as the set of all sets in $\mathscr{A}$ that are unbounded in $\mathscr{M}$ ordered by inclusion:

$$\mathbb{P} := \{S \in \mathscr{A} : \forall m \in M \exists s \in S \; s > m\}$$

We will be studying ultrafilters on this poset $\mathbb{P}$. In section 2, ultrafilters were defined in terms of I-completeness, here we adopt a similar property: We say that a filter is $(\mathscr{M}, \mathscr{A})$-*complete* if for every function f on M that is coded in $\mathscr{A}$ and that has a range bounded in $\mathscr{M}$, there is some $X \in \mathscr{U}$ such that f is constant on X. A similar line of reasoning as was used in section 2 yields that if a filter is $(\mathscr{M}, \mathscr{A})$-complete, then it is an ultrafilter.

We say that a subset $\mathscr{D}$ of $\mathbb{P}$ is *dense* if for every $X \in \mathbb{P}$, there is a $Y \in \mathscr{D}$ with $Y \subseteq X$. A subset $\mathscr{D}$ of $\mathbb{P}$ is *parametrically definable* in $(\mathscr{M}, \mathscr{A})$ if there is a formula $\psi(X, \mathbf{p})$ with $\mathbf{p}$ a set of parameters such that $S \in \mathscr{D} \Leftrightarrow (\mathscr{M}, \mathscr{A}) \models \psi(X,)$.

A filter $\mathscr{U}$ is called $\mathscr{A}$-*generic* if for every parametrically definabl dense subset $\mathscr{D} \subseteq \mathbb{P}$, we have that $\mathscr{U} \cap \mathscr{D} \neq \emptyset$. $\mathscr{U}$ is $(\mathscr{M}, \mathscr{A})$-*canonically Ramsey* if for every function $f : [M]^n \to M$ with $n \in \mathbb{N}$ and f coded in $\mathscr{A}$, there is an $X \in \mathscr{U}$ such that X is f-canonical.

Let Γ be a pairing function, a bijection from $M \times M$ to M. Every 2-valued function $g : M \to \{0, 1\}$ gives rise to a sequence $\langle S_a^g : a \in M \rangle$ of subsets of M, defined as follows:

$$S_a^g := \{b \in M : g(\Gamma(a, b)) = 1\}$$

We say that an ultrafilter $\mathscr{U} \subseteq \mathbb{P}$ is $(\mathscr{M}, \mathscr{A})$-*iterable* if for every $g \in \mathscr{A}$ such that $g : M \to \{0, 1\}$:

$$\{a \in M : S_a^g \in \mathscr{U}\} \in \mathscr{A}$$

The following theorem formalizes combinatorial results similar to Theorem 2.15 in ACA_0. The proof is beyond the scope of this text and therefore omitted.

Theorem 4.8. *For all $n \in \omega$, $ACA_0 \vdash$ "for every function $f : [\omega]^n \to \omega$ there is an unbounded $X \subseteq \omega$ such that X is f-canonical."*

The next lemma, based on the Rasiowa-Sirkorski Lemma, proves the existence of a generic filter on a countable model $(\mathscr{M}, \mathscr{A})$.

Lemma 4.9. *Given a countable model $(\mathscr{M}, \mathscr{A})$, there exists a $\mathscr{A}$-generic filter over $(\mathscr{M}, \mathscr{A})$.*

Proof. Let $\mathbb{P}$ be the poset of unbounded sets as defined before. Let $\mathscr{D}_{\mathbb{P}}$ denote the collection of parametrically definable dense subsets of $\mathbb{P}$. Since $(\mathscr{M}, \mathscr{A})$ is countable, so is $\mathscr{D}_{\mathbb{P}}$. Enumerate the elements of $\mathscr{D}_{\mathbb{P}}$ by $D_1, D_2, \ldots$. Fix a set $S_1 \in D_1$. Since D_2 is dense, there is some $S_2 \in D_2$ such that $S_2 \subseteq S_1$. Repeat this to obtain a sequence $\langle S_1 \supseteq S_2 \supseteq \ldots \rangle$.

Now define:

$$\mathscr{U} = \{Q \in \mathbb{P} : \exists i \in \omega \; S_i \subseteq Q\}$$

and we claim that $\mathscr{U}$ is a $\mathscr{A}$-generic filter. Closure under supersets is trivial. To verify closure under intersections, assume $X, Y \in \mathscr{U}$ and let S_X and S_Y be the associated sets contained in X and Y respectively, according to the definition of $\mathscr{U}$. Since $S_i \subseteq S_j$ if $i > j$, assume, without loss of generality that $S_X \subseteq S_Y$. Then $S_X \subseteq X \cap Y$ and we find that $X \cap Y \in \mathscr{U}$.

To verify $\mathscr{A}$-genericity, take any dense subset D_i of $\mathbb{P}$. We have that $S_i \in \mathscr{U}$ and therefore, $\mathscr{U} \cap D_i \supseteq S_i \neq \emptyset$, which is what we needed to show. □

Now that we have a generic filter, we'll need to show that it has certain desirable properties.

Lemma 4.10. *Let $(\mathscr{M}, \mathscr{A})$ be a model of ACA_0 and $\mathscr{U}$ a $\mathscr{A}$-generic filter on $(\mathscr{M}, \mathscr{A})$. The following are true:*
(a) $\mathscr{U}$ is $(\mathscr{M}, \mathscr{A})$-complete.
(b) $\mathscr{U}$ is $(\mathscr{M}, \mathscr{A})$-iterable.
(c) $\mathscr{U}$ is $(\mathscr{M}, \mathscr{A})$-canonically Ramsey.

Proof. (a): Take any $f \in \mathscr{A}$ with domain M and range bounded in $\mathscr{M}$. We need to show that there is a set in $\mathscr{U}$ on which f is constant. Define the set:

$$D_f := \{Y \in \mathbb{P} : f \restriction Y \text{ is constant}\}$$

Note that if D_f is dense, then by $\mathscr{A}$-genericity, it intersects with $\mathscr{U}$ and any set in this intersection can be used as the set we seek. Take any function f satisfying the conditions and set X in $\mathbb{P}$. Consider the set of level-sets of f, L_f. A level-set is either bounded or unbounded in $\mathscr{M}$. This gives rise to the set of unbounded level-sets of f, UL_f. The following is true:

$$D_f = \{Y \in \mathbb{P} : \exists Q \in UL_f \; Y \subseteq Q\}$$

Since the range of f is bounded, so is $M \setminus UL_f$, the union of bounded level-sets of f. Since $X \in \mathbb{P}$, we have that X is unbounded and that $X \cap UL_f$

is unbounded. Since there are boundedly many level-sets, by the pigeonhole principle, there is a level-set for which the intersection with X is unbounded. But this intersection is precisely an element of D_f.

(b): For sets X and Y in $\mathbb{P}$, write $X \subseteq_* Y$ ("X is almost contained in Y") if $X \setminus Y$ is bounded in $(M, <)$. Define the statement "X *decides* Y" as:

$$X \subseteq_* Y \text{ or } X \subseteq_* M \setminus Y$$

For a function $g : M \to \{0, 1\}$ with $g \in \mathscr{A}$, define:

$$D_g := \{Y \in \mathbb{P} : \forall a \in M\ Y \text{ decides } S^g_a$$

We claim that this set is dense. For this, take any $X \in \mathbb{P}$. Now we claim that there is a sequence $F = \langle F_a : a \in M\rangle$ coded in $\mathscr{A}$ with the following properties:

(I) $\forall a \in M\ [F_a = S^g_a \cap X \text{ or } F_a = X \setminus S^g_a]$

(II) $\forall a \in M \bigcap\limits_{b\leq a} F_b$ is unbounded in X.

To prove this claim, define for each function $s : [0, a] \to \{0, 1\}$, the sequence $\langle F^s_b : b \leq a\rangle$:

- $F^s_b = S^g_b \cap X$ if $s(b) = 1$
- $F^s_b = X\ S^g_b$ if $s(b) = 0$

Now let τ be the binary tree consisting of functions $s : [0, a] \to \{0, 1\}$. At each level b of the tree, at least one such s gives rise to an unbounded $\bigcap\limits_{b\leq a} F^s_b$, because X itself is unbounded. Now, delete all nodes (and branches that originate from them) for which $\bigcap\limits_{b\leq a} F^s_b$ is bounded. We are left with a tree $\tau' \subseteq \tau$ consisting of all functions s such that $\bigcap\limits_{b\leq a} F^s_b$ is unbounded. By Königs Lemma, this tree has a path and this path is the desired sequence $\langle F_a : a \in M\rangle$.

Define the set $Y = \{y_a : a \in M\} \in \mathbb{P}$ by induction in $(\mathscr{M}, \mathscr{A})$:

- y_0 is the least element of F_0.
- y_{a+1} is the least element of $\bigcap\limits_{b\leq a} F_b$ that is bigger than all y_b with $b \leq a$.

Given some $a \in M$, for every $c > a$, we have that $y_c \in \bigcap\limits_{b\leq a} F_b$ and therefore $y_c \in F_a$. This means that $Y \setminus F_a \subseteq \{y_0, \ldots, y_{a-1}\}$ and therefore that $Y \setminus F_a$ is bounded in M. So for all $a \in M$, $Y \subseteq_* F_a$ and by defintion of F_a, Y decides S_a^g. Note tht $Y \subseteq X$ and it follows that D_g is dense. Genericity of $\mathscr{U}$ then gives us that $\mathscr{U}$ is $(\mathscr{M}, \mathscr{A})$-iterable.

(c): Given $f : [M]^n \to M$ for a natural number n and $f \in \mathscr{A}$. Define:

$$D_f := \{Y \in \mathbb{P} : Y \text{ is } f\text{-canonical}\}$$

By Theorem 4.8, D_f is dense and by genericity of $\mathscr{U}$ this shows that every $f \in \mathscr{A}$ has a $X \in \mathscr{U}$ which is f-canonical. □

Lemma 4.11. *Suppose $(\mathscr{M}, \mathscr{A})$ is a model of ACA_0, then $(\mathscr{M}, S)_{S \in \mathscr{A}}$ has a proper elementary end extension $(\mathscr{N}, S^*)_{S \in \mathscr{A}}$ such that $\mathscr{A} = SSy_M(\mathscr{N})$.*

Proof. Note that Lemma 4.9 and 4.10 garantuee the existence of an iterable ultrafilter $\mathscr{U}$. Construct $(\mathscr{N}, S^*)_{S \in \mathscr{A}}$ by means of an ultrapower construction using the ultrafilter $\mathscr{U}$. Let the universe N be the set equivalence classes $[f]$ of functions $f : M \to M$ that are coded in $\mathscr{A}$. The equivalence relation is defined in the natural way:

$$f \;\; g \Leftrightarrow \{m \in M : f(m) = g(m)\} \in \mathscr{U}$$

Operations and the order relation are defined similarly, for example:

$$[f] <^{\mathscr{N}} [g] \Leftrightarrow \{m \in M : f(m) <^{\mathscr{M}} g(m)\} \in \mathscr{U}$$

For each $S \in \mathscr{A}$, the set S^* is defined as follows:

$$f] \in S^* \Leftrightarrow \{m \in M : f(m) \in S\} \in \mathscr{U}$$

A modified version of Theorem 2.14 implies that $\mathscr{N}$ as defined here is a proper elementary extension of $\mathscr{M}$. As in section 3, elements of $\mathscr{M}$ are identified with equivalence classes of constant functions c_m in $\mathscr{N}$. To verify that $\mathscr{N}$ is an end extension, suppose $\mathscr{N} \models [f] < [c_m]$ for some $m \in M$. We need to show that $[f] = [c_{m'}]$ for some $m' \in M$. Since $\mathscr{N} \models [f] < m$, we have some $X \in \mathscr{U}$ such that for all $x \in X$, $f(x) < m$. Define the function $f^* \in \mathscr{A}$ as follows: $f * (x) = f(x)$ if $x \in X$ and $f^*(x) = 0$ otherwise. Since $\mathscr{U}$ is $(\mathscr{M}, \mathscr{A})$-complete, there is some $Y \in \mathscr{U}$ on which f^* is constant, say with value m_0. Note that $m_0 \leq m$. The following are true:

$$\begin{aligned} \{m \in M : f^*(m) = m_0\} &= Y \in \mathscr{U} \\ \{m \in M : f^*(m) = f(m)\} &\supseteq X \in \mathscr{U} \end{aligned}$$

Which means that $[f] = [f^*] = [c_{m_0}]$ and we find that $\mathscr{N}$ is a proper elementary end extension of $\mathscr{M}$. Now take any $X \in \mathscr{A}$. We have that

$(\mathscr{N}, X^*)$ is an elementary end extension of $(\mathscr{M}, X)$ which satisfies $PA(X)$, so $(\mathscr{N}, X^*) \models PA(X^*)$. Because of this, for an arbitrary $d \in N \setminus M$, there is a $c \in N$ which codes precisely the elements of X^* which are less than d. Since $X = X^* \cap M$, we find that $X = c_E \cap M$, where c_E is the set coded by c. This shows that $X \in SSy_M(\mathscr{N})$.

Given an element $[f] \in N$, we want to show that the $[f]_E \cap M \in \mathscr{A}$. This means:

$$\{m \in M : \mathscr{N} \models mE[f]\} \in \mathscr{A}$$

By definition of $\mathscr{N}$, this is equivalent to:

$$\{m \in M : \{n \in M : \mathscr{M} \models mEf(n)\} \in \mathscr{U}\} \in \mathscr{A}$$

Note that there exists a function $g : M \to \{0, 1\}$ which is coded in $\mathscr{A}$ for which $g(x) = 1$ iff $\mathscr{M} \models (x)_0 E f((x)_1)$. The iterability of $\mathscr{U}$ means that with this g, the above condition is satisfied and we find that if $X \in SSy_M(\mathscr{N})$, then $X \in \mathscr{A}$. And we can conclude that $\mathscr{A} = SSy_M(\mathscr{N})$. $\square$

The ultrapower construction described above doesn't introduce any new subsets of $\mathscr{M}$, since $\mathscr{A} = SSy_M(\mathscr{N})$ and this allows us to repeat this construction finitely many times. Denote the n-fold iterated ultrapower by $Ult_{\mathscr{U},n}(\mathscr{M}, S)_{S \in \mathscr{A}}$. For any finite n, $\mathscr{U}^n$ is an ultrafilter on M^n defined as:

$$X \in \mathscr{U}^n \Leftrightarrow \{a_1 : \{\langle a_2, \ldots, a_n\rangle : \langle a_1, \ldots, a_n\rangle \in X\} \in \mathscr{U}^{n-1}\} \in \mathscr{U}$$

This process can be extended to an ultrapower construction along any linear order. The construction of such a model follows the same recipe as used in section 2; We begin with a set of n-types with certain properties relating to the ultrafilter. Then we augment the language with a symbol for each $l \in \mathbb{L}$. From this we construct the theory $T_{\mathscr{U},\mathbb{L}}$ and the model $Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S \in \mathscr{A}}$. Each $l \in \mathbb{L}$ is represented in $Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S \in \mathscr{A}}$ by c_l. Elements of $Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S \in \mathscr{A}}$ are of the form $f^*(c_{l_1}, \ldots, c_{l_n})$ with $f \in \mathscr{A}$ and $l_1 <_{\mathbb{L}} \ldots <_{\mathbb{L}} l_n$.

We have that for every formula $\phi(x_1, \ldots, x_n)$ and every $\mathbb{L}$-increasing sequence $(l_i)_{1 \leq i \leq n}$:

$$\begin{gathered} Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S \in \mathscr{A}} \models \phi(c_{l_1}, \ldots, c_{l_n}) \\ \Leftrightarrow \{\langle a_1, \ldots, a_n\rangle \in M^n : \mathscr{M} \models \phi(a_1, \ldots, a_n)\} \in \mathscr{U}^n \end{gathered}$$

Given any automorphism $j : \mathbb{L} \to \mathbb{L}$, we have an induced automorphism $\hat{j} : Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S \in \mathscr{A}} \to Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S \in \mathscr{A}}$ (let N denote the universe of this model), defined as follows:

$$\hat{j}(f^*(c_{l_1}, \ldots, c_{l_n})) = f^*(c_{j(l_1)}, \ldots, c_{j(l_n)})$$

Lemma 4.12. *Suppose $(\mathscr{M}, \mathscr{A}) \models ACA_0$ and j is a fixed-point free automorphism of a linear order $\mathbb{L}$. The fixed-point set of the induced automorphism $\hat{j}$ of $Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S\in\mathscr{A}}$ is precisely M.*

Proof. For any $m \in M$, the constant map $c_m(\mathbf{l}) = m$ is in $\mathscr{A}$. Therefore:

$$\hat{j}(c_m^*(\mathbf{l})) = c_m^*(j(\mathbf{l})) = m$$

So $\hat{j}$ fixes all elements of M. Take any element $f^*(c_{l_1}, \ldots, c_{l_n}) \in N$ fixed by $\hat{j}$. Since $f \in \mathscr{A}$ and $\mathscr{U}$ is canonically Ramsey, there is some $X \in \mathscr{U}$ and $S \subseteq \{1, \ldots, n\}$ such that for all increasing sequences $(a_i)_{1\leq i\leq n}$ and $(b_i)_{1\leq i\leq n}$ with elements of X:

$$f(a_1, \ldots, z_n) = f(b_1, \ldots, b_n) \Leftrightarrow \forall i \in S\ (a_i = b_i)$$

Consider the formula $\phi(x_1, \ldots, x_n) := \langle x_1, \ldots, x_n\rangle \in X^n$. We have that:

$$\{\langle a_1, \ldots, a_n\rangle \in M^n : \mathscr{M} \models \phi(a_1, \ldots, a_n)\} = X^n$$

and since $X^n \in \mathscr{U}^n$, it follows that:

$$Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S\in\mathscr{A}} \models \phi(c_{l_1}, \ldots, c_{l_n})$$

Since $\langle c_{l_1}, \ldots, c_{l_n}\rangle \in X^n$ and since j is fixed-point free while $f^*(c_{l_1}, \ldots, c_{l_n})$ is fixed by $\hat{j}$, we have that the set S must be empty and therefore that f is constant on X. Since $X \in \mathscr{U}$, this implies that $f^*(c_{l_1}, \ldots, c_{l_n})$ is equivalent to a constant function c_m and therefore $f^*(c_{l_1}, \ldots, c_{l_n}) \in M$. □

Let $\mathbb{L}$ be $\mathbb{Z}$ and take the automorphism $j : n \mapsto n + 1$. For any model $(\mathscr{M}, \mathscr{A})$ of ACA_0, we can construct the model $(\mathscr{N}, S^*)_{S\in\mathscr{A}} := Ult_{\mathscr{U},\mathbb{L}}(\mathscr{M}, S)_{S\in\mathscr{A}}$ of ACA_0 such that M is precisely the fixed-point set of the induced automorphism $\hat{j}$ of $(\mathscr{N}, S^*)_{S\in\mathscr{A}}$. Moreover, $SSy_M(\mathscr{N}) = \mathscr{A}$ and since $ACA_0 \vdash I\Delta_0$, the proof of (b) ⇒ (a) of Theorem 4.2 is completed. □

4.2 Set theory and automorphisms

We've already seen that set theory and arithmetic are closely related. Within a sufficiently strong arithmetical theory, it is possible to simulate fragments of set theory and vice versa. Just like in the arithmetical case, there is a connection between weaker and stronger theories of set theory through the means of automorphisms and their fixed-point sets. The paper [3] demonstrates such a connection and will be discussed here. Note that the details of set theory are beyond the scope of this text, which means that we will mainly focus on the results rather than the technical proofs and definitions. For more details, see the original paper by Enayat.

The language of set theory has one relation-symbol, the element-relation. Consequently, models of set theory consist of a universe and an interpretation of the element-relation. The main theory under investigation is the Zermelo-Fraenkel (ZF) set theory. This theory consists of 7 main axioms or axiom-schemes (although equivalent formulations or conservative extensions are possible).

- **Extensionality** - Two sets are equal if they have the same elements.
- **Foundation** - Any non-empty set A has an element B such that A and B are disjoint.
- **Pairing** - If A and B are sets, then there exists a set with A and B as elements.
- **Union** - For any set A, there is a set B whose elements are precisely the elements of the elements of A (Or in everyday terminology: for any set A, there is a set B which is the union of the elements of A).
- **Infinity** - There exists an infinite set.
- **Powerset** - For any set A, there exists a set B such that for any subset $C \subseteq A$, $C \in B$ (or: B is a superset of the powerset of A).
- **Replacement** - For any formula $\phi(x, y)$:

$$[\forall x \in a \exists! y\ \phi(x, y)] \rightarrow [\exists b \forall y\ (y \in b \leftrightarrow \exists x \in a\ \phi(x, y))]$$

The theory ZFC consists of ZF plus the Axiom of Choice. For any language $\mathscr{L} \supseteq \{\in\}$, the theories $ZF(\mathscr{L})$ and $ZFC(\mathscr{L})$ are ZF and ZFC respectively, augmented with the axiom-scheme of Replacement for every $\mathscr{L}$-formula.

Elementary Set Theory ($EST(\mathscr{L})$) is obtained from $ZFC(\mathscr{L})$ by deleting the Powerset and Replacement axioms and adding the following axiom-scheme of $\Delta_0(\mathscr{L})$-Separation, for any $\Delta_0(\mathscr{L})$-formula ϕ:

$$\forall a \exists b \forall x (x \in b \leftrightarrow x \in a \wedge \phi(x))$$

This scheme expresses that for any set a there is a subset b containing those $x \in a$ on which $\phi(x)$ holds.

Note that Separation is a direct consequence of the Replacement axiom-scheme used here. As a consequence, ZFC satisfies Separation for any formula $\phi(x)$.

Given a language with an additional binary relation symbol $\lhd$, the axiom GW (Global Well-ordering) expresses that $\lhd$ well-orders the universe. So $\lhd$ is a total order on the universe and every non-empty set has a $\lhd$-minimal element. GW^* is a strengthening of GW obtained by adding the following two axioms:
(1) $\forall x \forall y\ (x \in y \to x \lhd y)$
(2) $\forall x \exists y \forall z\ (z \in y \leftrightarrow z \lhd x)$

A common way to construct models of (fragments of) ZF is the construction of the so-called Von Neumann hierarchy of sets, often denoted by $\mathbf{V}$. The construction goes as follows:

- $V_0 := \emptyset$.
- For any ordinal α, $V_{\alpha+1}$ is the powerset of V_α.
- If λ is a limit ordinal, then $V_\lambda := \bigcup_{\alpha<\lambda} V_\alpha$.
- $\mathbf{V} := \bigcup_{\alpha} V_\alpha$.

Various intermediate stages of the construction of $\mathbf{V}$ are models of fragments of ZF.

The scheme $\Phi(\mathscr{L})$ consists of formulas ϕ_n for each $n \in \omega$ expressing that there exists a cardinal κ which is n-Mahlo and the structure $(V_\kappa, \in, \ldots)$ is a $\Sigma_n(\mathscr{L})$-elementary substructure of $(\mathbf{V}, \in, \ldots)$. A α-Mahlo cardinal is a particular type of large cardinal and the existence of the various Mahlo cardinals is independent from ZFC.

The theory GBC is the Gödel-Bernay theory of classes, a conservative extension of ZFC with two-sorted models, with one sort ranging over sets and the other over classes.

Theorem 4.13. *Let $\mathscr{L}$ be the language $\{\in, \lhd\}$.*
(a) Let T be a consistent completion of $ZFC + \Phi$. There is a model $\mathscr{M}$ of T such that for some proper elementary end extension $\mathscr{N}$ of $\mathscr{M}$, there is an automorphism whose fixed-point set is M.
(b) For any model $\mathscr{N}$ of $EST(\mathscr{L}) + GW^*$, if M is the fixed-point set of an automorphism of $\mathscr{N}$ and M is an initial segment of N, then $\mathscr{M} \models ZFC + \Phi$.

Theorem 4.13 is different in style than the previous two main theorems, since it is not an equivalence of two statements, but rather two independent implications that are almost eachothers converse. The reaon for this lies in the proof of part (a). The proof uses a model $(\mathscr{M}, \mathscr{A})$ of the theory GBC

extended with the statement that "**Ord** is weakly compact" (OWC). Theorem 2.1 in [3] garantuees that any completion of $ZFC + \Phi$ has a countable model that can be expanded to a model of $GBC + OWC$.

The question remains if every countable model of $ZFC + \Phi$ can be expanded in such a way. If so, then Theorem 4.13 can be formulated in the same style as Theorems 3.1 and 4.2, an equivalence of two statements.

With the existence of a model of $GBC + OWC$ established, the proof of part (a) follows the exact same recipe as the proof of (b) $\Rightarrow$ (a) of Theorem 4.2; It starts with the existence of a generic ultrafilter over the poset of unbounded subsets of **Ord**. This ultrafilter is then shown to be ($\mathscr{M}, \mathscr{A}$-complete, -iterable and -canonically Ramsey in the same way as in Theorem 4.2.

The model $\mathscr{N}$ is then constructed by the same iterated ultrapower construction along the linear order $\mathbb{Z}$ and finally, an automorphism like $n \mapsto n+1$ which leaves no element of $\mathbb{Z}$ fixed will induce an automorphism on the model $\mathbb{N}$ which has M as fixed-point set.

Like in Theorems 3.1 and 4.2, the proof of the other part of Theorem 4.13 mostly consists of using the automorphism and the fact that it fixed M to verify that M has the required properties. It is first proven that with $\mathscr{A} = \{a_E \cap M : a \in N\}$ (here a_E is the set coded in $\mathscr{N}$ by a), $(\mathscr{M}, \mathscr{A}) \models GBC + OWC$ and that from this follows that $\mathscr{M} \models ZFC + \Phi$.

5 Conclusion

In the introduction, the question "Are our axiomatizations of foundational theories natural?" was asked. After having seen theorems 3.1, 4.2 and 4.13 the answer to this question can be a cautious "yes". While the theories discussed in these theorems don't arise from some mystical oracle of universal truth, we have found that they are very strongly related to weaker theories.

Theorem 3.1 gives a clear-cut correlation between the theories $I\Delta_0 + B\Sigma_1 + Exp$ and $I\Delta_0$, through models generated by automorphisms. This means that while $I\Delta_0 + B\Sigma_1 + Exp$ is a stronger theory than $I\Delta_0$, it can be characterized completely by $I\Delta_0$ since $\mathscr{M}$ is a model of $I\Delta_0 + B\Sigma_1 + Exp$ if and only if it is the largest initial segment that is fixed by an automorphism of a model of $I\Delta_0$.

The same result is obtained for ACA_0, a fragment of second-order arithmetic. By Theorem 4.2, this theory is also completely characterized by $I\Delta_0$. The characterization here is slightly different as we no longer require the smaller model to be the largest initial segment fixed by the automorphism, but rather that the smaller model is the fixed-point set of the automorphism.

An extra criterium is added that requires the class of sets in the model of ACA_0 to be equal to those sets that are coded in the larger model. The end-result remains the same though, $(\mathscr{M}, \mathscr{A})$ is a model of ACA_0 if and only if M is the fixed-point set of an automorphism of a model $\mathscr{N}$ of $I\Delta_0$ and $\mathscr{A} = SSy_M(\mathscr{N})$.

The set-theoretic result, Theorem 4.13 is not as powerful as the previous two. It requires that any countable model of $ZFC + \Phi$ can be extended to a model of $GBC + OWC$. Without this, a full equivalence can't be established.

It is worth noting that all three proofs use similar constructions. The ultrapower construction is used in similar ways in all three proofs and plays a pivotal role. Similarly, certain combinatorial aspects and Ramseys Theorem show up in all of the proofs. In the two arithmetical theorems, finite set theory simulated within arithmetic is used, as well as the powerful technique of coding of sequences.

In the end, we can conclude that these results inspire confidence that our choice of axiomatization for some of our foundational theories is not just an arbitary choice that worked out well, but that these stronger theories can be traced back to a basis of weaker theories. The picture is not yet complete though; in the set-theoretic case the equivalence hasn't been fully established.

And the question remains if we can characterize our theories in terms of even weaker fragments than $I\Delta_0$. In order to establish such results (if that is at all possible), new machinery will have to be developed first, since if we step down to theories weaker than $I\Delta_0$ we quickly lose some of the tools that were necessary to establish the results that we already have, such as coding, arithmetized set-theory and basic (Δ_0) induction.

References

[1] A. Enayat, "Automorphisms of models of bounded arithmetic," *Fundamenta Mathematicae*, 2006.

[2] A. Enayat, "From bounded arithmetic to second-order arithmetic via automorphisms," in *Logic in Tehran*, 2003.

[3] A. Enayat, "Automorphisms, mahlo cardinals and nfu," in *Nonstandard Models of Arithmetic and Set Theory*, 2004.

[4] J. H. Bennet, *On Spectra.* PhD thesis, Princeton University, 1962.

[5] P. Hájek and P. Pudlák, *Metamathematics of First Order Arithmetic.* Springer, Heidelberg, 1993.

[6] C. Dimitracopoulos and H. Gaifman, “Fragments of peano arithmetic and the mrdp theorem,” in *Logic and Algorithmic*, 1982.

[7] A. Wilkie and J. Paris, “On the existance of end extension of models of bounded induction,” in *Logic, methodology and philosophy of science*, 1989.

[8] W. Veldman, *Lecture Notes: Model Theory*, ch. 6. Radboud University Nijmegen, 2006.

[9] P. R. R. Graham and J. Spencer, *Ramsey Theory*. Wiley-Interscience Publications, New York, 1980.

[10] P. Erdös and R. Rado, “A combinatorial theorem,” *Journal of the London Mathematical Society*, 1950.