

## Automorphisms of models of bounded arithmetic

by

Ali Enayat (Washington, DC)

**Abstract.** We establish the following model-theoretic characterization of the fragment  $I\Delta_0 + \text{Exp} + B\Sigma_1$  of Peano arithmetic in terms of *fixed points* of automorphisms of models of bounded arithmetic (the fragment  $I\Delta_0$  of Peano arithmetic with induction limited to  $\Delta_0$ -formulae).

**THEOREM A.** *The following two conditions are equivalent for a countable model  $\mathfrak{M}$  of the language of arithmetic:*

- (a)  $\mathfrak{M}$  satisfies  $I\Delta_0 + B\Sigma_1 + \text{Exp}$ ;
- (b)  $\mathfrak{M} = I_{\text{fix}}(j)$  for some nontrivial automorphism  $j$  of an end extension  $\mathfrak{N}$  of  $\mathfrak{M}$  that satisfies  $I\Delta_0$ .

Here  $I_{\text{fix}}(j)$  is the largest initial segment of the domain of  $j$  that is pointwise fixed by  $j$ ,  $\text{Exp}$  is the axiom asserting the totality of the exponential function, and  $B\Sigma_1$  is the  $\Sigma_1$ -collection scheme consisting of the universal closure of formulae of the form

$$[\forall x < a \exists y \varphi(x, y)] \rightarrow [\exists z \forall x < a \exists y < z \varphi(x, y)],$$

where  $\varphi$  is a  $\Delta_0$ -formula. Theorem A was inspired by a theorem of Smoryński, but the method of proof of Theorem A is quite different and yields the following strengthening of Smoryński's result:

**THEOREM B.** *Suppose  $\mathfrak{M}$  is a countable recursively saturated model of PA and  $I$  is a proper initial segment of  $\mathfrak{M}$  that is closed under exponentiation. There is a group embedding  $j \mapsto \hat{j}$  from  $\text{Aut}(\mathbb{Q})$  into  $\text{Aut}(\mathfrak{M})$  such that  $I = I_{\text{fix}}(\hat{j})$  for every nontrivial  $j \in \text{Aut}(\mathbb{Q})$ . Moreover, if  $j$  is fixed point free, then the fixed point set of  $\hat{j}$  is isomorphic to  $\mathfrak{M}$ .*

Here  $\text{Aut}(X)$  is the group of automorphisms of the structure  $X$ , and  $\mathbb{Q}$  is the ordered set of rationals.

### 1. INTRODUCTION

In recent work [E-1, E-2] the author has embarked upon the project of characterizing *strong* foundational axiomatic systems of set theory and arith-

---

2000 *Mathematics Subject Classification*: Primary 03F30, 03C62, 03H15; Secondary 03C15, 20B27.

*Key words and phrases*: first order arithmetic, bounded arithmetic, recursive saturation, automorphism.

metic in terms of the fixed point sets of automorphisms of models of *weak* systems of set theory and arithmetic. For example [E-1, Theorem B] shows that if  $j$  is a nontrivial automorphism of a model  $\mathfrak{N}$  of a weak system of set theory whose set of fixed points forms an *initial segment* of  $\mathfrak{N}$ , then the set of fixed points gives rise to a model of full Zermelo–Fraenkel set theory ZFC that additionally satisfies the scheme  $\Phi$  asserting the existence of  $\Sigma_n$ -reflective  $n$ -Mahlo cardinals of all finite orders  $n$ . Moreover, this result has a strong “reversal”: every completion of  $ZFC + \Phi$  has a model  $\mathfrak{M}$  which has an elementary end extension to a model  $\mathfrak{N}$  that possesses a nontrivial automorphism whose set of fixed points is precisely the universe of  $\mathfrak{M}$  [E-1, Theorem A]. As explained in [E-1, E-2], this project is intimately linked to the study of the metamathematics of the system NFU, introduced by Jensen [J] as a modification of Quine’s unorthodox *New Foundations* (NF) system of set theory with a universal set introduced in [Q]. However, the fruits of the project can equally well be viewed as contributions to the chapter of model theory that focuses on structural characterizations of axiomatic theories, especially foundational ones <sup>(1)</sup>.

The paper [E-2] extended the set-theoretic ideas initiated in [E-1] to the realm of arithmetic and exhibited model-theoretic characterizations of PA (Peano arithmetic),  $ACA_0$  (arithmetical comprehension schema with restricted induction), and  $Z_2$  (full second order arithmetic) in terms of automorphisms of models of bounded arithmetic (the fragment  $I\Delta_0$  of PA). The characterization of PA in [E-2] is analogous to the aforementioned characterization of  $ZFC + \Phi$ : [E-2, Theorem B] shows that if  $j$  is a nontrivial automorphism of a model  $\mathfrak{N}$  of  $I\Delta_0$  whose set of fixed points  $M$  forms an initial segment of  $\mathfrak{N}$ , then  $(M, \oplus^{\mathfrak{N}}, \odot^{\mathfrak{N}})$  is a model of PA. Moreover, *every* model  $\mathfrak{M}$  of PA has an elementary end extension to a model  $\mathfrak{N}$  that possesses a nontrivial automorphism  $j$  whose set of fixed points is precisely  $M$  (the latter result is implicit in Gaifman’s [Ga], but it is given a new proof in [E-2, Theorem A]).

In this paper we take a further step in the arithmetical realm of our project by characterizing the important fragment  $I\Delta_0 + \text{Exp} + B\Sigma_1$  of PA in terms of automorphisms of models of  $I\Delta_0$ . More specifically, in Theorem A of Section 3 we prove that countable models of the language of first order arithmetic that satisfy  $I\Delta_0 + \text{Exp} + B\Sigma_1$  are precisely countable models of the form

$$I_{\text{fix}}(j) := \{x \in \text{dom}(j) : \forall y \leq x \ j(y) = y\},$$

---

<sup>(1)</sup> Two prominent sources of work in this direction that deal with arithmetical theories are those by Ressayre [R] and Kaye [Ka-1]. Ressayre’s work provides characterizations of PA, and of its fragment  $I\Sigma_1$ , in terms of *endomorphisms* of models of  $I\Delta_0$  onto proper initial segments of themselves. Kaye’s work, on the other hand, characterizes PA amongst extensions of  $I\Delta_0 + \text{Exp}$  in terms of the behavior of elementary extensions of its models.

where  $j$  is a nontrivial automorphism of a model of  $I\Delta_0$ . This result was motivated by a theorem, due to Smoryński [Sm], that shows that any proper initial segment of a countable recursively saturated model  $\mathfrak{M}$  of PA that is closed under exponentiation can be realized as  $I_{\text{fix}}(j)$  for some automorphism  $j$  of  $\mathfrak{M}$ . However, our methods are quite different from Smoryński's, and as shown in Theorem B of Section 4, they yield a perspicuous proof of an extension of his result. In Section 5 we discuss further work which characterizes the conservative *second order* extension  $WKL_0^*$  of  $I\Delta_0 + \text{Exp} + B\Sigma_1$ .

**Acknowledgments.** I am indebted to the anonymous referee for helpful comments on earlier drafts of the paper, and most importantly, for detecting a gap in my initial attempt in establishing part (a) of Lemma 3.7. I am also grateful to Roman Kossak and Jim Schmerl for steady encouragement, to Zosia Adamowicz, Jeremy Avigad, Jerry Keisler, Joe Mileti, Steve Simpson, and Robert Solovay for stimulating correspondence, and to Mauro Di Nasso for inviting me to present my work in Pisa during June 2004.

## 2. PRELIMINARIES

In this section we review key notions and results regarding the metamathematics of first order arithmetic that are central to this paper. We refer the reader to the texts of Hájek–Pudlák [HP] and Kaye [Ka-2] for further elaboration.

### First order arithmetic

- The language of first order arithmetic,  $\mathcal{L}_A$ , is  $\{+, \cdot, \text{Succ}(x), <, 0\}$ .
- Models of  $\mathcal{L}_A$  are of the form  $\mathfrak{M} = (M, \oplus^{\mathfrak{M}}, \dots)$ ,  $\mathfrak{N} = (N, \oplus^{\mathfrak{N}}, \dots)$ , etc. For models  $\mathfrak{M}$  and  $\mathfrak{N}$  of  $\mathcal{L}_A$ , we say that  $\mathfrak{N}$  *end extends*  $\mathfrak{M}$  (equivalently:  $\mathfrak{M}$  is an *initial* submodel of  $\mathfrak{N}$ ), written  $\mathfrak{M} \subseteq_e \mathfrak{N}$ , if  $\mathfrak{M}$  is a submodel of  $\mathfrak{N}$  and  $a < b$  for every  $a \in M$  and  $b \in N \setminus M$ .  $\mathfrak{N}$  is a *cofinal extension* of  $\mathfrak{M}$ , written  $\mathfrak{M} \subseteq_c \mathfrak{N}$ , if for every  $b \in N$  there is some  $a \in M$  with  $a < b$ .
- Given a language  $\mathcal{L} \supseteq \mathcal{L}_A$ , an  $\mathcal{L}$ -formula  $\varphi$  is said to be a  $\Delta_0(\mathcal{L})$ -*formula* if all the quantifiers of  $\varphi$  are bounded by terms of  $\mathcal{L}$ , i.e., they are of the form  $\exists x \leq t$  or  $\forall x \leq t$ , where  $t$  is a term of  $\mathcal{L}$  not involving  $x$ .  $\Delta_0(\mathcal{L})$ -formulae are also known as *bounded* formulae of  $\mathcal{L}$ . A  $\Sigma_1(\mathcal{L})$ -*formula* is of the form  $\exists x \varphi$ , where  $\varphi$  is a  $\Delta_0(\mathcal{L})$ -formula. We shall omit the reference to  $\mathcal{L}$  if  $\mathcal{L} = \mathcal{L}_A$ , e.g., the set of  $\Delta_0$ -formulae is simply the set of  $\Delta_0(\mathcal{L}_A)$ -formulae.
- *Bounded arithmetic*, or  $I\Delta_0$ , is the fragment of Peano arithmetic with the induction scheme limited to  $\Delta_0$ -formulae. More specifically, it is a theory formulated in the language  $\mathcal{L}_A$ , and is obtained by adding

the scheme of induction for  $\Delta_0$ -formulae to Robinson's arithmetic  $Q$ . When  $\mathcal{L} \supseteq \mathcal{L}_A$ , we shall use  $I\Delta_0(\mathcal{L})$  to refer to the extension of  $I\Delta_0$  which includes induction for  $\Delta_0(\mathcal{L})$ -formulas. The metamathematical study of bounded arithmetic has close ties with the subject of computational complexity; see [HP] or [Kr] for thorough introductions.

- Every model  $\mathfrak{M}$  of  $I\Delta_0$  has an initial segment  $\mathbb{N}$  consisting of the standard elements of  $\mathfrak{M}$ . We use  $\mathbb{N}^+$  to denote  $\mathbb{N} \setminus \{0\}$ , and use  $\omega$  for the order type of  $\mathbb{N}$ .
- Bennett [Ben] showed that the graph of the exponential function  $y = 2^x$  can be defined by a  $\Delta_0$ -predicate in the standard model of arithmetic. This result was later fine-tuned by Paris <sup>(2)</sup> who found another  $\Delta_0$ -predicate  $\text{Exp}(x, y)$  which has the additional feature that  $I\Delta_0$  can prove the familiar algebraic laws about exponentiation for  $\text{Exp}(x, y)$  [DG, Appendix 1], in particular:

LEMMA 2.1.  *$I\Delta_0$  proves the following statements:*

- (a)  $\forall x \exists^{\leq 1} y \text{Exp}(x, y)$ ;
- (b)  $\forall x (\exists y \text{Exp}(x, y) \rightarrow \forall z < x \exists y \text{Exp}(z, y))$ ;
- (c)  $\forall x \forall y (\text{Exp}(x, y) \rightarrow \text{Exp}(x + 1, 2y))$ .

- By a classical theorem of Parikh,  $I\Delta_0$  can only prove the totality of functions with a polynomial growth rate, hence

$$I\Delta_0 \not\vdash \forall x \exists y \text{Exp}(x, y).$$

- $I\Delta_0 + \text{Exp}$  is the extension of  $I\Delta_0$  obtained by adding the axiom

$$\text{Exp} := \forall x \exists y \text{Exp}(x, y).$$

The theory  $I\Delta_0 + \text{Exp}$  might not appear to be particularly strong since it cannot even prove the totality of the superexponential function, but experience has shown that it is a remarkably robust theory that is able to prove an extensive array of theorems of number theory and finite combinatorics. This has prompted Harvey Friedman to put forth the conjecture that all “arithmetical theorems” proved in the journal *Annals of Mathematics* (such as Wiles' proof of Fermat's Last Theorem) can be implemented within  $I\Delta_0 + \text{Exp}$ . The reader interested in further pursuing this topic is referred to Avigad's thorough discussion in [Av-2].

- For  $\mathcal{L} \supseteq \mathcal{L}_A$ ,  $B\Sigma_1(\mathcal{L})$  is the scheme consisting of the universal closure of formulae of the form

---

<sup>(2)</sup> Independently, Pudlák [Pu] also provided an  $I\Delta_0$ -treatment of the exponential function. There is also a detailed treatment of this topic in [Bu] and [HP, Section V3(c)].

$$[\forall x < a \exists y \varphi(x, y)] \rightarrow [\exists z \forall x < a \exists y < z \varphi(x, y)],$$

where  $\varphi(x, y)$  is a  $\Delta_0(\mathcal{L})$ -formula. It has been known since the work of Parsons [Pars] that there are instances of  $B\Sigma_1$  that are unprovable in  $I\Delta_0 + \text{Exp}$ ; indeed Parson's work shows that even strengthening  $I\Delta_0 + \text{Exp}$  with the set of  $\Pi_2$ -sentences that are true in the standard model of arithmetic fails to prove all instances of  $B\Sigma_1$ . However, Harvey Friedman and Jeff Paris have shown, independently, that adding  $B\Sigma_1$  does not increase the  $\Pi_2$ -consequences of  $I\Delta_0 + \text{Exp}$  [Ka-2, Corollary 10.9]. See also [Sie], [Av-1], [Ka-3], [Bek], and [H] for further refinements.

- $I$  is a *cut* of  $\mathfrak{M}$  if  $I$  is a nonempty *proper* initial segment of  $\mathfrak{M}$  with no last element.
- If  $I$  is a cut of a model  $\mathfrak{M}$  of  $I\Delta_0$  that is closed under addition and multiplication, then we continue to use  $I$  to refer to the model

$$(I, \oplus^{\mathfrak{M}}, \odot^{\mathfrak{M}}, \dots).$$

The following results will be useful in this paper.

LEMMA 2.2. *Suppose  $\mathfrak{M}$  is a model of  $I\Delta_0(\mathcal{L})$ , and let  $S_\varphi$  be the solution set of some  $\Delta_0(\mathcal{L})$ -formula  $\varphi(x, \mathbf{a})$  in  $\mathfrak{M}$ , where  $\mathbf{a}$  is a sequence of parameters from  $M$ . If  $S_\varphi \neq \emptyset$ , then:*

- $[\Delta_0\text{-MIN}]$   $S_\varphi$  has a minimum element;
- $[\Delta_0\text{-MAX}]$  if  $S_\varphi$  is bounded in  $\mathfrak{M}$ , then  $S_\varphi$  has a maximum element;
- $[\Delta_0\text{-OVERSPILL}]$  if  $S_\varphi$  includes a cut  $I$  of  $\mathfrak{M}$ , then for some  $b \in M \setminus I$ ,  $\{x \in M : x < b\} \subseteq S_\varphi$ .

*Proof.* A routine proof by contradiction proves (a), with  $\Delta_0(\mathcal{L})$  induction applied to  $\varphi^*(v) := \forall x \leq v \neg \varphi(x)$ ; (b) follows from (a) since the maximum of  $S_\varphi$  is the least upper bound of  $S_\varphi$ , and (c) follows from (b). ■

LEMMA 2.3 (Folklore, see [WP, Theorem 1]). *If  $I$  is a cut of a model of  $I\Delta_0$  that is closed under multiplication, then  $I$  satisfies  $I\Delta_0 + B\Sigma_1$ .*

THEOREM 2.4 (Wilkie–Paris [WP], see [Ad-1] for refinements). *Every countable model of  $I\Delta_0 + \text{Exp} + B\Sigma_1$  has an end extension to a model of  $I\Delta_0 + B\Sigma_1$ .*

REMARK 2.4.1. Theorem 2.4 above is slightly stronger than the original form of the Paris–Wilkie result, which makes no mention of arranging the end extension to satisfy  $B\Sigma_1$ . However, using  $\Delta_0\text{-OVERSPILL}$  and Lemma 2.3, one can easily derive Theorem 2.4 from the original Paris–Wilkie result as follows. Suppose  $\mathfrak{M}$  is a countable model of  $I\Delta_0 + \text{Exp} + B\Sigma_1$ , and let  $\mathfrak{M}^*$  be an end extension of  $\mathfrak{M}$  which satisfies  $I\Delta_0$ . Choose  $d \in M^* \setminus M$ , and consider the  $\Delta_0$ -formula  $\varphi(x) := \exists y < d \text{Exp}(x, y)$ . Since every  $m \in M$  is a

solution of  $\varphi(x)$ , there is some  $c \in M^* \setminus M$  for which  $2^c$  exists in  $\mathfrak{M}^*$ . The desired end extension of  $\mathfrak{M}$  satisfying  $I\Delta_0 + B\Sigma_1$  is the submodel of  $\mathfrak{M}^*$  consisting of elements of  $M^*$  that are less than  $c^n$  for some  $n \in \mathbb{N}$ .

**THEOREM 2.5** (Dimitracopoulos–Gaifman [DG, Prop. 2.3], see also [Bu, Theorem 1.2.7.3, and its corollary]). *Suppose  $\mathfrak{M}$  is a model of  $I\Delta_0 + B\Sigma_1$  and  $\mathcal{F}$  is the family of all  $M$ -valued functions  $f(x_1, \dots, x_n)$  on  $M^n$  (where  $n \in \mathbb{N}^+$ ) such that for some  $\Sigma_1$ -formula  $\delta(x_1, \dots, x_n, y)$ ,  $\delta$  defines the graph of  $f$  in  $\mathfrak{M}$  and for some term  $(^3) t(x_1, \dots, x_n)$ ,  $f(a_1, \dots, a_n) \leq t(a_1, \dots, a_n)$  for all  $a_i \in M$ . Then the expanded structure*

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

*satisfies  $I\Delta_0(\mathcal{L}_{\mathcal{F}}) + B\Sigma_1(\mathcal{L}_{\mathcal{F}})$ , where  $\mathcal{L}_{\mathcal{F}}$  is the result of augmenting the language of arithmetic with names for each  $f \in \mathcal{F}$ .*

**REMARK 2.5.1.** Since for each  $m \in M$ , the constant function  $c_m : M \rightarrow \{m\}$  is a member of  $\mathcal{F}$ , for all intents and purposes  $\mathcal{L}_{\mathcal{F}}$  has a name for each element of  $M$ .

**Set theory and combinatorics within bounded arithmetic.** One can use *Ackermann coding* to simulate finite set theory and combinatorics within  $I\Delta_0$  by using a  $\Delta_0$ -predicate  $E(x, y)$  that reasonably expresses

“the  $x$ th digit in the binary expansion of  $y$  is 1”

(see [HP]).  $E$  in many ways behaves like the membership relation  $\in$ ; indeed, it is well known that  $\mathfrak{M}$  is a model of PA iff  $(M, E)$  is a model of  $ZF \setminus \{\text{Infinity}\} \cup \{\neg\text{Infinity}\}$ .

- We shall reserve the symbol  $E$  throughout the paper to refer to “Ackermann’s  $\in$ ”.

When  $\mathfrak{M}$  is a model of  $I\Delta_0$ , then  $(M, E)$  is still a model of a decent fragment of set theory, as witnessed by the following result (see [DG], [HP, I.1(B)] for more detail):

**THEOREM 2.6.** *If  $\mathfrak{M} \models I\Delta_0(\mathcal{L})$ , and  $E$  is Ackermann’s  $\in$ , then  $\mathfrak{M}$  satisfies the following axioms:*

- (a) *Extensionality:*

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

- (b) *Conditional Pairing* [ $\forall x \forall y$  (“if  $x < y$  and  $2^y$  exists, then  $\{x, y\}$  exists”)]:

$$\forall x \forall y ((x < y) \wedge \exists u \text{Exp}(y, u)) \rightarrow \exists t \forall w (wEt \leftrightarrow (w = x) \vee (w = y));$$

---

(<sup>3</sup>) In this context, the notation  $t(x_1, \dots, x_n)$  is employed for a term whose variables form a *subset* of the displayed variables.

(c) *Union*:

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

(d) *Conditional Power Set* [ $\forall x$  (“if  $2^x$  exists, then the power set of  $x$  exists”)]:

$$\forall x (\exists y \text{Exp}(x, y) \rightarrow (\exists z \forall w (wEz \leftrightarrow w \subseteq x))),$$

where  $w \subseteq x$  abbreviates  $\forall t (tEw \rightarrow tEx)$ ;

(e) *Conditional  $\Delta_0(\mathcal{L})$ -Comprehension Scheme*: for each  $\Delta_0(\mathcal{L})$ -formula  $\varphi(x, y)$ , and any  $z$  for which  $2^z$  exists, “ $\{xEz : \varphi(x, y)\}$  exists”, i.e.,

$$\forall y \forall z [\exists s \text{Exp}(z, s) \rightarrow \exists u \forall t (tEu \leftrightarrow (tEz \wedge \varphi(x, y)))].$$

- We shall say that  $X \subseteq M$  is *coded* in  $\mathfrak{M}$  if there is some  $c \in M$  such that  $X = c_E := \{m \in M : mEc\}$ .
- Given  $c \in M$ ,  $\bar{c} := \{x \in M : x < c\}$ . Note that  $\bar{c}$  is coded in an  $\mathfrak{M} \models I\Delta_0$  provided  $2^c$  exists in  $\mathfrak{M}$ .
- Suppose  $I$  is a cut of  $\mathfrak{M}$ , and set  $\text{SSy}_I(\mathfrak{M}) := \{c_E \cap I : c \in N\}$ . When  $I$  is the *standard cut*  $\mathbb{N}$  of  $\mathfrak{M}$ , then  $\text{SSy}_I(\mathfrak{M})$  is what is known in the literature as the *standard system* of  $\mathfrak{M}$ .
- Within  $I\Delta_0$  one can define a *partial* function  $\text{Card}(x) = t$ , expressing “the cardinality of the set coded by  $x$  is  $t$ ”. More specifically  $\text{Card}(x) = t$  expresses “there is a bijection between  $x_E$  and  $\bar{t}$ ”. It is important to note that  $I\Delta_0$  can prove that  $\text{Card}(x)$  is defined (and is well-behaved) if  $2^x$  exists (this is implicit in [HP, p. 42, Theorem 1.41]).
- In light of the above discussion, finite combinatorial statements have reasonable arithmetical translations in models of bounded arithmetic provided “enough powers of 2 exist”. We shall therefore use the Erdős notation  $a \rightarrow (b)_d^n$  for the *arithmetical* translation of the set-theoretic statement “if  $\text{Card}(X) = a$  and  $f : [X]^n \rightarrow \bar{d}$ , then there is  $H \subseteq X$  with  $\text{Card}(H) = b$  such that  $H$  is  $f$ -monochromatic.” Here  $[X]^n$  is the collection of *increasing*  $n$ -tuples from  $X$  (where the order on  $X$  is inherited from the ambient model of arithmetic), and  $H$  is  $f$ -*monochromatic* iff  $f$  is constant on  $[H]^n$ .
- We also write  $a \rightarrow *(b)^n$  for the arithmetical translation of the following canonical partition relation: if  $\text{Card}(X) = a$  and  $f : [X]^n \rightarrow Y$ , then there is  $H \subseteq X$  with  $\text{Card}(H) = b$  which is  $f$ -*canonical*, i.e., there is some  $S \subseteq \{1, \dots, n\}$  such that for all sequences  $s_1 < \dots < s_n$  and  $t_1 < \dots < t_n$  of elements of  $H$ ,

$$f(s_1, \dots, s_n) = f(t_1, \dots, t_n) \Leftrightarrow \forall i \in S (s_i = t_i).$$

Note that if  $S = \emptyset$ , then  $f$  is constant on  $[H]^n$ , and if  $S = \{1, \dots, n\}$ , then  $f$  is injective on  $[H]^n$ .

- We need certain quantitative forms of Ramsey's partition theorem, as well as its canonical generalization by Erdős and Rado. Before stating them, let us review the definition of the iterated exponential function, dubbed the *superexponential function*  $\text{Superexp}(n, x)$  in this paper:  $\text{Superexp}(0, x) = x$ , and

$$\text{Superexp}(n + 1, x) = 2^{\text{Superexp}(n, x)}.$$

Thus for  $n \geq 1$ ,  $\text{Superexp}(n, x)$  is the exponential stack of length  $n+1$ , where the top element is  $x$ , and the remaining  $n$  entries form a tower of 2's.

**THEOREM 2.7.** *For each  $n \in \mathbb{N}^+$ , the following is provable in  $I\Delta_0$ :*

- (a) [Ramsey]  $a \rightarrow (b)_c^n$ , if  $a = \text{Superexp}(2n, bc)$  and  $b \geq n^2$ ;
- (b) [Erdős–Rado]  $a \rightarrow *(b)^n$  if  $a = \text{Superexp}(4n, b \cdot 2^{2^{2n^2-n}})$  and  $b \geq 4n^2$ .

*Proof.* Part (a) follows immediately from Ramsey's original proof (reproduced in [GRS]). Part (b) can be obtained by coupling (a) with the proof of the Erdős–Rado canonical partition theorem [ER, Sec. 6]. More specifically, the Erdős–Rado proof shows that  $a \rightarrow *(b)^n$  is derivable from  $a \rightarrow (b)_{f(n)}^{2n}$ , where  $f(n)$  is the number of *partitions* of  $[\overline{2n}]^2$ , i.e.,

$$f(n) := B(2n^2 - n) < 2^{2^{2n^2-n}}.$$

Here  $B(s)$  is the number of partitions of an  $s$ -element set (by elementary considerations  $B(s) < 2^{2^s}$ ). For example, if  $a \rightarrow (b)_{203}^4$ , then  $a \rightarrow *(b)^2$  since  $f(2) = B(6) = 203$  (see [GRS, Theorem 2, Sec. 5.5]). ■

### Recursive saturation

- $\mathfrak{M}$  is *recursively saturated* if for every finite sequence  $\mathbf{m}$  of elements of  $M$ , every recursive finitely realizable type over the expanded model  $(\mathfrak{M}, \mathbf{m})$  is realized in  $\mathfrak{M}$ .
- For  $\mathfrak{M} \models \text{PA}$  let  $F \subseteq M$  be the set of Gödel numbers of  $\mathcal{L}_A$ -formulas, as computed in  $\mathfrak{M}$  (note that  $F$  will include nonstandard elements if  $\mathfrak{M}$  is nonstandard). A *satisfaction class* of  $\mathfrak{M}$  is a subset  $S$  of  $M$  satisfying the following two conditions:

- (a)  $(\mathfrak{M}, S) \models \text{PA}(S)$ ,
- (b)  $S$  correctly codes the satisfaction relation of  $\mathfrak{M}$  for all standard formulas.

Condition (b) can be written as a scheme consisting of the sentence (1) below plus the collection of sentences  $(2_n)$  below (for each  $n \in \mathbb{N}^+$ );

- (1)  $S$  consists of coded ordered pairs of the form  $\langle a, b \rangle$ , where  $a \in F$  and  $b \in M$ ;
- (2 <sub>$n$</sub> ) [ $S$  is  $n$ -correct]  $S$  satisfies Tarski's inductive conditions for a truth predicate for all formulas of quantifier rank  $n$  (including any non-standard ones).

It is well known that for each standard  $n$  there is a parameter free definable subset  $S_n$  of  $\mathfrak{M}$  that satisfies (1) and (2 <sub>$n$</sub> ), but of course Tarski's undefinability of truth theorem dictates that any  $\mathfrak{M}$ -definable  $S$  that satisfies (1) must fail (2 <sub>$n$</sub> ) for some  $n$ . Note that if  $S$  is a satisfaction class of a nonstandard model of PA, then  $S$  is  $s$ -correct for some *nonstandard*  $s$ . This follows from overspill and the fact that (2 <sub>$n$</sub> ) can be uniformly expressed by a single formula  $\varphi(S, n)$  with parameter  $n$  in the language of arithmetic augmented with the unary predicate  $S$ .

The following two theorems tie the notion of recursive saturation with satisfaction classes, and with cofinal extensions.

**THEOREM 2.8** (Barwise–Schlipf [BS]). *A countable model  $\mathfrak{M}$  of PA is recursively saturated iff  $\mathfrak{M}$  has a satisfaction class.*

**THEOREM 2.9** (Smoryński–Stavi [Sm-St]). *A cofinal extension of a recursively saturated model of PA remains recursively saturated.*

Theorem 2.8 can be derived from Theorem 2.7, coupled with the following theorem (see also [Ka-2, Exercise 14.9]).

**THEOREM 2.10** (Kotlarski [Kot], Schmerl [Sc-1]). *If  $\mathfrak{M}^*$  is a cofinal elementary extension of a model  $\mathfrak{M}^*$  of PA, and  $X \subseteq M$  is piecewise coded (i.e., for every  $m \in M$ ,  $\overline{m} \cap X$  is coded in  $\mathfrak{M}$ ), then there is a (unique)  $X^*$  such that*

$$(\mathfrak{M}, X) \prec (\mathfrak{M}^*, X^*).$$

### 3. AUTOMORPHISMS AND $I\Delta_0 + \text{Exp} + B\Sigma_1$

Our point of departure is the following result that characterizes cuts of countable recursively saturated models  $\mathfrak{M}$  of PA that are closed under exponentiation as precisely those of the form  $I_{\text{fix}}(j)$  for some automorphism  $j$  of  $\mathfrak{M}$ .

**THEOREM 3.1** <sup>(4)</sup>. *Suppose  $\mathfrak{M}$  is a model of PA.*

- (a) *If  $j \in \text{Aut}(\mathfrak{M})$ , then  $I_{\text{fix}}(j) \models \text{Exp}$ .*

---

<sup>(4)</sup> Smoryński established the much harder part (b) of Theorem 3.1 and left the status of part (a) as an open problem. It is not clear who first established part (a) of Theorem 3.1, but by now it is considered part of the folklore, e.g., see [Ka-4, Proposition 2.2].

- (b) (Smoryński [Sm]) *If  $\mathfrak{M}$  is countable and recursively saturated, and  $I$  is a cut of  $\mathfrak{M}$  that satisfies  $\text{Exp}$ , then there are continuum-many  $j \in \text{Aut}(\mathfrak{M})$  such that  $I = I_{\text{fix}}(j)$ .*

The first principal result of this section (Lemma A.2) improves (a) of Theorem 3.1 by showing that (a) remains valid upon replacing the assumption  $\mathfrak{M} \models \text{PA}$  with the weaker assumption  $\mathfrak{M} \models I\Delta_0$ . This result shows that the mere existence of a nontrivial automorphism  $j$  of a model  $\mathfrak{M}$  of  $I\Delta_0$  produces the cut  $I_{\text{fix}}(j)$  of  $\mathfrak{M}$  that satisfies the robust theory  $I\Delta_0 + \text{Exp} + B\Sigma_1$ . We shall then establish a “reversal” of this result as follows: beginning with a cut  $I$  of a countable model  $\mathfrak{M}$  of  $I\Delta_0$  that is closed under exponentiation, we fine-tune an Ehrenfeucht–Mostowski-type construction of Paris and Mills [PM] in order to build an extension of  $\mathfrak{M}$  that (i) satisfies  $I\Delta_0$ , (ii) does not introduce new elements below any  $i \in I$ , and (iii) possesses an automorphism  $j$  such that  $I_{\text{fix}}(j) = I$ . Coupled with Wilkie and Paris’s fundamental Theorem 2.4, this yields the reversal. To summarize, in this section we shall prove:

**THEOREM A.** *The following two conditions are equivalent for a countable model  $\mathfrak{M}$  of the language  $\mathcal{L}_A$  of arithmetic:*

- (a)  $\mathfrak{M} = I_{\text{fix}}(j)$  for some nontrivial automorphism  $j$  of a model  $\mathfrak{M}^*$  of  $I\Delta_0$ ;  
 (b)  $\mathfrak{M} \models I\Delta_0 + B\Sigma_1 + \text{Exp}$ .

**The proof of (a) $\Rightarrow$ (b) of Theorem A.** The proof is subdivided into the following three lemmas.

**LEMMA A.0.**  $I_{\text{fix}}(j) \models I\Delta_0$ .

*Proof.* We first verify that  $I_{\text{fix}}(j)$  is closed under the operations of the ambient structure  $\mathfrak{M}$ . Suppose  $x$  and  $y$  are elements of  $I_{\text{fix}}(j)$  with  $x \leq y$  and, without loss of generality, assume that  $x$  and  $y$  are both nonstandard elements. Since  $x+y < xy \leq y^2$ , it suffices to show that  $y^2 \in I_{\text{fix}}(j)$ . Observe that  $I\Delta_0$  can prove that any number  $z < y^2$  can be written as  $z = qy + r$ , where both  $q$  and  $r$  are less than  $y$  (since the division algorithm can be implemented in  $I\Delta_0$ , so  $q$  and  $r$  are respectively the quotient and remainder of the division of  $z$  by  $y$ ). Therefore,

$$j(z) = j(qy + r) = j(q)j(y) + j(r) = qy + r = z.$$

This shows that  $I_{\text{fix}}(j)$  is closed under the operations of  $\mathfrak{M}$ . Since  $I_{\text{fix}}(j)$  is end extended by  $\mathfrak{M}$  (by definition), and  $\Delta_0$ -predicates are absolute for end extensions, this shows that  $\mathfrak{M}$  inherits  $I\Delta_0$  from  $\mathfrak{N}$ . ■

**LEMMA A.1.**  $I_{\text{fix}}(j) \models B\Sigma_1$ .

*Proof.* This lemma immediately follows from Lemma 2.3 and A.0 since  $j$  is assumed to be a nontrivial automorphism, and therefore  $I_{\text{fix}}(j)$  must be a cut of  $\mathfrak{M}$  that is closed under multiplication. ■

LEMMA A.2.  $I_{\text{fix}}(j) \models \text{Exp}$ .

*Proof.* The proof has three stages.

STAGE 1. The argument establishing part (a) of Theorem 3.1 can be carried out in the present context, i.e.,

(1) If  $a \in I_{\text{fix}}(j)$  and  $2^a$  is defined in  $\mathfrak{M}$ , then  $2^a \in I_{\text{fix}}(j)$ .

To see this, we first observe that the usual proof of the existence of the base 2 expansion for a positive integer  $y$  can be implemented within  $I\Delta_0$  provided some power of 2 exceeds  $y$  (see [HP] or [Bu]). Therefore, for every  $y < 2^a$ , there is some element  $c$  that codes a subset of  $\{0, 1, \dots, a-1\}$  such that

$$y = \sum_{i \in c} 2^i.$$

The next observation is that  $j(c) = c$ . This hinges on the fact that  $E$  satisfies Extensionality, and that  $iEc$  implies  $j(i) = i$  (since  $a \in I_{\text{fix}}(j)$ , and  $iEc$  implies that  $i < a$ ). Therefore,

$$j(y) = j\left(\sum_{i \in c} 2^i\right) = \sum_{i \in j(c)} 2^i = \sum_{i \in c} 2^i = y.$$

So every  $y < 2^a$  is fixed by  $j$  and therefore  $2^a \in I_{\text{fix}}(j)$ .

STAGE 2. Let  $J := \{m \in M : 2^m \text{ is defined in } \mathfrak{M}\}$ . Note that  $J$  forms an initial segment of  $\mathfrak{M}$  by Lemma 2.1. We claim:

(2)  $\{2^m : m \in J\}$  is cofinal in  $M$ .

This is established by contradiction: if some  $c \in M$  is an upper bound of  $K$ , then  $K$  is the solution set of the  $\Delta_0$ -predicate  $\varphi(x, c)$ , where

$$\varphi(x, c) := [x < c \text{ and } \exists y < c \text{ Exp}(x, y)].$$

Therefore by  $I\Delta_0$ -MAX, there is a *last* power of 2 in  $\mathfrak{M}$ , which is absurd.

STAGE 3. We now use (1) and (2) to prove that if  $a \in I_{\text{fix}}(j)$ , then  $2^a$  is defined and is a member of  $I_{\text{fix}}(j)$ . In light of (1), it suffices to show that  $I_{\text{fix}}(j) \subsetneq J$ , where  $J$  is the cut defined in Stage 2. To see that  $I_{\text{fix}}(j) \subsetneq J$  assume to the contrary that  $J \subseteq I_{\text{fix}}(j)$ . It follows from (1) and (2) that  $I_{\text{fix}}(j) = M$ , which contradicts the assumption that  $j$  is a nontrivial automorphism. ■

REMARK 3.2. If  $I$  is a cut closed under exponentiation, then  $I$  is closed under addition and multiplication. To see this, note that  $I\Delta_0$  can prove that

if  $1 < x \leq y$ , then

$$x + y \leq xy \leq 2^{x+y} \leq 2^{2^y}.$$

This shows that Lemma A.0 follows from Lemma A.2.

**The proof of (b) $\Rightarrow$ (a) of Theorem A.** The initial step of the proof involves the construction of an appropriate ultrafilter, accomplished in Theorem 3.3 below.

- Throughout this section,  $\mathfrak{M}$  is a model of  $I\Delta_0 + B\Sigma_1$ ,  $I$  is a cut of  $\mathfrak{M}$  that satisfies Exp, and  $c \in M \setminus I$  such that  $2^c$  exists in  $\mathfrak{M}$  (such an element  $c$  exists by  $\Delta_0$ -OVERSPILL, see Remark 2.4.1).
- $\mathcal{F}$  and  $\mathcal{L}_{\mathcal{F}}$  are as in Theorem 2.5, and  $\mathcal{F}_c$  is the family of all  $M$ -valued functions  $f(x_1, \dots, x_n)$  on  $[\bar{c}]^n$  (where  $n \in \mathbb{N}^+$ ) obtained by restricting the domains of  $n$ -ary functions in  $\mathcal{F}$  to  $[\bar{c}]^n$ .
- Recall that  $\bar{c}$  is the set of predecessors of  $c$ . For a coded subset  $X$  of  $\bar{c}$ ,  $\mathcal{P}(X)$  is the power set of  $X$  in the sense of  $(M, E)$ .
- $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is a *filter* if  $\mathcal{U}$  is closed under intersections and is upward closed.
- A filter  $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is  *$I$ -complete* if for every  $f \in \mathcal{F}_c$  and  $i \in I$ , if  $f : \bar{c} \rightarrow \bar{i}$ , then there is some  $X \in \mathcal{U}$  such that  $f$  is constant on  $X$ . Note that if  $\mathcal{U}$  is  $I$ -complete, then  $\mathcal{U}$  is an ultrafilter on  $\mathcal{P}(\bar{c})$ , since for each  $Y \in \mathcal{P}(\bar{c})$  the characteristic function  $\chi_Y$  of  $Y$  is constant on some member of  $\mathcal{U}$ . We therefore refer to  $I$ -complete filters as *ultrafilters*.
- An ultrafilter  $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is *nonprincipal* if  $\mathcal{U}$  does not contain any singletons.
- A filter  $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is *Ramsey* if for every  $f \in \mathcal{F}_c$  and every  $n \in \mathbb{N}^+$ , if  $f : [\bar{c}]^n \rightarrow \{0, 1\}$ , then there is some  $f$ -monochromatic  $H \in \mathcal{U}$ .
- A filter  $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is *canonically Ramsey* if for every  $f \in \mathcal{F}_c$  there is some  $H \in \mathcal{U}$  such that  $H$  is  $f$ -canonical. It is easy to see that if  $\mathcal{U}$  is canonically Ramsey, then  $\mathcal{U}$  is Ramsey.
- A filter  $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is  *$I$ -tight* if for every  $f \in \mathcal{F}_c$  and every  $n \in \mathbb{N}^+$ , if  $f : [\bar{c}]^n \rightarrow M$ , then there is some  $H \in \mathcal{U}$  such either  $f$  is constant on  $H$ , or there is some  $m_0 \in M \setminus I$  such that  $f(\mathbf{x}) > m_0$  for all  $\mathbf{x} \in [H]^n$ .

**THEOREM 3.3.**  $\mathcal{P}(\bar{c})$  carries a nonprincipal ultrafilter  $\mathcal{U}$  with the following four properties:

- (a)  $\mathcal{U}$  is  $I$ -complete;
- (b)  $\mathcal{U}$  is canonically Ramsey;

(c)  $\mathcal{U}$  is  $I$ -tight;

(d)  $\{\text{Card}(X) : X \in \mathcal{U}\}$  is downward cofinal in  $M \setminus I$ .

- Let us say that  $X \in \mathcal{P}(\bar{c})$  is  $I$ -large if  $\text{Card}(X) \notin I$ . The proof of Theorem 3.3 is based on Lemmas 3.3.1 through 3.3.3 which reveal salient combinatorial features of  $I$ -large sets.

LEMMA 3.3.1. *If  $X$  is  $I$ -large, and  $f : \bar{c} \rightarrow \bar{m}$  for some nonzero  $m \in I$  with  $f \in \mathcal{F}_c$ , then there is some  $I$ -large subset of  $X$  on which  $f$  is constant.*

*Proof.* Let  $\lfloor x/y \rfloor = \max\{t \leq x : ty \leq x\}$ . First observe that, in light of Remark 3.2,  $I$  is closed under multiplication and therefore if  $b \notin I$  and  $m \in I$ , then  $\lfloor b/m \rfloor \notin I$ . Now suppose that for some  $b \in M \setminus I$ ,  $\text{Card}(X) = b$ , and let

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

Note that by Theorems 2.5 and 2.6(e) each  $S_i$  is coded in  $\mathfrak{M}$ . It is easy to see that there is some  $i$  for which  $\text{Card}(S_i) \geq \lfloor b/m \rfloor$ , since otherwise for all  $i \leq m$ ,

$$\text{Card}(S_i) < \lfloor b/m \rfloor - 1,$$

which, coupled with  $X = \bigcup_{i < m} S_i$ , implies the following contradiction:

$$b = \text{Card}(X) < m(\lfloor b/m \rfloor - 1) \leq b - m. \quad \blacksquare$$

LEMMA 3.3.2. *If  $f : [X]^n \rightarrow M$ , where  $X$  is  $I$ -large,  $f \in \mathcal{F}_c$ , and  $n \in \mathbb{N}^+$ , then there is an  $I$ -large subset of  $X$  that is  $f$ -canonical.*

*Proof.* Suppose  $i \in I$ . The closure of  $I$  under exponentiation implies that

$$\exists j \in I \ \mathfrak{M} \models j = \text{Superexp}(4n, i \cdot 2^{2^{2n-2n}}).$$

Therefore by part (b) of Theorem 2.7, if  $i \geq 4n^2$ , then  $i$  is a solution of the  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -predicate “there is an  $f$ -canonical subset of  $X$  cardinality  $i$ ” (this is a bounded statement since the monochromatic subset will be an element of  $\mathcal{P}(X)$ , and  $\mathcal{P}(X)$  is coded). By Theorem 2.5 and  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -OVERSPILL, therefore, there is an  $I$ -large subset of  $X$  that is  $f$ -canonical.  $\blacksquare$

LEMMA 3.3.3. *If  $X$  and  $f$  are as in Lemma 3.3.2, then there is an  $I$ -large  $Y \subseteq X$  such that either (a)  $f$  is constant on  $Y$ , or (b) there is some  $m_0 \in M \setminus I$  such that  $f(\mathbf{x}) > m_0$  for all  $\mathbf{x} \in [Y]^n$ .*

*Proof.* For  $m \in M$  define the function  $f_m : [X]^n \rightarrow \{0, 1\}$  in  $\mathfrak{M}$  by defining  $f_m(\mathbf{x}) = 0$  iff  $f(\mathbf{x}) \leq m$ . By Lemma 3.3.2, each  $f_m$  has an  $I$ -large monochromatic subset  $Y_m \subseteq X$ . We now consider two cases:

CASE I: For some  $i \in I$ ,  $f(Y_i) = \{0\}$ .

CASE II: For every  $i \in I$ ,  $f(Y_i) = \{1\}$ .

Suppose Case I holds, and  $f(Y_i) = \{0\}$  for some  $i \in I$ . Then by Lemma 3.3.1, there is an  $I$ -large subset of  $Y_i$  on which  $f$  is constant. Therefore (a)

is true if Case I holds. Case II, on the other hand, requires an overspill argument. Consider the following  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -formula  $\varphi(v)$ :

$$\varphi(v) := \exists Y \in \mathcal{P}(X) \ (\text{Card}(Y) > v \text{ and } f_v(\mathbf{x}) = 1 \text{ for all } \mathbf{x} \in [Y]^n).$$

If Case II holds then every element of  $I$  is a solution of  $\varphi(v)$  and therefore by  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -OVERSPILL there is some  $m_0 \in M \setminus I$  that is a solution of  $\varphi(v)$ , i.e., there is some  $Y \subseteq X$  such  $\text{Card}(Y) = m_0 \notin I$  and for all  $\mathbf{x} \in [Y]^n$ ,  $f(\mathbf{x}) > m_0$ . This shows that (b) is true if Case II holds. ■

We are now in a position to present:

*Proof of Theorem 3.3.* Let  $\langle f_n : n < \omega \rangle$  enumerate all maps in  $\mathcal{F}_c$  whose domain is  $\bar{c}$  and whose range is bounded in  $I$ ;  $\langle g_n : n < \omega \rangle$  enumerate all maps in  $\mathcal{F}_c$ , with  $g_n : [\bar{c}]^{k_n} \rightarrow M$  (note that for a fixed  $n$ ,  $k_n$  is also fixed); and fix a sequence  $\langle a_n : n \in \omega \rangle$  of elements of  $M$  which is downward cofinal in  $M \setminus I$  with  $a_0 \leq c$ . Using Lemmas 3.3.1 through 3.3.3, and truncation, we can inductively build four sequences  $\langle W_n : n < \omega \rangle$ ,  $\langle X_n : n < \omega \rangle$ ,  $\langle Y_n : n < \omega \rangle$ , and  $\langle Z_n : n < \omega \rangle$  of  $I$ -large elements of  $\mathcal{P}(\bar{c})$  such that for all  $n < \omega$ :

1.  $W_n \supseteq X_n \supseteq Y_n \supseteq Z_n \supseteq W_{n+1}$ ;
2.  $f_n$  is constant of  $W_n$ ;
3.  $X_n$  is  $g_n$ -canonical;
4.  $g_n$  is constant on  $Y_n$ , or there exists  $m_0 \in M \setminus I$  such that  $g_n(\mathbf{x}) > m_0$  for all  $\mathbf{x} \in [Y_n]^{k_n}$ ;
5.  $\text{Card}(Z_n) < a_n$ .

The desired ultrafilter  $\mathcal{U}$  is  $\{S \in \mathcal{P}(\bar{c}) : \exists n \in \omega (W_n \subseteq S)\}$ . ■

In the next step, we use the ultrafilter  $\mathcal{U}$  constructed in Theorem 3.3 to build a family of models  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$ , where  $\mathbb{L}$  is a prescribed linear order, such that  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  is an extension of  $\mathfrak{M}$  that satisfies  $I\Delta_0$  and possesses desirable automorphisms.

- Let  $\mathcal{U}$  be the ultrafilter produced in Theorem 3.3, and for each  $n \in \mathbb{N}^+$ , consider the family of (partial)  $n$ -types  $\Gamma_n(x_1, \dots, x_n)$  over  $\mathcal{L}_{\mathcal{F}}$  defined via:  $\varphi(x_1, \dots, x_n) \in \Gamma_n(x_1, \dots, x_n)$  iff there exists  $S \in \mathcal{U}$  such that  $\mathfrak{M}_{\mathcal{F}} \models \varphi(a_1, \dots, a_n)$  for all sequences  $a_1 < \dots < a_n$  from  $S$ .
- $T_{\mathcal{U}} = \bigcup_{n \in \mathbb{N}^+} \Gamma_n(x_1, \dots, x_n)$ .
- Given a linear order  $\mathbb{L}$ ,  $\mathcal{L}_{\mathcal{F}, \mathbb{L}}$  is the language obtained by augmenting  $\mathcal{L}_{\mathcal{F}}$  with constant symbols  $l$  for each  $l \in \mathbb{L}$ .
- The theory  $T_{\mathcal{U}, \mathbb{L}}$  is formulated within  $\mathcal{L}_{\mathcal{F}, \mathbb{L}}$  via

$$T_{\mathcal{U}, \mathbb{L}} := \{\varphi(l_1, \dots, l_n) : \varphi \in T_{\mathcal{U}} \text{ and } l_1 <_{\mathbb{L}} \dots <_{\mathbb{L}} l_n\}.$$

LEMMA 3.4.  $T_{\mathcal{U}, \mathbb{L}}$  is consistent and is  $\Delta_0(\mathcal{L}_{\mathcal{F}, \mathbb{L}})$ -complete.

*Proof.*  $T_{\mathcal{U}, \mathbb{L}}$  is consistent since it is finitely satisfiable in  $\mathfrak{M}$ . To verify  $\Delta_0(\mathcal{L}_{\mathcal{F}, \mathbb{L}})$ -completeness of  $T_{\mathcal{U}, \mathbb{L}}$ , suppose  $\varphi(x_1, \dots, x_n)$  is a  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -formula and consider

$$S := \{(x_1, \dots, x_n) \in (\bar{c})^n : \mathfrak{M}_{\mathcal{F}} \models \varphi(x_1, \dots, x_n)\}.$$

It is easy to see that the characteristic function  $\chi_S$  of  $S$  is a member of  $\mathcal{F}$ . Therefore, by the Ramsey property of  $\mathcal{U}$  there is some  $H \in \mathcal{U}$  on which  $\chi_S$  is constant. Hence either  $\varphi(x_1, \dots, x_n)$  or its negation is in  $\Gamma_n(x_1, \dots, x_n)$ . ■

- $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  is the model of arithmetic described by  $T_{\mathcal{U}, \mathbb{L}}$ , more specifically:
  - (a) The universe  $N_{\mathcal{U}, \mathbb{L}}$  of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  consists of the equivalence classes  $[\tau]$  of terms  $\tau$  of  $\mathcal{L}_{\mathcal{F}}$  of the form  $\tau = f(l_1, \dots, l_n)$ , where  $f \in \mathcal{F}$ ,  $(l_1, \dots, l_n) \in [\mathbb{L}]^n$ , and the equivalence relation  $\sim$  at work is defined via
 
$$f(l_1, \dots, l_r) \sim g(l'_1, \dots, l'_s) \Leftrightarrow (f(l_1, \dots, l_r) = g(l'_1, \dots, l'_s)) \in T_{\mathcal{U}, \mathbb{L}}.$$
  - (b) The operations and the ordering relation of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  are those naturally given by  $T_{\mathcal{U}, \mathbb{L}}$ , e.g.,

$$[f(l_1, \dots, l_r)] \oplus [g(l'_1, \dots, l'_s)] = [h(l''_1, \dots, l''_t)]$$

$$\Updownarrow$$

$$(f(l_1, \dots, l_r) + g(l'_1, \dots, l'_s) = h(l''_1, \dots, l''_t)) \in T_{\mathcal{U}, \mathbb{L}},$$

and

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

(it is routine to verify that the operations and relation of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  are well defined).

- There is an embedding  $e_1 : \mathfrak{M} \rightarrow \mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  given by

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

where  $l \in \mathbb{L}$ . Moreover, there is an embedding  $e_2 : \mathbb{L} \rightarrow (N_{\mathcal{U}, \mathbb{L}}, \triangleleft)$  via

$$l \mapsto_{e_2} [\text{id}(l)],$$

where  $\text{id} : M \rightarrow M$  is the identity function. In this light, we shall identify the element  $[c_m(l)]$  of  $N_{\mathcal{U}, \mathbb{L}}$  with  $m$ , and the element  $[\text{id}(l)]$  with  $l$ .

**LEMMA 3.5.** *Suppose  $\varphi(x_1, \dots, x_k)$  is a  $\Sigma_1$ -formula of  $\mathcal{L}_A$  with the indicated free variables, and  $[\tau_1], \dots, [\tau_k]$  are elements of  $N_{\mathcal{U}, \mathbb{L}}$ . The following two conditions are equivalent:*

- (a)  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}} \models \varphi([\tau_1], \dots, [\tau_k])$ ;
- (b)  $\varphi([\tau_1], \dots, [\tau_k]) \in T_{\mathcal{U}, \mathbb{L}}$ .

*Proof.* The proof of Lemma 3.5 is reminiscent of the proof of the fundamental theorem of ultraproducts and employs induction on the complexity

of formulas. When  $\varphi$  is atomic, the equivalence of (a) and (b) is trivially implied by the definition of the operations and the ordering relation on  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$ . The inductive argument establishing the equivalence of (a) and (b) also easily goes through when  $\varphi$  is of the form  $\theta_1 \wedge \theta_2$ . However, the negation and existential quantification steps merit a brief explanation. For the negation step, suppose  $\theta(x_1, \dots, x_k)$  is a  $\Delta_0$ -formula such that (a) and (b) are equivalent for any choice of  $k$  elements from  $N_{\mathcal{U}, \mathbb{L}}$  with  $\varphi = \theta$ . The equivalence of (a) and (b) for  $\varphi = \neg\theta$  can then be easily established by considering the  $\mathcal{L}_{\mathcal{F}, \mathbb{L}}$ -formula  $\theta(\tau_1, \dots, \tau_k)$ , and invoking Lemma 3.4 to get hold of some  $A \in \mathcal{U}$  such that either  $\theta(\tau_1, \dots, \tau_k)$  or its negation is in  $T_{\mathcal{U}, \mathbb{L}}$ . For the existential quantification step, the inductive proof of (a) $\Rightarrow$ (b) is easy to establish, but the proof of (b) $\Rightarrow$ (a) is more delicate and requires the following claim regarding the existence of  $\Delta_0$ -Skolem functions in  $\mathcal{F}$ .

**CLAIM  $\clubsuit$ .** *If for some  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -formula  $\psi(x_1, \dots, x_n, y)$ ,*

$$(i) \mathfrak{M}_{\mathcal{F}} \models \forall x_1 \cdots \forall x_n ((x_1 < \cdots < x_n < c) \rightarrow \exists y \psi(x_1, \dots, x_n, y)),$$

*then there exists  $g(x_1, \dots, x_n) \in \mathcal{F}$  such that:*

$$(ii) \mathfrak{M}_{\mathcal{F}} \models \forall x_1 \cdots \forall x_n ((x_1 < \cdots < x_n < c) \rightarrow \psi(x_1, \dots, x_n, g(x_1, \dots, x_n))).$$

To verify Claim  $\clubsuit$ , assume (i) and let  $\delta(x_1, \dots, x_n, y)$  abbreviate the following  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -formula:

$$\psi(x_1, \dots, x_n, y) \wedge \forall z < y \neg\psi(x_1, \dots, x_n, z).$$

By  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -MIN and  $B\Sigma_1(\mathcal{L}_{\mathcal{F}})$ , there is some  $b \in M$  such that

$$\mathfrak{M}_{\mathcal{F}} \models \forall x_1 \cdots \forall x_n ((x_1 < \cdots < x_n < c) \rightarrow \exists! y < b \delta(x_1, \dots, x_n, y)).$$

Let  $g$  be the function on  $M^n$  whose graph is defined by  $g(a_1, \dots, a_n) = a_{n+1}$  iff

$$\begin{aligned} \mathfrak{M}_{\mathcal{F}} \models & ((a_1 < \cdots < a_n < c) \wedge \delta(a_1, \dots, a_n, a_{n+1})) \\ & \vee (\neg(a_1 < \cdots < a_n < c) \wedge (a_{n+1} = 0)). \end{aligned}$$

It is easy to see that  $g \in \mathcal{F}$  and  $g$  satisfies (ii). This concludes the verification of Claim  $\clubsuit$ .

Going back to the existential quantification step of the proof of Lemma 3.5, suppose that for some formula  $\exists y \theta(x_1, \dots, x_k, y)$ , where  $\theta$  is a  $\Delta_0$ -formula, the equivalence of (a) and (b) holds for  $\varphi = \theta(x_1, \dots, x_k, y)$  for any choice of  $k+1$  elements from  $N_{\mathcal{U}, \mathbb{L}}$ . To verify that (b) $\Rightarrow$ (a), suppose (b) holds for  $\varphi = \exists y \theta$  for some choice  $[\tau_1], \dots, [\tau_k]$  of elements from  $N_{\mathcal{U}, \mathbb{L}}$ . To simplify notation, we shall assume that for some choice of  $(l_1, \dots, l_n) \in [\mathbb{L}]^n$ , each  $\tau_i$  can be written as  $f_i(l_1, \dots, l_n)$ . The definition of  $T_{\mathcal{U}, \mathbb{L}}$  shows that there is some  $A \in \mathcal{U}$  such that for all  $(a_1, \dots, a_n) \in [A]^n$ ,

$$\mathfrak{M} \models \exists y \theta(f_1(a_1, \dots, a_n), \dots, f_k(a_1, \dots, a_n), y).$$

Let  $d \in M$  be an element coding  $A$ ,  $\alpha(x_1, \dots, x_n)$  be the formula

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

and  $\psi(x_1, \dots, x_n, y)$  be the conjunction of the formula

$$\alpha(x_1, \dots, x_n) \rightarrow \theta(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n), y)$$

with the formula

$$(\neg \alpha(x_1, \dots, x_n)) \rightarrow y = 0.$$

Note that  $\psi(x_1, \dots, x_n, y)$  is a  $\Delta_0(\mathcal{L}_{\mathcal{F}})$ -formula since  $E$  has a  $\Delta_0$ -definition and we have access to a name for  $d$  in  $\mathcal{L}_{\mathcal{F}}$  (see Remark 2.5.1). By Claim  $\clubsuit$ , there is some  $g(x_1, \dots, x_n) \in \mathcal{F}$  such that for every  $(a_1, \dots, a_n) \in [A]^n$ ,

$$\mathfrak{M}_{\mathcal{F}} \models \psi(a_1, \dots, a_n, g(a_1, \dots, a_n)).$$

Coupled with the inductive hypothesis, this shows the following, thus concluding the proof of (b) $\Rightarrow$ (a) of the existential quantification step:

$$\mathfrak{N}_{\mathcal{U}, \mathbb{L}} \models \theta([\tau_1], \dots, [\tau_k], [g(l_1, \dots, l_n)]). \quad \blacksquare$$

LEMMA 3.6.

- (a)  $\mathfrak{M}$  is cofinal in  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$ ;
- (b)  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  satisfies  $I\Delta_0$ ;
- (c)  $\mathbb{L}$  is a set of  $\Sigma_1$ -indiscernibles in  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$ ;
- (d)  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  end extends  $I$ ;
- (e)  $M \setminus I$  is downward cofinal in  $N_{\mathcal{U}, \mathbb{L}} \setminus I$ .

*Proof.* (a) is a consequence of  $\mathfrak{M} \models B\Sigma_1$ , and Lemma 3.5 immediately implies (b) and (c). The  $I$ -completeness of  $\mathcal{U}$ , coupled with Lemma 3.5, yields (d). To verify (e), suppose

$$[f(l_1, \dots, l_n)] \in N_{\mathcal{U}, \mathbb{L}} \setminus I.$$

Since  $\mathcal{U}$  is  $I$ -tight, there is some  $H \in \mathcal{U}$  such either  $f$  is constant on  $H$  or there is some  $m_0 \in M \setminus I$  such that  $f(\mathbf{x}) > m_0$  for all  $\mathbf{x} \in [H]^n$ . Therefore, by Lemma 3.5 there is some  $m_0 \in M \setminus I$  such that  $m_0 \leq [f(l_1, \dots, l_n)]$ .  $\blacksquare$

- In what follows,  $\text{fix}(\widehat{j})$  is the fixed point set of  $\widehat{j}$ .

LEMMA 3.7. *Every automorphism  $j$  of  $\mathbb{L}$  induces an automorphism  $\widehat{j}$  of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  such that  $j \mapsto \widehat{j}$  is a group embedding of  $\text{Aut}(\mathbb{L})$  into  $\text{Aut}(\mathfrak{N}_{\mathcal{U}, \mathbb{L}})$ . Moreover,*

- (a)  $I_{\text{fix}(\widehat{j})} = I$  for every nontrivial  $j \in \text{Aut}(\mathbb{L})$ ;
- (b)  $\text{fix}(\widehat{j}) = M$  for every fixed point free  $j \in \text{Aut}(\mathbb{L})$ .

*Proof.* The fact that an automorphism  $j$  of  $\mathbb{L}$  induces an automorphism  $\widehat{j}$  of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  follows from the same line of reasoning used in the classical argument of Ehrenfeucht and Mostowski and is based on the fact that  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$

is generated by a copy of  $\mathbb{L}$  via the functions in  $\mathcal{F}$ . In other words, since each element of  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  can be represented as  $[f(l_1, \dots, l_n)]$  for an appropriate choice of  $f \in \mathcal{F}$  and  $l_1, \dots, l_n$  of  $\mathbb{L}$ , the desired  $\widehat{j}$  can be defined via

$$(*) \quad \widehat{j}([f(l_1, \dots, l_n)]) = [f(j(l_1), \dots, j(l_n))].$$

It is easy to see, using  $(*)$  above, that the correspondence  $j \mapsto \widehat{j}$  indeed defines a group embedding of the automorphism group  $\text{Aut}(\mathbb{L})$  of  $\mathbb{L}$  into the automorphism group  $\text{Aut}(\mathfrak{N}_{\mathcal{U},\mathbb{L}})$  of  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$ .

We now verify that for a nontrivial automorphism  $j$  of  $\mathbb{L}$ ,  $\widehat{j}$  fixes members of  $I$ , but moves elements arbitrarily close to  $I$ . First note that if  $j \in \text{Aut}(\mathbb{L})$ , then  $\widehat{j}$  fixes each element of  $M$  (since each element of  $M$  is represented by a constant function of  $\mathcal{F}$ ). This shows, *a fortiori*, that  $\widehat{j}$  fixes members of  $I$ . Recall from Theorem 3.3 that there is a sequence  $\langle a_n : n \in \omega \rangle$  of elements of  $M \setminus I$  that is downward cofinal in  $M \setminus I$ , and a sequence  $\langle Z_n : n \in \omega \rangle$  of elements of  $\mathcal{U}$  such that  $\text{Card}(Z_n) < a_n$ . Consider the sequence  $\langle \tau_n(x) : n \in \omega \rangle$  of terms of  $\mathcal{L}_{\mathcal{F}}$  defined by:

$$\tau_n(x) := y \text{ iff } x \text{ is the } y\text{th element of } Z_n \text{ under its natural ordering.}$$

Note that  $\tau_n(x) < a_n$ . Now, if  $j \in \text{Aut}(\mathbb{L})$  with  $j(k) = l \neq k$ , then

$$\widehat{j}(\tau_n(k)) = \tau_n(l).$$

By the definition of  $T_{\mathcal{U},\mathbb{L}}$ ,  $k$  and  $l$  are (distinct) members of  $X_n$ . But since  $\tau_n(x)$  defines a one-to-one map,  $\widehat{j}$  moves an element below  $a_n$ , namely  $\tau_n(\overline{k})$ . In light of the fact that the  $a_n$ 's were chosen to be downward cofinal in  $M \setminus I$ , and  $M \setminus I$  is downward cofinal in  $N_{\mathcal{U},\mathbb{L}} \setminus I$  (by Lemma 3.6(e)), this shows that  $I_{\text{fix}(\widehat{j})} = I$ .

We now verify (b). We already know that  $M \subseteq \text{fix}(\widehat{j})$  for every  $j \in \text{Aut}(\mathbb{L})$ . To see that  $\text{fix}(\widehat{j}) \subseteq M$  for a fixed point free  $j$ , suppose that for some element  $[f(l_1, \dots, l_n)]$  of  $N_{\mathcal{U},\mathbb{L}}$ ,

$$(1) \quad [f(j(l_1), \dots, j(l_n))] = [f(l_1, \dots, l_n)].$$

Since  $f \in \mathcal{F}$  and  $\mathcal{U}$  is  $\mathcal{F}$ -canonically Ramsey, there is some  $H \in \mathcal{U}$  and some  $S \subseteq \{1, \dots, n\}$  such that for all sequences  $x_1 < \dots < x_n$  and  $y_1 < \dots < y_n$  of elements of  $H$ ,

$$(2) \quad f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \Leftrightarrow \forall i \in S (x_i = y_i).$$

Therefore, by Lemma 3.5,

$$(3) \quad \text{for all } l_1 < \dots < l_n \text{ and } k_1 < \dots < k_n \text{ from } \mathbb{L},$$

$$[f(l_1, \dots, l_n)] = [f(k_1, \dots, k_n)] \Leftrightarrow \forall i \in S (l_i = k_i).$$

Coupled with (1), (3) shows that  $S = \emptyset$ . So  $f$  must be *constant* on  $H$ , thereby showing that  $[f(l_1, \dots, l_n)] \in M$ , as desired. ■

Putting Lemmas 3.4 through 3.7 together, we obtain the following general result.

**THEOREM 3.8.** *Suppose  $\mathbb{L}$  is a linearly ordered set, and  $\mathcal{U}$  has properties (a), (b), (c) and (d) of Theorem 3.3. The model  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  has the following properties:*

- (a)  $\mathfrak{M} \subseteq \mathfrak{N}_{\mathcal{U},\mathbb{L}}$  and  $I \subseteq_e \mathfrak{N}_{\mathcal{U},\mathbb{L}}$ ;
- (b) for a  $\Sigma_1$ -formula  $\varphi(x_1, \dots, x_n)$ , and  $(l_1, \dots, l_n) \in [\mathbb{L}]^n$ ,  $\mathfrak{N}_{\mathcal{U},\mathbb{L}} \models \varphi(l_1, \dots, l_n)$  iff
 
$$\exists S \in \mathcal{U} \forall (a_1, \dots, a_n) \in [S]^n \mathfrak{M} \models \varphi(a_1, \dots, a_n);$$
- (c)  $\mathbb{L}$  is a set of  $\Sigma_1$ -indiscernibles in  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$ ;
- (d) every  $j \in \text{Aut}(\mathbb{L})$  induces an automorphism  $\hat{j} \in \text{Aut}(\mathfrak{N}_{\mathcal{U},\mathbb{L}})$  such that  $j \mapsto \hat{j}$  is a group embedding of  $\text{Aut}(\mathbb{L})$  into  $\text{Aut}(\mathfrak{N}_{\mathcal{U},\mathbb{L}})$ ;
- (e) if  $j \in \text{Aut}(\mathbb{L})$  is nontrivial, then  $I_{\text{fix}}(\hat{j}) = I$ ;
- (f) if  $j \in \text{Aut}(\mathbb{L})$  is fixed point free, then  $\text{fix}(\hat{j}) = M$ .

**REMARK 3.8.1.** If  $\mathfrak{M}$  is a model of full PA, then the restrictions to  $\Sigma_1$ -formulas in Lemma 3.5, and to  $\Delta_0$ -formulas in Lemma 3.6 can both be eliminated. This in turn allows the restriction to the corresponding restrictions to be eliminated from Theorem 3.8.

We are now in a position to complete the proof of Theorem A.

*Proof of (b) $\Rightarrow$ (a) of Theorem A.* Suppose  $\mathfrak{M}_0$  is a countable model of  $I\Delta_0 + B\Sigma_1 + \text{Exp}$ . By Theorem 2.4,  $\mathfrak{M}_0$  can be end extended to a model  $\mathfrak{M}$  that satisfies  $I\Delta_0$ . This allows us to invoke Theorem 3.3 (with  $I := M_0$ ) to produce an ultrafilter  $\mathcal{U}$  satisfying conditions (1) through (3) of Theorem 3.3. By Theorem 3.8, the ultrafilter  $\mathcal{U}$  can be used to give rise to the model  $\mathfrak{N}_{\mathcal{U},\mathbb{Z}}$ , where  $\mathbb{Z}$  is the ordered set of integers (note that  $\mathfrak{N}_{\mathcal{U},\mathbb{Z}}$  satisfies  $I\Delta_0$  and  $\mathfrak{M}_0 \subseteq_e \mathfrak{N}_{\mathcal{U},\mathbb{Z}}$ ). Let  $j$  be any nontrivial automorphism of  $\mathbb{Z}$ , e.g.,  $j(n) = n + 1$ . By Theorem 3.8(e),  $\hat{j}$  is an automorphism of  $\mathfrak{N}_{\mathcal{U},\mathbb{Z}}$  with  $I_{\text{fix}}(\hat{j}) = M$ , as desired. ■

Theorem A, combined with the downward Löwenheim–Skolem theorem, yields:

**COROLLARY 3.9.**  *$I\Delta_0 + B\Sigma_1 + \text{Exp}$  is the theory of the class of models whose universes are of the form  $I_{\text{fix}}(j)$  for some nontrivial automorphism  $j$  of a model of  $I\Delta_0$ , i.e., the following are equivalent for sentences  $\varphi$  in  $\mathcal{L}_A$ :*

- (a)  $I\Delta_0 + B\Sigma_1 + \text{Exp} \vdash \varphi$ ;
- (b)  $\varphi$  holds in every model of the form  $I_{\text{fix}}(j)$ , where  $j$  is a nontrivial automorphism of some model of  $I\Delta_0$ .

**REMARK 3.10.** By a theorem of Solovay [Pari, Theorem 4] every countable recursively saturated model  $\mathfrak{M}$  of  $I\Delta_0 + B\Sigma_1$  is isomorphic to a proper

initial segment of itself, and therefore  $\mathfrak{M}$  has an end extension that satisfies  $I\Delta_0$ . This result can be substituted for the Wilkie–Paris theorem (Theorem 2.4) in the proof of Corollary 3.9 since every consistent countable theory has a countable recursively saturated model.

#### 4. SMORYŃSKI'S THEOREM, REVISITED

Smoryński's theorem (part (b) of Theorem 3.1) was established in [Sm] by an elaborate back-and-forth argument (see also [Ka-4]). We now explain how to derive an extension of this result with an entirely different proof, using our work in the previous section. This new proof can be summarized as follows:

(1) If  $\mathfrak{M}$  is a model of PA, then as pointed out in Remark 3.8.1 the model  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  of Theorem 3.8 turns out to be a cofinal *elementary extension* of  $\mathfrak{M}$ . Indeed, this is precisely what is accomplished by Paris and Mills in [PM, Theorem 6].

(2) By an appropriate choice of ultrafilter  $\mathcal{U}$ ,  $\mathfrak{M}$  and  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  can be arranged to have the same  $I$ -standard system.

(3) If  $\mathfrak{M}$  and  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  have the same  $I$ -standard system,  $\mathfrak{M}$  is recursively saturated, and  $\mathbb{L}$  is countable, then  $\mathfrak{M}$  can be shown to be isomorphic to  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  via an isomorphism that is the identity on  $I$ . Smoryński's theorem now follows from Theorem 3.8 by representing  $\mathfrak{M}$  as  $\mathfrak{N}_{\mathcal{U},\mathbb{Q}}$ , where  $\mathbb{Q}$  is the ordered set of rationals (recall:  $|\text{Aut}(\mathbb{Q})| = 2^{\aleph_0}$ ).

- To set the stage, suppose  $\mathfrak{M} \models I\Delta_0$ ,  $I$  is a cut of  $\mathfrak{M}$  closed under exponentiation, and  $c \in M \setminus I$  such that for each  $n \in \mathbb{N}$ ,  $2^{(c^n)}$  exists. This will ensure that for each  $n \in \mathbb{N}^+$ , there is an element in  $\mathfrak{M}$  that codes all subsets of the Cartesian product  $(\bar{c})^n$  that are coded in  $\mathfrak{M}$  (in other words:  $\mathcal{P}(c^n)$  exists in  $\mathfrak{M}$ ). Thanks to  $\Delta_0$ -OVERSPILL, this is easy to arrange since every member of  $I$  is a solution of the  $\Delta_0$ -predicate  $\varphi(x) := "2^{2^x}$  exists" and therefore there is  $c \in M \setminus I$  for which  $2^{(2^c)}$  exists in  $\mathfrak{M}$  (recall that for nonstandard  $c$  and  $n \in \mathbb{N}^+$ ,  $c^n < 2^c$ ).
- A subset  $X$  of  $\bar{c}$  *decides* a subset  $K$  of  $[\bar{c}]^n$  (where  $n \in \mathbb{N}^+$ ) if either  $[X]^n \subseteq K$  or  $[X]^n \subseteq [\bar{c}]^n \setminus K$ .
- A filter  $\mathcal{U} \subseteq \mathcal{P}(\bar{c})$  is  *$I$ -conservative* if for every  $n \in \mathbb{N}^+$  and every  $\mathfrak{M}$ -coded sequence  $\langle K_i : i < c \rangle$  of subsets of  $[\bar{c}]^n$  there is some  $X \in \mathcal{U}$  and some  $d \in M$  with  $I < d \leq c$  such that  $X$  decides  $K_i$  for all  $i < d$ .

The following result explains the importance of  $I$ -conservative ultrafilters. In what follows,  $\mathfrak{M}$ ,  $\mathcal{U}$ , and  $\mathfrak{N}_{\mathcal{U},\mathbb{L}}$  are as in the previous section.

LEMMA 4.1. *If  $\mathcal{U}$  is  $I$ -conservative, then  $\text{SSy}_I(\mathfrak{N}_{\mathcal{U},\mathbb{L}}) = \text{SSy}_I(\mathfrak{M})$ .*

*Proof.* Since  $I \subseteq_e \mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  and  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  extends  $\mathfrak{M}$ ,  $\text{SSy}_I(\mathfrak{N}_{\mathcal{U}, \mathbb{L}}) \supseteq \text{SSy}_I(\mathfrak{M})$ . To see that  $\text{SSy}_I(\mathfrak{N}_{\mathcal{U}, \mathbb{L}}) \subseteq \text{SSy}_I(\mathfrak{M})$ , suppose  $[f(l_1, \dots, l_n)]$  is a member of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$ , and define  $A_{f(l_1, \dots, l_n)}$  via

$$A_{f(l_1, \dots, l_n)} := \{i \in I : \mathfrak{N}_{\mathcal{U}, \mathbb{L}} \models i E [f(l_1, \dots, l_n)]\}.$$

We wish to show

$$(1) A_{f(l_1, \dots, l_n)} \in \text{SSy}_I(\mathfrak{M}).$$

Consider the  $\mathfrak{M}$ -coded sequence  $\langle K_i : i < c \rangle$  defined by

$$K_i := \{(a_1, \dots, a_n) \in [\bar{c}]^n : \mathfrak{M}_{\mathcal{F}} \models i E f(a_1, \dots, a_n)\}.$$

Note that by Lemma 3.5,

$$(2) A_{f(l_1, \dots, l_n)} = \{i \in I : \exists X \in \mathcal{U} ([X]^n \subseteq K_i)\}.$$

Invoking the  $I$ -conservativity of  $\mathcal{U}$ , for some  $X_0 \in \mathcal{U}$  and  $d \in M$  with  $I < d \leq c$ ,  $X_0$  decides  $K_i$  for all  $i < d$ .

Therefore  $A_{f(l_1, \dots, l_n)} = \{i \in I : [X_0]^n \subseteq K_i\}$ , which makes it evident that (1) holds and the proof is complete. ■

In order to show that the ultrafilter  $\mathcal{U}$  employed in the construction of  $\mathfrak{N}_{\mathcal{U}, \mathbb{L}}$  can be arranged to be  $I$ -conservative we need to establish another combinatorial property of  $I$ -large sets in the next lemma.

LEMMA 4.2. *Suppose  $S$  is  $I$ -large and  $\langle K_i : i < c \rangle$  is an  $\mathfrak{M}$ -coded sequence of subsets of  $[S]^n$  for some fixed  $n \in \mathbb{N}^+$ . Then there is some  $d$  with  $I < d \leq c$ , and some  $I$ -large subset  $S'$  of  $S$  such that  $S'$  decides  $K_i$  for all  $i < d$ .*

*Proof.* Given any  $i < c$  consider the map

$$F_i : [S]^n \rightarrow \{0, 1\}^i$$

defined by: for  $1 \leq j \leq i$ , the  $j$ th coordinate of  $F_i(\mathbf{x})$  is 1 iff  $\mathbf{x} \in K_j$  (where  $\mathbf{x} \in [S]^n$ ). Since  $I$  is closed under exponentiation, and  $\text{Card}(\{0, 1\}^i) = 2^i$ ,  $F_i$  can be viewed as  $F_i : [S]^n \rightarrow \bar{k}$  for  $k := 2^i \in I$ . Therefore, by Theorem 2.7(a), for every  $i \in I$ , the following  $\Delta_0$ -formula holds in  $\mathfrak{M}$ :

$$(1) \text{ there is some } F_i\text{-monochromatic } X \subseteq S \text{ such that } \text{Card}(X) > i.$$

It is easy to see that (1) implies that for each  $i \in I$ , the following  $\Delta_0$ -formula holds in  $\mathfrak{M}$ :

$$(2) \text{ there exists } X \subseteq S \text{ such that for all } j \leq i, X \text{ is } \chi_{K_j}\text{-monochromatic and } \text{Card}(X) > i \text{ (here } \chi_{K_j} \text{ is the characteristic function of } K_j).$$

By coupling  $\Delta_0$ -OVERSPILL and (2), we obtain

$$(3) \text{ for some } d > I, \text{ there exists } S' \subseteq S \text{ such that for all } j \leq d, S' \text{ is } \chi_{K_j}\text{-monochromatic and } \text{Card}(X_0) > d.$$

It is now easy to see that the  $S'$  of (3) will serve as the desired  $I$ -large subset of  $S$ . ■

**THEOREM 4.3.** *Theorem 3.3 can be strengthened by requiring that the ultrafilter  $\mathcal{U}$  be additionally  $I$ -conservative.*

*Proof.* Enumerate all  $\mathfrak{M}$ -coded sequences of length  $c$  of subsets of finite Cartesian powers of  $\bar{c}$  as  $\langle h_n : n < \omega \rangle$ . More specifically, each  $h_n$  codes a sequence of the form  $\langle S_i : i < c \rangle$ , where every  $S_i$  is a subset of  $[\bar{c}]^{m_n}$  and  $m_n \in \mathbb{N}^+$  only depends on  $n$ . Thanks to Lemma 4.2, we can now modify the proof of Theorem 3.3 by inductively constructing *five* sequences  $\langle V_n : n < \omega \rangle$ ,  $\langle W_n : n < \omega \rangle$ ,  $\langle X_n : n < \omega \rangle$ ,  $\langle Y_n : n < \omega \rangle$  and  $\langle Z_n : n < \omega \rangle$  of  $I$ -large elements of  $\mathcal{P}(\bar{c})$  such that for all  $n < \omega$ :

1.  $V_n \supseteq W_n \supseteq X_n \supseteq Y_n \supseteq Z_n \supseteq V_{n+1}$ ;
2.  $V_n$  decides every member of the sequence coded by  $h_n$ ;
3.  $f_n$  is constant on  $W_n$ ;
4.  $X_n$  is  $g_n$ -canonical;
5.  $g_n$  is constant on  $Y_n$ , or there exists  $m_0 \in M \setminus I$  such that  $g_n(\mathbf{x}) > m_0$  for all  $\mathbf{x} \in [Y_n]^{k_n}$ ;
6.  $\text{Card}(Z_n) \leq a_n$ .

The desired ultrafilter  $\mathcal{U}$  is  $\{S \in \mathcal{P}(\bar{c}) : \exists n \in \omega (V_n \subseteq S)\}$ . ■

Suppose  $\mathfrak{M}$  and  $\mathfrak{M}^*$  are two models of bounded arithmetic that share a cut  $I$  closed under exponentiation. It is clear that if there is an isomorphism between  $\mathfrak{M}$  and  $\mathfrak{M}^*$  that is the identity on  $I$ , then  $\text{Th}(\mathfrak{M}, i)_{i \in I} = \text{Th}(\mathfrak{M}^*, i)_{i \in I}$ , and  $\text{SSy}_I(\mathfrak{M}) = \text{SSy}_I(\mathfrak{M}^*)$ . As shown by the next lemma, this result has a converse if  $\mathfrak{M}^*$  is a *cofinal* elementary extension of  $\mathfrak{M}$ , and  $\mathfrak{M}$  is a countable recursively saturated model of PA.

**LEMMA 4.4.** *Suppose  $I$  is a cut closed under exponentiation in a countable recursively saturated model  $\mathfrak{M}$  of PA, and  $\mathfrak{M}^*$  is a cofinal countable elementary extension of  $\mathfrak{M}$  such that  $I \subseteq_e \mathfrak{M}^*$  with  $\text{SSy}_I(\mathfrak{M}) = \text{SSy}_I(\mathfrak{M}^*)$ . Then  $\mathfrak{M}$  and  $\mathfrak{M}^*$  are isomorphic over  $I$ , i.e., there is an isomorphism between  $\mathfrak{M}$  and  $\mathfrak{M}^*$  that is the identity on  $I$ .*

*Proof.* The desired isomorphism can be constructed via a routine back-and-forth argument, once we establish the following central claim:

**CLAIM.** *Suppose  $n \in \mathbb{N}$  and  $(\mathfrak{M}, a_1, \dots, a_n, i)_{i \in I} \equiv (\mathfrak{M}^*, b_1, \dots, b_n, i)_{i \in I}$ .*

(a) *For every  $c \in M$  there is  $d \in M^*$  such that*

$$(\mathfrak{M}, a_1, \dots, a_n, c, i)_{i \in I} \equiv (\mathfrak{M}^*, b_1, \dots, b_n, d, i)_{i \in I}.$$

(b) *For every  $d \in M^*$  there is  $c \in M$  such that*

$$(\mathfrak{M}, a_1, \dots, a_n, c, i)_{i \in I} \equiv (\mathfrak{M}^*, b_1, \dots, b_n, d, i)_{i \in I}.$$

We shall prove part (b) of the claim only. The proof of (a) is left as an exercise for the reader (it is similar and does not need the assumption  $\text{SSy}_I(\mathfrak{M}) = \text{SSy}_I(\mathfrak{M}^*)$ ). It is well known that the isomorphism type of a countable recursively saturated model  $\mathfrak{M}$  of arithmetic is uniquely determined by  $\text{Th}(\mathfrak{M})$  and  $\text{SSy}_{\mathbb{N}}(\mathfrak{M})$ . We may therefore assume, without loss of generality, that  $I$  is longer than  $\mathbb{N}$ . By Theorem 2.8 there is a satisfaction class  $S$  on  $\mathfrak{M}$  that is  $s$ -correct for some nonstandard  $s$ . Since  $I \neq \mathbb{N}$ , by shortening  $S$  and  $s$  if necessary, we can also safely assume that

$$(1) \quad s \in I \text{ and } \langle \lceil \varphi \rceil, a \rangle \in S \Rightarrow \lceil \varphi \rceil < s.$$

Theorem 2.9 implies that there is some  $s$ -correct satisfaction class  $S^*$  on  $\mathfrak{M}^*$  such that  $(\mathfrak{M}, S) \prec (\mathfrak{M}^*, S^*)$  and (1) holds with  $S$  replaced by  $S^*$ .

Suppose that  $\mathbf{a} := (a_1, \dots, a_n)$ ,  $\mathbf{b} := (b_1, \dots, b_n)$ , and

$$(2) \quad (\mathfrak{M}, \mathbf{a}, i)_{i \in I} \equiv (\mathfrak{M}^*, \mathbf{b}, i)_{i \in I}.$$

Given  $d \in M^*$  we wish to find some  $c \in M$  such that

$$(\mathfrak{M}, \mathbf{a}, c, i)_{i \in I} \equiv (\mathfrak{M}^*, \mathbf{b}, d, i)_{i \in I}.$$

To do so, first consider  $Y \subseteq I$  defined as follows:

$$Y := \{ \langle i, \lceil \varphi(x, \mathbf{y}, z) \rceil \rangle : i \in I \text{ and } \langle \lceil \varphi(x, \mathbf{y}, z) \rceil, \langle i, \mathbf{b}, d \rangle \rangle \in S^* \}.$$

Recall that, intuitively speaking,  $\langle \lceil \varphi(x, \mathbf{y}, z) \rceil, \langle i, \mathbf{b}, d \rangle \rangle \in S^*$  if the potentially nonstandard formula  $\varphi(i, \mathbf{b}, d)$  is true in the sense of  $S^*$ . It is easy to see, using the fact that  $(\mathfrak{M}^*, S^*)$  satisfies  $\text{PA}(S^*)$ , that  $Y \in \text{SSy}_I(\mathfrak{M}^*)$ . Furthermore, for any  $i \in I$  and any standard formula  $\varphi(x, \mathbf{y}, z)$  with  $\mathbf{y} := (y_1, \dots, y_n)$ ,

$$\mathfrak{M}^* \models \varphi(i, \mathbf{b}, d) \Leftrightarrow \langle i, \lceil \varphi(x, \mathbf{y}, z) \rceil \rangle \in Y.$$

For each  $i \in I$ , let

$$Y_i := \{ \langle j, \lceil \varphi \rceil \rangle \in Y : j < i \}.$$

The assumption that  $I$  is closed under exponentiation together with (1) implies that for each  $i \in I$  there is some  $m_i \in I$  such that

$$Y_i = (m_i)_E.$$

Clearly

$$(3) \quad \text{if } \lceil \varphi \rceil < s \text{ and } i \in I, \text{ then } (\mathfrak{M}^*, \mathbf{b}, d) \text{ satisfies:}$$

$$\forall j < i \quad (\langle \lceil \varphi(x, \mathbf{y}, z) \rceil, \langle j, \mathbf{b}, d \rangle \rangle \in S^* \leftrightarrow \langle j, \lceil \varphi(x, \mathbf{y}, z) \rceil \rangle \in Em_i).$$

Therefore

$$(4) \quad \text{if } \lceil \varphi \rceil < s \text{ and } i \in I, \text{ then } (\mathfrak{M}^*, \mathbf{b}) \text{ satisfies:}$$

$$\exists z_0 \forall j < i \quad (\langle \lceil \varphi(x, \mathbf{y}, z) \rceil, \langle j, \mathbf{b}, z_0 \rangle \rangle \in S^* \leftrightarrow \langle j, \lceil \varphi(x, \mathbf{y}, z) \rceil \rangle \in Em_i).$$

Let  $f : I \rightarrow I$  be defined by  $f(i) = m_i$ . The fact that  $(\mathfrak{M}^*, S^*) \models \text{PA}(S^*)$  makes it evident that for some  $\bar{f} \in M$ ,  $\bar{f} \upharpoonright I = f$ . Since  $f$  can be canonically coded as a subset of  $I$  and  $\text{SSy}_I(\mathfrak{M}^*) = \text{SSy}_I(\mathfrak{M})$ , this shows that there is some  $\tilde{f} \in M^*$  such that

$$(5) \quad \forall i \in I \quad \tilde{f}(i) = \bar{f}(i) = m_i.$$

Thanks to (2), (4), and (5),

$$(6) \quad \forall i \in I \quad (\mathfrak{M}, \mathbf{a}, \bar{f}, S) \models \theta(i), \text{ where } \theta(i) \text{ denotes the formula}$$

$$\exists z_0 \forall j < i \langle [\varphi(x, \mathbf{y}, z)], \langle j, \mathbf{a}, z_0 \rangle \rangle \in S \leftrightarrow \forall j < i \langle \langle j, [\varphi(x, \mathbf{y}, z)] \rangle E\bar{f}(i) \rangle.$$

So by overspill applied to  $\theta(i)$ , for some  $k \in M^* \setminus I$ , there is some  $c \in M^*$  such that

$$(7) \quad \text{for all standard } \varphi,$$

$$(\mathfrak{M}, \mathbf{a}, c) \models \forall j < k \quad (\varphi(j, \mathbf{a}, c) \leftrightarrow \langle j, \varphi(x, \mathbf{y}, z) \rangle Em_k).$$

This completes the proof of part (b) of the claim since (7) and (3) together imply that  $(\mathfrak{M}, \mathbf{a}, c, i)_{i \in I} \equiv (\mathfrak{M}^*, \mathbf{b}, d, i)_{i \in I}$ . ■

We are now ready to establish the following strengthening of Smoryński's theorem.

**THEOREM B.** *Suppose  $\mathfrak{M}$  is a countable recursively saturated model of PA and  $I$  is a cut of  $\mathfrak{M}$  that is closed under exponentiation. There is a group embedding  $j \mapsto \tilde{j}$  from  $\text{Aut}(\mathbb{Q})$  into  $\text{Aut}(\mathfrak{M})$  such that:*

- (a)  $I_{\text{fix}}(\tilde{j}) = I$  for every nontrivial  $j \in \text{Aut}(\mathbb{Q})$ ;
- (b)  $\text{fix}(\tilde{j}) \cong \mathfrak{M}$  for every fixed point free  $j \in \text{Aut}(\mathbb{Q})$ .

*Proof.* Choose  $c \in M \setminus I$  and let  $\mathcal{U}$  be the  $I$ -conservative ultrafilter over  $\mathcal{P}(\bar{c})$  constructed in Theorem 4.3. Use  $\mathcal{U}$  to build the cofinal elementary extension  $\mathfrak{N}_{\mathcal{U}, \mathbb{Q}}$  of  $\mathfrak{M}$ , where  $\mathbb{Q}$  is the ordered set of rationals (see Remark 3.8.1). Invoking parts (d), (e), and (f) of Theorem 3.8, there is a group embedding

$$j \mapsto \lambda \hat{j}$$

from  $\text{Aut}(\mathbb{Q})$  into  $\text{Aut}(\mathfrak{N}_{\mathcal{U}, \mathbb{Q}})$  such that  $I_{\text{fix}}(\hat{j}) = I$  for every nontrivial  $j \in \text{Aut}(\mathbb{Q})$ , and  $\text{fix}(\hat{j}) \cong \mathfrak{M}$  for every fixed point free  $j \in \text{Aut}(\mathbb{Q})$ . On the other hand, by Theorem 2.8 recursive saturation is preserved in the passage from  $\mathfrak{M}$  to  $\mathfrak{N}_{\mathcal{U}, \mathbb{Q}}$  and therefore by Lemmas 4.1 and 4.4,  $\mathfrak{M}$  and  $\mathfrak{N}_{\mathcal{U}, \mathbb{Q}}$  are isomorphic over  $I$  via an isomorphism  $\theta : \mathfrak{M} \rightarrow \mathfrak{N}_{\mathcal{U}, \mathbb{Q}}$ . This allows us to define the desired embedding  $j \mapsto \tilde{j}$  by

$$\alpha = \theta^{-1} \circ \lambda \circ \theta.$$

This is illustrated by the following commutative diagram:

$$\begin{array}{ccc}
 \mathfrak{M} & \xrightarrow{\tilde{j}=\alpha(j)} & \mathfrak{M} \\
 \theta \downarrow & & \uparrow \theta^{-1} \\
 \mathfrak{N}_{\mathcal{U},\mathbb{Q}} & \xrightarrow{\hat{j}=\lambda(j)} & \mathfrak{N}_{\mathcal{U},\mathbb{Q}}
 \end{array}$$

REMARK 4.5. (a) As shown by Kossak [Kos], if  $\mathbb{N}$  is not a strong cut of a countable recursively saturated model  $\mathfrak{M}$  of PA, then the fixed point set of any automorphism of  $\mathfrak{M}$  is isomorphic to  $\mathfrak{M}$  itself. On the other hand, [E-3] confirms a conjecture of Schmerl by showing that if  $\mathbb{N}$  is strong in  $\mathfrak{M}$ , then the isomorphism type of every elementary substructure of  $\mathfrak{M}$  can be realized by a fixed point set of  $\mathfrak{M}$ . [E-3] also includes other results regarding automorphisms of models of PA, including refinements of some of the major results of [KKK].

(b) The existence of a *group embedding* of  $\text{Aut}(\mathbb{Q})$  into  $\text{Aut}(\mathfrak{M})$ , where  $\mathfrak{M}$  is a countable recursively saturated model of PA, was first established as corollary of a deep theorem of Schmerl [Sc-2], which states that every countable recursively saturated model with a definable  $\beta$ -function  $f$  (i.e., a function  $f$  coding finite sequences) is generated via  $f$  from a set of order indiscernibles of any prescribed countable order type with no last element. Elementary considerations show that  $\text{Aut}(\mathfrak{M})$  is also embeddable in  $\text{Aut}(\mathbb{Q})$ . Indeed, as shown in [KKK, Theorem 4.4] there is an embedding of  $\text{Aut}(\mathfrak{M})$  into  $\text{Aut}(\mathbb{Q})$  whose range is dense in  $\text{Aut}(\mathbb{Q})$  (under its natural topology). It is known, however, that  $\text{Aut}(\mathbb{Q}) \not\cong \text{Aut}(\mathfrak{M})$ , since for example,  $\text{Aut}(\mathbb{Q})$  is a divisible group (see [Gl]), but  $\text{Aut}(\mathfrak{M})$  is not (see [KB]). Indeed, as shown in [KKK, Theorem 4.7],  $\text{Aut}(\mathfrak{M})$  is not isomorphic to the automorphism group of any countable  $\aleph_0$ -categorical structure with the small-index property.

(c) Nurkhaidarov [N-1, N-2] has established that for a (fully) saturated model  $\mathfrak{M}$  of PA of power  $\aleph_1$ , a cut  $I$  of  $\mathfrak{M}$  is of the form  $I_{\text{fix}}(j)$  for some nontrivial  $j \in \text{Aut}(\mathfrak{M})$  iff  $I$  is closed under exponentiation and the downward cofinality of  $M \setminus I$  is  $\aleph_1$ . It is easy to see that if PA has a saturated model of power  $\aleph_\alpha$ , then the unique saturated linear order of power  $\aleph_\alpha$ , dubbed  $\eta_\alpha$  by Hausdorff, exists. As shown in [E-6], the method of proof of Theorem B can be adapted to extend the right-to-left direction of Nurkhaidarov’s result by showing that there is a group embedding  $j \mapsto \hat{j}$  of  $\text{Aut}(\eta_1)$  into  $\text{Aut}(\mathfrak{M})$  such that  $I_{\text{fix}}(\hat{j}) = I$  for every nontrivial  $j \in \text{Aut}(\eta_1)$ .

(d) By a corollary of a theorem of Kossak and Kotlarski [KK, Theorem 2.1, Corollary 2.3], the conclusion of Lemma 4.4 continues to hold if the assumption  $\mathfrak{M} \prec_{\text{cofinal}} \mathfrak{M}^*$  is replaced with the assumption that  $I$  is not coded from above by  $\mathbb{N}$  in neither  $\mathfrak{M}$  nor  $\mathfrak{M}^*$ . In light of the fact that the aforementioned result of Kossak and Kotlarski is framed within the more

general context of extendability of automorphisms, the referee has suggested that the strategy of the proof of Lemma 4.4 should also yield an extendability result. The author concurs with the referee's opinion, but has not verified the nitty gritty details of the argument.

(e) As shown by Togha and the author [To, Theorem 3], Smoryński's theorem has a natural analogue for models of ZFC set theory. The proof of Theorem B can be adapted to models of ZFC (with the Erdős–Rado partition theorem taking the place of the finite Ramsey's theorem) to prove an analogue of Theorem B for models of ZFC. This is accomplished in a forthcoming paper [E-4], which also includes a set-theoretical analogue of Theorem A of this paper.

## 5. A REFINEMENT OF THEOREM A

The author has recently established a refinement of Theorem A by characterizing the subsystem  $WKL_0^*$  of second order arithmetic in terms of automorphisms of models of  $I\Delta_0$ .  $WKL_0^*$  is a weakening of the well known subsystem  $WKL_0$  of second order arithmetic in which the  $\Sigma_1^0$ -induction scheme is replaced by  $I\Delta_0 + \text{Exp}$ .  $WKL_0^*$  was introduced by S. Simpson and R. Smith in [Si-Sm] (see also [Sim, Chapter X.4]) who proved, among other things, that  $I\Delta_0 + \text{Exp} + B\Sigma_1$  is the first order part of  $WKL_0^*$  (in contrast to  $WKL_0$ , whose first order part is  $I\Sigma_1$ ). More specifically:

THEOREM 5.1 (Simpson–Smith [Si-Sm]).

- (a) *If  $(\mathfrak{M}, \mathcal{A})$  is a model of  $WKL_0^*$ , then  $\mathfrak{M} \models I\Delta_0 + \text{Exp} + B\Sigma_1$ .*
- (b) *Every countable model of  $I\Delta_0 + \text{Exp} + B\Sigma_1$  can be expanded to a model of  $WKL_0^*$ .*

In light of Theorem 5.1, the following result is a refinement of Theorem A.

THEOREM C ([E-5]). *The following two conditions are equivalent for a countable model  $(\mathfrak{M}, \mathcal{A})$  of the language of second order arithmetic:*

- (a)  $\mathfrak{M} = I_{\text{fix}}(j)$  for some nontrivial automorphism  $j$  of a model  $\mathfrak{N}$  of  $I\Delta_0$  and  $\mathcal{A} = \text{SSy}_M(\mathfrak{N})$ ;
- (b)  $(\mathfrak{M}, \mathcal{A}) \models WKL_0^*$ .

The direction (a) $\Rightarrow$ (b) of Theorem C easily follows from Lemmas A.0–A.2 and known results. The direction (b) $\Rightarrow$ (a), however, is much harder and uses the methods of this paper and the following result, which generalizes the Wilkie–Paris theorem (Theorem 2.4) and improves a key result of Tanaka [Ta]:

THEOREM 5.2 ([E-5]). *Suppose  $(\mathfrak{M}, \mathcal{A})$  is a countable model of  $WKL_0^*$ . There is an end extension  $\mathfrak{N}$  of  $\mathfrak{M}$  that satisfies  $I\Delta_0$  such that  $\mathcal{A} = \text{SSy}_M(\mathfrak{N})$ .*

## References

- [Ad-1] Z. Adamowicz, *A recursion-theoretic characterization of instances of  $B\Sigma_1$  provable in  $\Pi_{n+1}(\mathbb{N})$* , Fund. Math. 129 (1988), 231–236.
- [Ad-2] —, *End extending models of  $I\Delta_0 + \exp + B\Sigma_1$* , ibid. 136 (1990), 133–145.
- [Av-1] J. Avigad, *Saturated models of universal theories*, Ann. Pure Appl. Logic 118 (2002), 219–234.
- [Av-2] —, *Number theory and elementary arithmetic*, Philosophia Math. 11 (2002), 257–284.
- [BS] J. Barwise and J. Schlipf, *On recursively saturated models of arithmetic*, in: Model Theory and Algebra: a tribute to A. Robinson (D. Saracino and V. Weispennig, eds.), Lecture Notes in Math. 498, Springer, 1975, 42–55.
- [Bek] L. Beklemishev, *A proof theoretic analysis of collection*, Arch. Math. Logic 37 (1998), 275–296.
- [Ben] J. H. Bennett, *On spectra*, Ph.D. dissertation, Princeton Univ., 1962.
- [Bu] S. Buss, *First-order proof theory of arithmetic*, in: Handbook of Proof Theory, S. Buss (ed.), North-Holland, Amsterdam, 1998, 79–147.
- [DG] C. Dimitracopoulos and H. Gaifman, *Fragments of Peano’s arithmetic and the MRDP theorem*, in: Logic and Algorithmic, Monogr. Enseign. Math. Univ. of Geneva, 1982, 187–206.
- [E-1] A. Enayat, *Automorphisms, Mahlo cardinals, and NFU*, in: Nonstandard Models of Arithmetic and Set Theory, A. Enayat and R. Kossak (eds.), Contemp. Math. 361, Amer. Math. Soc., 2004, 37–59.
- [E-2] —, *From bounded arithmetic to second order arithmetic via automorphisms*, in: Logic in Tehran, A. Enayat et al. (eds.), Lecture Notes in Logic 26, ASL and A. K. Peters, 2006, 87–113.
- [E-3] —, *Automorphisms of models of arithmetic: a unified view*, Ann. Pure Appl. Logic, to appear.
- [E-4] —, *Automorphisms of models of set theory*, in preparation.
- [E-5] —, *Automorphisms and  $WK L_0^*$* , in preparation.
- [E-6] —, *Automorphisms of saturated models of arithmetic*, in preparation.
- [ER] P. Erdős and R. Rado, *A combinatorial theorem*, J. London Math. Soc. 25 (1950), 249–255.
- [Ga] H. Gaifman, *Models and types of arithmetic*, Ann. Math. Logic 9 (1976), 223–306.
- [Gl] A. Glass, *Ordered Permutation Groups*, London Math. Soc. Lecture Note Ser. 55, Cambridge Univ. Press, Cambridge, 1981.
- [GRS] R. Graham, B. Rothschild, and J. Spencer, *Ramsey Theory*, Wiley-Interscience Publ., New York, 1980.
- [H] P. Hájek, *Interpretability and fragments of arithmetic*, in: Arithmetic, Proof Theory, and Computational Complexity, P. Clote and J. Krajíček (eds.), Oxford Univ. Press, Oxford, 1993, 185–196.
- [HP] P. Hájek and P. Pudlák, *Metamathematics of First Order Arithmetic*, Springer, Heidelberg, 1993.
- [J] R. B. Jensen, *On the consistency of a slight (?) modification of Quine’s New Foundations*, Synthese 19 (1969), 250–263.
- [Ka-1] R. Kaye, *Model-theoretic properties characterizing Peano arithmetic*, J. Symbolic Logic 56 (1991), 949–963.
- [Ka-2] —, *Models of Peano Arithmetic*, Oxford Logic Guides 15, Oxford Univ. Press, 1991.

- [Ka-3] R. Kaye, *Using Herbrand-type theorems to separate strong fragments of arithmetic*, in: *Arithmetic, Proof Theory, and Computational Complexity*, P. Clote and J. Krajíček (eds.), Oxford Univ. Press, Oxford, 1993, 238–246.
- [Ka-4] —, *A Galois correspondence for countable recursively saturated models of Peano arithmetic*, in [KM], 293–312.
- [KKK] R. Kaye, R. Kossak, and H. Kotlarski, *Automorphisms of recursively saturated models of arithmetic*, *Ann. Pure Appl. Logic* 55 (1991), 67–99.
- [KM] R. Kaye and D. MacPherson (eds.), *Automorphisms of First-Order Structures*, Oxford Univ. Press, Oxford, 1994.
- [Kos] R. Kossak, *Automorphisms of recursively saturated models of Peano arithmetic: fixed point sets*, *Log. J. IGPL* 5 (1997), 787–794.
- [KB] R. Kossak and N. Bamber, *On two questions concerning the automorphism groups of countable recursively saturated models of PA*, *Arch. Math. Logic* 36 (1996), 73–79.
- [KK] R. Kossak and H. Kotlarski, *Results on automorphisms of recursively saturated models of PA*, *Fund. Math.* 129 (1988), 9–15.
- [Kot] H. Kotlarski, *On cofinal extensions of models of arithmetic*, *J. Symbolic Logic* 48 (1983), 311–319.
- [Kr] J. Krajíček, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge Univ. Press, Cambridge, 1995.
- [N-1] E. Nurkhaidarov, *On automorphisms of models of arithmetic*, Ph.D. dissertation, Univ. of Connecticut, Storrs, 2004.
- [N-2] —, *Automorphism groups of saturated models of PA of cardinality  $\aleph_1$* , to appear.
- [Pari] J. Paris, *Some conservation results for fragments of arithmetic*, in: *Lecture Notes in Math.* 890, Springer, 1981, 251–262.
- [PM] J. Paris and G. Mills, *Closure properties of countable nonstandard integers*. *Fund. Math.* 103 (1979), 205–215.
- [Pars] C. Parsons, *On a number theoretic choice schema and its relation to induction*, in: *Intuitionism and Proof Theory* (Buffalo, NY, 1968), North-Holland, Amsterdam, 1970, 459–473.
- [Pu] P. Pudlák, *A definition of exponentiation by a bounded arithmetical formula*, *Comment. Math. Univ. Carolin.* 24 (1983), 667–671.
- [Q] W. V. O. Quine, *New foundations for mathematical logic*, *Amer. Math. Monthly* 44 (1937), 70–80.
- [R] J. P. Ressayre, *Nonstandard universes with strong embeddings, and their finite approximations*, in: *Logic and Combinatorics* (Arcata, CA, 1985), S. Simpson (ed.), *Contemp. Math.* 65, Amer. Math. Soc., 1987, 333–358.
- [Sc-1] J. Schmerl, *Recursively saturated rather classless models of Peano arithmetic*, in: *Logic Year 1979-80*, *Lecture Notes in Math.* 859, Springer, 1981, 268–282.
- [Sc-2] —, *Recursively saturated models generated by indiscernibles*, *Notre Dame J. Formal Logic* 25 (1985), 99–105.
- [Sie] W. Sieg, *Fragments of arithmetic*, *Ann. Pure Appl. Logic* 28 (1985), 33–72.
- [Sim] S. Simpson, *Subsystems of Second Order Arithmetic*, Springer, 1999.
- [Si-Sm] S. Simpson and R. Smith, *Factorization of polynomials and  $\Sigma_1^0$ -induction*, *Ann. Pure Appl. Logic* 31 (1986), 289–306.
- [Sm] C. Smoryński, *Back-and-forth inside a recursively saturated model of arithmetic*, in: *Logic Colloquium '80*, D. van Dalen *et al.* (eds.), North-Holland, Amsterdam, 1982, 273–278.

- [Sm-St] C. Smoryński and J. Stavi, *Cofinal extension preserves recursive saturation*, in: Model Theory of Algebra and Arithmetic (Karpacz, 1979), Lecture Notes in Math. 834, Springer, 1980, 338–345.
- [Ta] K. Tanaka, *The self-embedding theorem of  $WKL_0$  and a non-standard method*, Ann. Pure Appl. Logic 84 (1997), 41–49.
- [To] A. Togha, *Automorphisms of countable recursively saturated models of set theory*, in: Nonstandard Models of Arithmetic and Set Theory, A. Enayat and R. Kossak (eds.), Contemp. Math. 361, Amer. Math. Soc., 2004, 163–167.
- [WP] A. Wilkie and J. Paris, *On the existence of end extensions of models of bounded induction*, in: Logic, Methodology and Philosophy of Science, VIII (Moscow, 1987), Stud. Logic Found. Math. 126, North-Holland, Amsterdam, 1989, 143–161.

Department of Mathematics and Statistics  
American University  
4400 Mass. Ave. N.W.  
Washington, DC 20016-8050, U.S.A.  
E-mail: enayat@american.edu

*Received 30 September 2005;  
in revised form 15 May 2006*