To appear in the: *Annals of Pure and Applied Logic*

End extensions of models of linearly bounded arithmetic

Domenico Zambella[1]
Depepartment of Mathematics and Computer Science, University of Amsterdam
Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands
Email: `domenico@fwi.uva.nl` WWW: `http://turing.fwi.uva.nl/~domenico/`

Abstract

We show that every model of $I\Delta_0$ has an end extension to a model of a theory (extending Buss' S^0_2) where logspace computable function are formalizable. We also show the existence of an isomorphism between models of $I\Delta_0$ and models of linear arithmetic LA (i.e., second-order Presburger arithmetic with finite comprehension for bounded formulas).

0 Introduction.

In the last two decades the research on bounded arithmetic has been focussed mainly on the theories of $I\Delta_0$ and $I\Delta_0+\Omega_1$ and on their fragments. The interest in these theories is in part motivated by complexity theoretical considerations. It is well known that the provably recursive function of $I\Delta_0+\Omega_1$ are those computable by algorithms in the polynomial time hierarchy while the provably recursive functions of $I\Delta_0$ correspond to the linear time hierarchy. Some open problems in bounded arithmetic are known to be equivalent to problems of complexity theory. More precisely, to the same problems of complexity theory formalized in models of these theories. For instance, it is known that $I\Delta_0+\Omega_1$ is finitely axiomatizable if and only if $I\Delta_0+\Omega_1$ *proves* that the polynomial time hierarchy collapses (one direction is trivial, the converse is not, see [1], [10]). The first is one of the central problem of bounded arithmetic the second (with true arithmetic in place of $I\Delta_0+\Omega_1$) is one of the central problem in complexity theory.

Other central problems in bounded arithmetic are justified by considerations independent of complexity theory. For instance, we do not know if $I\Delta_0$ proves the pigeonhole principle or

[1]Research supported by the Netherlands Foundation for Scientific Research (NWO) grant PGS 22-262

even some weak version of it (see, below). The provability of these and other combinatorial statements is natural and interesting in itself and also in connection with number theory in models of bounded arithmetic (see [9]). (Also complexity theoretical translations of these problems exists, see [4], but the arithmetical form captures more intriguing aspects.)

A third group of important open problems in bounded arithmetic is connected to the so-called "end extension problem" and/or to the "Π_1-conservativity problem". The end extension problem [8] asks whether every model of $I\Delta_0+B\Sigma_1$ has a proper end extension to a model of $I\Delta_0$, or, more generically, it asks for characterizations of models of $I\Delta_0$ with a proper end extension to models of $I\Delta_0$. The Π_1-conservativity problem is the following question.

* Is every Π_1 sentence provable in $I\Delta_0+\Omega_1$ provable also in $I\Delta_0$?

It is generally accepted that this is not the case. Possible candidates to confute Π_1-conservativity are: the weak pigeonhole principle (no Δ_0 formula defines an injection from $2n$ to n) or the infinity of primes (in the form: for every x there is a prime $x<p<x^2$).

Let us consider a question connected both with the Π_1-conservativity problem and with the end extension problem.

** Does every model of $I\Delta_0$ has and end extension to a model of $I\Delta_0+\Omega_1$?

Clearly, a positive answer to ** would imply a positive answer to the Π_1-conservativity problem but it would have also other generally unaccepted consequences. In fact, every model of $I\Delta_0$ that has a proper end extension to a model of $I\Delta_0$ is a model of $B\Sigma_1$. So, from a positive answer to ** we could infer that $I\Delta_0+\neg\Omega_1$ proves $B\Sigma_1$. This is open but it is conjectured to be false. (The problem of whether of $I\Delta_0+\neg\Omega_1$ prove $B\Sigma_1$ is reminiscent of a famous question posed by Paris and Wilkie in [8]: does $I\Delta_0+\neg\exp$ proves $B\Sigma_1$?)

Problems * and ** are open also if $I\Delta_0+\Omega_1$ is replaced with some of its fragments. E.g., let PV_1 be the fragment of $I\Delta_0+\Omega_1$ that has symbol for every polynomial time computable function and is axiomatized by the recursive equations defining these functions: questions * and ** with PV_1 substituted for $I\Delta_0+\Omega_1$ are open. (We are inclined to conjecture a negative answer in this case as well.)

Let us call *Logrec* the theory defined in the same way as PV_1 but having symbols and axioms only for the functions computable in logarithmic space. We prove that question ** has positive answer if Logrec is substituted for $I\Delta_0+\Omega_1$.

Actually, the theorem is stated and proved in a different setting than what we claimed in the previous paragraph. We shall work with second-order theories that correspond to $I\Delta_0$, $I\Delta_0+\Omega_1$ and *Logrec*. The second-order setting comes naturally along with the idea of the proof: the end extension is build very constructively adding numbers at the top of a model of

$I\Delta_0$. These numbers are identified with the set they code in the model of $I\Delta_0$ (in other words: their binary representation is present in the model of $I\Delta_0$ though the number itself may not).

The plan of the paper is as follows. The main result is precisely stated in the next section. Section 2 and 3 are of introductory nature while the technical work is confined in Section 4 and 5. The result is presented in a second-order setting and it is to a large extent selfcontained, the exact translation of it in a first-order form is not spelled out here, but in Section 2 and 3 we provide enough details to the reader who wishes to undertake this enterprise by him/herself. The last section may be read independently of the proof of the main theorem; it aims to present the theory Σ_0^p-*rec* in relation to other fragments of BA and the open problem of wheather $\Sigma_0^p\text{-}rec = BA$ in relation with other siminilar open problems.

1 Preliminaries

Here we introduce the definitions needed to state precisely the results of the paper. We shall try to be reasonably selfcontained, the reader willing to know more on basic facts about BA, its fragments and the relation with Buss' setup will find some material in [10]. Our basic languages are $L_2(+,\cdot)$ and $L_2(+)$, i.e., that of second-order arithmetic with and respectively without the symbol of multiplication. Specifically, $L_2(+,\cdot)$ consists of two symbols for constants: 0, 1, two symbols for binary functions: $+$, $\cdot$ and two symbols for binary relations: $<$, $\in$. Moreover, there are two sorts of variables: first and second-order. The language $L_2(+)$ coincides with $L_2(+,\cdot)$ but for the absence of the symbol $\cdot$ of multiplication.

First and second-order variables are meant to range respectively over numbers and finite sets of numbers. Terms are constructed from first-order variables only. The intended meaning of $X{<}y$ is: "all elements of X are less than y". Let t be a term in which x does not occur. We adopt the following abbreviations with the usual meaning

$$(Qx{<}t)\varphi,\ (Qx{\in}Y)\varphi,\ (QX{<}t)\varphi,$$

where Q is either $\forall$ or $\exists$. Quantifiers occurring in one of these contexts are called **bounded quantifiers**. Specifically, we shall speak about **polynomial quantifiers** or **linear quantifiers** according to whether the bounding term t is in $L_2(+,\cdot)$ or in $L_2(+)$. A formula is **polynomial** or **linear**, if it is bounded and it is a formula of $L(+,\cdot)$, or respectively, $L(+)$. The set of polynomial formulas is denoted by PH. The set of linear formulas by LH.

We classify bounded formulas of PH and LH in the **polynomial hierarchy** and **linear hierarchy** by counting alternations of second-order quantifiers. We use one of the symbols Π_0^p or Σ_0^p for the class of polynomial formulas containing atomic formulas and closed under Boolean connectives and polynomial first-order quantifiers. We define inductively Σ^p_{i+1} as the minimal class of formulas containing Π^p_i, closed under disjunction, conjunction and polynomial existential quantification. The class Π^p_{i+1} is the minimal class of formulas containing Σ^p_i, closed under disjunction, conjunction and polynomial universal quantification. So, PH equals $\bigcup_{i\in\omega}\Sigma^p_i$ and $\bigcup_{i\in\omega}\Pi^p_i$. The classes Σ^l_i and Π^l_i are defined analogously but atomic formulas and all quantifiers are required to be linear. Clearly Σ^l_i and Π^l_i coincide with the intersections of Σ^p_i and Π^p_i with $L_2(+)$.

Finally, the symbols for classes of formulas just defined may occur prefixed by $\exists$ and/or $\forall$ to mean that formulas in the class may be prefixed by unbounded (first and/or second-order) existential, resp. universal, quantifiers.

It is not difficult to realize that we have given an alternative concise way of defining the polynomial time hierarchy. In fact, up to identifying sets with strings, the classes Σ^p_{i+1} and Π^p_{i+1} coincide with those of the Meyer-Stockmeyer polynomial time hierarcy. In particular NP sets are the Σ^p_1 definable classes and $coNP$ the Π^p_1 definable classes. It is also true (but, by far, less trivial to see) that sets in the linear time hierarchy are exactly those which are definable by linear formulas. (But it is unknown if a level-by-level correspondence between Σ^l_{i+1}, Π^l_{i+1} and the classes of the linear time hierarchy holds.)

Second-order **polynomially bounded arithmetic** (BA) is axiomatized by the following set of proper axioms plus the schema below where φ is a polynomial formula not containing free occurrences of the variable X. The first three lines contain the usual recursive equations for $+$, $\cdot$ and $<$. The fourth line contains the axiom of extensionality, the defining equation of $X{<}y$ and the **least upper bound axiom**. This last axiom deserves some special remark. It claims the existence of the least upper bound of every set, so, the least number principle follows from it (over some comprehension). It entails also that all sets are 'finite'. The least upper bound of the set X will be denoted by $|X|$; the largest element of a nonempty X is then $|X|{-}1$. Finally, in the last line below we display the schema of **finite comprehension**.

$0 \neq 1$	$a{+}(b{+}1) = (a{+}b){+}1$	$a \neq 0 \leftrightarrow (\exists x{<}a)(x{+}1 = a)$
$a{+}0 = a$	$a{\cdot}(b{+}1) = (a{\cdot}b){+}a$	$a \leq b \leftrightarrow a{<}b{+}1$
$a{+}1 = b{+}1 \rightarrow a = b$	$a{\cdot}0 = 0$	$a \leq b{+}1 \leftrightarrow a{<}b$
$A = B \leftrightarrow A{\subseteq}B \wedge B{\subseteq}A$	$A{<}b \leftrightarrow (\forall x{\in}A)(x{<}b)$	$A \neq \emptyset \rightarrow (\exists x{\in}A)(A{<}x{+}1)$

$$(\exists X{<}a)(\forall x{<}a)\ [x{\in}X \ \leftrightarrow\ \varphi(x)].$$

(The expressions $a \leq b$, $A = \emptyset$ and $A{\subseteq}B$ stand for the usual abbreviations.) The theory of **linearly bounded arithmetic** (LA) is axiomatized by those axioms above which are formulas of $L_2(+)$.

For Δ any of the classes of bounded formulas defined above we shall call Δ finite comprehension (abreviate with Δ-*comp*) the theory obtained restricting the schema of finite comprehension to formulas in Δ. The theory of Σ_0^p first-order recursion (abreviated with Σ_0^p-*rec*) is axiomatized by Σ_0^p-*comp* and a schema stating that there is a set coding an arbitrarily long path through any given Σ_0^p definable directed graph without terminating nodes. That is, the following schema for φ a Σ_0^p formula where Z does not occur free:

$$(\forall x{<}a)(\exists y{<}a)\varphi(x,y) \rightarrow \exists Z\,(\forall w{<}b)\varphi(Z(w), Z(w{+}1)),$$

where $Z(x)$ is the value at x of the function coded by the set Z (in some natural coding of functions as sets). We are ready to state the main theorem.

Theorem 1 *Every model of LA has an end extension to a model of Σ_0^p-rec.*

2 Some complexity theoretical aspects.

Let us conclude the introductory part of the paper by commenting on the complexity theoretical strength of the fragment Σ_0^p-*rec*. We claim that functions computable in logarithmic space are provably total in this theory. We shall not prove this fact in detail but we hope to give enough arguments to convince the reader of this fact. We need a technical observation on the schema of Σ_0^p-*rec*. Namely, that for all φ in Σ_0^p, the schema below is derivable from Σ_0^p-*rec*:

$$(\forall w{<}b)(\forall x{<}a)(\exists y{<}a)\varphi(w,x,y) \rightarrow \exists Z\ (\forall w{<}b)\varphi(w, Z(w), Z(w{+}1)).$$

To prove this fix a b and define ψ as follows: "$\big\langle\langle x,w\rangle, \langle y,z\rangle\big\rangle$ iff $\varphi(w,x,y)$ and z is $w{+}1$ modulo $b{+}1$". A path of length $2b$ through ψ can be easily transformed, using Σ_0^p comprehension, into a Z satisfying the formula above.

We need this more general schema of recursion to derive that if $(\forall x{<}a)(\exists y{<}a)\varphi(x,y)$ and $x_0{<}a$ is given, then there is a path through φ that starts from x_0. To see this, apply the schema above to the formula $[w = 0 \wedge y = x_0] \vee [w{>}0 \wedge \varphi(x,y)]$; then shift the resulting path Z by one to the left.

Let $\mathfrak{M}$ be a model of Σ_0^p-*rec*. The first-order part of $\mathfrak{M}$ satisfies $I\Delta_0$ (this because of Σ_0^p-*comp*). So, we have a Δ_0-definition of (first-order) exponentiation and to every x we can associate a string of length $\log x$ (see [3] Ch.V Sec.3). This makes it possible to formalize computation of a Turing machine whose space resources are bounded by the logarithm of the length of the input in the way we explain below. Let us associate each set I with a binary string of length $|I|$. Our deterministic Turing machine reads the input I in a read-only tape and writes the output O in a write-only tape. The working space is bounded by the logarithm of $|I|$ times some fixed constant n (that we think of as a standard number). So, internal states of the Turing machine can be coded by first-order elements $x{<}|I|^n$. We can formalize, by using a Σ^p_0-formula with I as parameter, the next-state relation among states of a Turing machine having written I in the input tape. Let $\varphi(x,y,I)$ be this formula. If we assume that the Turing machine never halts (but possibly loops in a state), the antecedent of the schema of Σ^p_0-*rec* is satisfied by the next-state formula φ (with $|I|^n$ for a). The axiom of recursion claims the existence of a path Z that, in our case, yields the code of a computation of this Turing machine. By the remark in the previous paragraph we can require the path starts from the state: 'empty working tape'. So, Z actually codes a computation on input I. The output of the computation can be Σ^p_0-defined reading the 'write instructions' that are coded in Z.

3 The first-second-order isomorphism

Nonstandard second-order models are always denoted with Gothic capital letters, first-order models (or the first-order parts of second-order models) are denoted by (the corresponding) lower-case letters. Given a first-order model $\mathfrak{m}$ in which the usual notion of logarithm and of binary string are formalizable, we construct a second-order model with a canonical procedure[2]. Namely, let $\log x$ and $\mathrm{Log}\, x$ denote respectively the logarithm of $x{+}1 \in \mathfrak{m}$ and the set

$$\mathrm{Log}\, x := \big\{ y{<}\log x \ \ : \ \ (x)_y = 1 \big\}$$

(where $(x)_y$ is the y-th digit in the binary expansion of x). The domain of the second-order model $\mathfrak{Log}\,\mathfrak{m}$ is

$$\mathfrak{Log}\,\mathfrak{m} := \big\{ \log x, \mathrm{Log}\, x \ \ : \ \ x{\in}\mathfrak{m} \big\}.$$

Relations and functions on $\mathfrak{Log}\,\mathfrak{m}$ are defined in the natural way. It is routine to check that if $\mathfrak{m}$ is a model of $I\Delta_0{+}\Omega_1$ then $\mathfrak{Log}\,\mathfrak{m}$ is a model of BA. In general, if $\mathfrak{m}$ is only a first-order model of $I\Delta_0$, $\mathfrak{Log}\,\mathfrak{m}$ is a model of LA. In fact, the first-order sentence Ω_1 asserts exacly the closure of the logarithmic cut under multiplication.

Vice versa, every second-order model $\mathfrak{M}$ of BA or of LA is the $\mathfrak{L}$ogarithm of some $\mathfrak{n}$ model of $I\Delta_0{+}\Omega_1$ or, respectively, $I\Delta_0$. For BA this is relatively simple to check. The domain of the model $\mathfrak{n}$ consists of the second-order elements of $\mathfrak{M}$. They are now interpreted as first order objects, namely as the numbers $\sum_{x\in X} 2^x$. One has to define 0_2, 1_2, $+_2$, $\cdot_2$ and $<_2$ in $\mathfrak{n} := \{X : X{\in}\mathfrak{M}\}$ in order that $\mathfrak{n}$ satisfies all axioms of $I\Delta_0{+}\Omega_1$. The definition of 0_2, 1_2 and $<_2$ is immediate:

[2]Takeuti was the first to discuss this isomorfism in depth under the name 'RSUV' isomorfism'. See [5].

$$0_2 := \emptyset, \qquad 1_2 := \{0\}, \qquad X <_2 Y \overset{def}{\longleftrightarrow} X \neq Y \wedge |X \triangle Y| - 1 \in Y$$

(recall that $|X \triangle Y|-1$ is the largest element which is in Y but not in X or vice versa). For addition and multiplication one has to formalize more or less directly the school algorithms for the arithmetical operations on numbers written in a binary base. In fact, these can be easily translated in polynomial formulas and BA will prove both totality and the recursive equations for the new second-order functions. Finally, we have to check (see Lemma 4 below) that the least number principle holds in $\mathfrak{n}$.

Finally the reader may check that the two operations are mutually inverse, i.e., that $\mathfrak{M}$ is actually (isomorphic to) $\mathfrak{L}og\, \mathfrak{n}$.

The isomorphism presented above applies also to fragments of BA, resp. S_2. In fact, Σ^p_{i+1}-*comp* corresponds to S_2^{i+1} while adding to Σ^p_{i+1}-*comp* the $<_2$-least number principle we obtain the second-order theory which is isomorphic to T_2^{i+1}. We have seen in the previous section that logspace computations are formalizable in Σ^p_0-*rec*. We know (see, e.g., [3] Ch.V Sec.2(f)) that we can design Turing machines that computes additon resp. multiplication of binary numbers by using, essentially, the school algorithms. The amount of tape needed for the computation of the two basic arithmetical operations grows logarithmically with the length of the input. So, we can assume that a sutable formalization of these algorithms can be used to define a first-second-order isomorphism for a weak fragment such as Σ^p_0-*rec*. In this article we shall never need to make the first-order theory which corresponds to Σ^p_0-*rec* explicit. But it adds relevance to our result to know that such a first-order theory exists. (As far as we know, a first-order theory corresponding to Σ^p_0-*rec* has never been studied. It should contain S_2^0 and prove comprehension for Σ^b_0 formulas as well as the (obvious) translation of the schema of first-order recursion. An explicit presentation of this theory require some work of bootstrapping which is, due to the absence of S_2^1, rather lengthy.)

In principle, one could attempt the construction of a first-second-order isomorphism for models of LA in a similar way. But, unfortunately, a direct formalization of the school algorithms for plus and times is not possible in LA. The non totality of (first-order) multiplication forces to repeated use of divide and conquer techniques to define the graph of (second-order) multiplication. So, the final check of the recursive equations. For this reason we shall avoid the use of the first-second-order isomorphism for LA. Still, since the existence of such an isomorphism is heuristically interesting, we suggest a the following brief informal argument: given a model $\mathfrak{M}$ of LA end extend it to a model of Σ^p_0-*rec* and construct the first-order model $\mathfrak{n}$ isomorphic to it. Observe that the immage of $\mathfrak{M}$ onder this isomorphism is an initial segment of $\mathfrak{n}$ and is a model of $I\Delta_0$ isomorphic to $\mathfrak{M}$.

4 Bootstrapping

In this section we discuss some routine work of bootstrapping. While in BA bootstrapping is a matter of a few lines, the details of the bootstrapping of LA are very lengthy. The exposition will gain in clarity if the task of working out the plan outlined below is left to the diligent reader. The most important things to show are that the graphs of multiplication and exponentiation are definable by linear formulas and that 'small' sets may be coded by numbers in the usual way. (The definition of multiplication is given at the end of this section. The definition of exponentiation can be given using similar ideas.) Clearly, multiplication and exponentiation are not provably total in LA but their recursive equations are provable. In particular their inverse functions, division, roots and logarithms are total functions.

One needs also to check that every model of $LA + \forall x, y\ (x{\cdot}y){\downarrow}$ has an unique expansion to a model of BA. From this and from the fact that $x^n{\downarrow}$ implies $(2x)^n{\downarrow}$ we have that in a model $\mathfrak{M}$ of LA, the initial segment of $\mathfrak{M}$ with domain

$$\Big\{x, X\ \ :\ \ \text{for all } n{\in}\omega\ \mathfrak{M} \models x^n{\downarrow}\ \ \text{resp. } \mathfrak{M} \models |X|^n{\downarrow}\Big\}$$

is (expandable to) a model of BA. The following lemma will be often used in the sequel to tranform polynomial formulas into linear formulas whenever a sufficiently large parameter is at hand. Tthe reader can find some hint for the proof in [3] Ch.I Sec.1(b). We shall refer to the formula φ^l in the lemma below as the **linear translation** of φ.

Lemma 2 For every polynomial formula $\varphi(\vec{x}, \vec{X})$ there is a linear formula $\varphi^l(q, \vec{x}, \vec{X})$ such that BA proves

$$\forall a\, \exists q\ (\forall \vec{x}, \vec{X}{<}a)\Big[\varphi(\vec{x}, \vec{X}) \leftrightarrow \varphi^l(q, \vec{x}, \vec{X})\Big].$$

Moreover, we can assume that there is some standard n depending on φ such that, for all $q'', q' \geq a^n$ and for all $\vec{x}, \vec{X}{<}a$ the formulas $\varphi^l(q', \vec{x}, \vec{X})$ and $\varphi^l(q'', \vec{x}, \vec{X})$ are equivalent over LA. ∎

The linear definability of exponentiation is mainly needed to have a good notion of (L)logatithm. What we need is that Logarithms commute with the second-order operation given (mentioned) in the previous section.

Lemma 3 Let $\mathfrak{M}$ be a model of LA. For every a and every $C{<}\log a$ in $\mathfrak{M}$ there is a $c \leq a$ such that $C = \operatorname{Log} c$. Moreover this c is unique. Let $q{\in}\mathfrak{M}$ be nonstandard. Let $X +_2 Y$ and $X \cdot_2 Y$ be the polynomial functions formalizing second-order addition and multiplication (as explained in Section 1). Let $X +_2^q Y$ and $X \cdot_2^q Y$ be their linear translations as in the lemma above. Then for all a, b and $c{<}q$ such that $a{\cdot}b = c$ we have

$$\operatorname{Log} a +_2^q \operatorname{Log} b \;=\; \operatorname{Log}(a+b) \quad \text{and} \quad \operatorname{Log} a \cdot_2^q \operatorname{Log} b \;=\; \operatorname{Log} c.$$

Moreover we have that if $a<b$ then $\operatorname{Log} a <_2 \operatorname{Log} b$. ∎

Lemma 4 *LA proves the $<_2$-least number principle for every linear formula.*

Proof. The $<_2$-least number principle is the schema

$$\varphi(A) \;\rightarrow\; (\exists X \leq_2 A)\big[\varphi(X) \wedge (\forall Y <_2 X)\neg\varphi(Y)\big].$$

Let φ be a linear formula. Assume $\varphi(A)$ and let x be the least element of the set

$$\Big\{y \leq |A| \;:\; (\exists X \leq_2 A)\Big[\varphi(X) \wedge (\forall Y <_2 X)\big[\varphi(Y) \rightarrow |X \triangle Y|-1 < y\big]\Big]\Big\}.$$

(This set is nonempty because it contains $|A|$.) If we can show that $x = 0$ we are done. So, assume $x = y+1$ and let X be such that

(*) $$(\forall Y <_2 X)\big[\varphi(Y) \rightarrow |X \triangle Y|-1 < y+1\big].$$

By the minimality of $y+1$, there is a $Y <_2 X$ such that

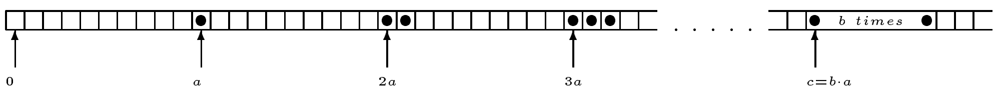
(**) $$\varphi(Y) \;\wedge |X \triangle Y|-1 \;=\; y.$$

We shall contradict the minimality of $y+1$ by showing that

$$(\forall Z <_2 Y)\big[\varphi(Z) \rightarrow |Y \triangle Z|-1 < y\big].$$

Let $Z <_2 Y$ be such that $\varphi(Z)$. By transitivity, $Z <_2 X$ and, by (*), $|X \triangle Z|-1 < y+1$. The latter together with (**) implies $|Y \triangle Z|-1 < y+1$. It remains to exclude $|Y \triangle Z|-1 = y$. From $Y <_2 X$ and (**) it follows that $y \notin Y$ but, by definition, $Z <_2 Y$ means $|Y \triangle Z|-1 \in Y$. So, $|Y \triangle Z|-1$ can not be y. The proof is complete. ∎

We conclude this section giving as promised the linear definition of (first-order) multiplication. Below we define the formula $M(a,b,c)$ that claims the existence of the set that can be depicted as follows



An interval is a set of the form $\{x : a \leq x < a+b\}$ for some $b>0$ and is denoted by $[a, a+b)$. b is called the length of the interval. When $a = 0$ we write $[b)$ for $[0, b)$. An interval of Z is an interval which is contained in Z and which is maximal, i.e., it is not properly contained in an interval which is also a subset of Z. The formula expressing "$[a, a+b)$ is an interval of Z" is Σ_0^l.

Definition 5 When $a \geq b{>}0$, $M(a,b,c)$ is the formula asserting the existence of a set Z such that three conditions below are satisfied

(o) $Z{<}c{+}b$,

(i) $[0,2a) \cap Z = \{a\}$,

(ii) for every $x,y{<}c$ such that $0{<}x{<}y$,
$[x,y)$ is an interval of Z iff $[x{+}a, y{+}a{+}1)$ is an interval of Z,

(iii) $[c,c{+}b)$ is an interval of Z.

When $b{>}a{>}0$, we let $M(a,b,c)$ assert the same but exchanging the roles of a and b. Finally if either one of a and b is 0 then $M(a,b,c)$ is simply $c = 0$. ∎

5 The proof of the main theorem

Finally, we can start the construction of the end extension. Let $\mathfrak{M}_L$ be a model of LA. Assume $\mathfrak{M}_L$ is not closed under first-order multiplication, otherwise, $\mathfrak{M}_L$ is a model of BA and Σ_0^p*-rec* follows trivially. Let $\mathfrak{M}_P$ be the maximal cut of $\mathfrak{M}_L$ which is closed under multiplication.

$$\mathfrak{M}_P \;:=\; \Big\{ x, X{\in}\mathfrak{M}_L \;\;:\;\; \text{for all } n{\in}\omega, \;\; \mathfrak{M}_L \models x^n{\downarrow} \;\text{ and }\; \mathfrak{M}_L \models |X|^n{\downarrow} \Big\}.$$

Let $\mathfrak{m}_0$ be the first-order model of $I\Delta_0{+}\Omega_1$ obtained from $\mathfrak{M}_P$ via the first-second-order isomorphism. I.e., $\mathfrak{m}_0 := \{X \,:\, X{\in}\mathfrak{M}_P\}$. We expand it to a second-order model $\mathfrak{M}_0$. The sets of $\mathfrak{M}_0$ are all those bounded subsets of $\mathfrak{m}_0$ which are linearly definable over $\mathfrak{M}_L$, i.e., subsets of the form

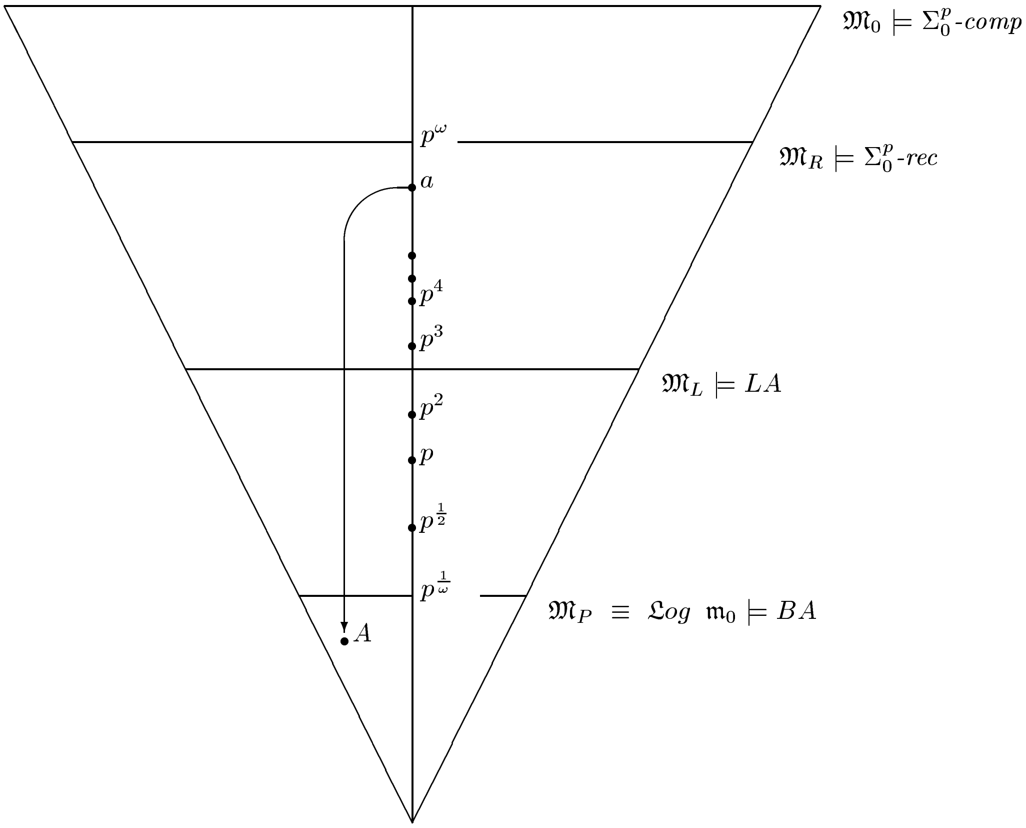
$$C_{\varphi(X)} := \{X{<_2}A :\; \mathfrak{M}_L \models \varphi(X)\};$$

where $A{\in}\mathfrak{M}_P$ and $\varphi(X)$ is a linear formula depending on parameters in $\mathfrak{M}_L$, at most X free. Functions and relations of $\mathfrak{M}_0$ are 0_2, 1_2, $+_2$, $\cdot_2$ and $<_2$ as defined in Section 3, the relation $\in_2$ is defined in the the natulal way. The reader may check that, up to isomorphism, $\mathfrak{M}_0$ is an end extension of $\mathfrak{M}_L$. Now, define,

$$\mathfrak{M}_R := \Big\{ x, X{\in}\mathfrak{M}_0 \;:\; \mathfrak{M}_0 \models x, X{<}p^n \text{ for some } n{\in}\omega,\; p{\in}\mathfrak{M}_L \Big\}.$$

We are going to prove that $\mathfrak{M}_R$ is a model of Σ_0^p*-rec*. Note that for arbitrary $p{\in}\mathfrak{M}_L \setminus \mathfrak{M}_P$

$$\mathfrak{M}_R := \Big\{ x, X{\in}\mathfrak{M}_0 \;:\; \mathfrak{M}_0 \models x, X{<}p^n \text{ for some } n{\in}\omega \Big\}.$$



$$\mathfrak{M}_P := \Big\{ x, X {\in} \mathfrak{M}_L \;:\; \mathfrak{M}_L \models x, X {<} p^{\frac{1}{n}} \;\text{ for all } n{\in}\omega \Big\}.$$

The situation is depicted in the figure below.

A polynomial formula with parameters in $\mathfrak{M}{\cdot}R$ is called a **quasi-linear formula** if all its second-order quantifiers are bounded by elements of $\mathfrak{M}_L$.

Lemma 6 $\mathfrak{M}_R$ satisfies comprehension for all quasi-linear formulas. Also, the $<_2$-least number principle holds in $\mathfrak{M}_R$ for every quasi-linear formula $\varphi(X)$ which holds for some X in $\mathfrak{M}_L$.

Proof. Consider a quasilinear formula $\varphi(x, Y)$. Assume without loss of generality that all the second-order quantifiers of φ are bounded by some $c{\in}\mathfrak{M}_L \smallsetminus \mathfrak{M}_P$. Now, use lemma 3 to write a linear formula $\psi(X, Y)$ such that for all $x{\in}\mathfrak{M}_R$ and all $Y{<}c$,

(*) $$\mathfrak{M}_R \models \varphi(x, Y) \;\Leftrightarrow\; \mathfrak{M}_L \models \psi(\operatorname{Log} x, Y).$$

By the definition of the sets of $\mathfrak{M}_0$, this is sufficient to have comprehension. From this fact and Lemma 4 the $<_2$ least number principle restricted to quasi linear formulas which are witnessed by sets in $\mathfrak{M}_L$ follows. ∎

Quasi-linear functions are those defined as

$$F(\vec{x},\vec{X}) := \{y<|\vec{x},\vec{X}|^n \ : \ \varphi(y,\vec{x},\vec{X})\},$$

where φ is quasi-linear, n is standard and $|\vec{x},\vec{X}|$ is the least upper bound of $\vec{x},\vec{X}$. When ψ is a quasi-linear formula and F is a quasi-linear function, the formula $\psi(\vec{y},\vec{Y},F(\vec{x},\vec{X}))$ is considered as the abbreviation of the quasi-linear formula obtained by unfolding the definition of F inside ψ (in other words: an expansion of the language is not necessary). So, the composition of quasi-linear functions is again a quasi-linear function. In the lemma below we show that in $\mathfrak{M}_R$ quasi-linear functions are closed under recursion provided that their values do not get too large. Precisely, we prove the following.

Lemma 7 For every quasi-linear formula φ and every $a\in\mathfrak{M}_L$ such that for some standard rational $\epsilon>0$, $a^{1+\epsilon}\downarrow\in\mathfrak{M}_L$ the following formula holds in $\mathfrak{M}_R$

$$(\forall X<a)(\exists Y<a)\varphi(X,Y) \rightarrow \exists Z\ (\forall w<b)\varphi(Z^{[w]},Z^{[w+1]})].$$

where $Z^{[x]}$ is defined as $\{y<a : x\cdot(a+y)\in Z\}$.

Proof. Fix an $a\in\mathfrak{M}_L$ such that $a^{1+\epsilon}\downarrow$ and let q be an arbitrary element of $\mathfrak{M}_L\setminus\mathfrak{M}_P$. If a belongs to $\mathfrak{M}_L\setminus\mathfrak{M}_P$, let p be a^ϵ, otherwise, let p be the largest element of the set $\{x:\ a\cdot x\downarrow<q\}$. Clearly, in both cases p is in $\mathfrak{M}_L\setminus\mathfrak{M}_P$ and so, $\{p^n\}_{n\in\omega}$ is cofinal in $\mathfrak{M}_R$. Also, in both cases $a\cdot p\downarrow\in\mathfrak{M}_L$. We shall prove, by induction on n standard, that for all quasi-linear φ, if $(\forall X<a)(\exists Y<a)\varphi(X,Y)$ then there is a quasi-linear formula F such that for all $X<a$

$$(\circ)\quad F(0,X)=X \ \wedge\ (\forall w<p^n)\varphi(F(w,X),F(w+1,X)),$$

The lemma will follow from the cofinality of $\{p^n\}_{n\in\omega}$ in $\mathfrak{M}_R$, and Lemma 6. Let $n=1$ and asume $(\forall X<a)(\exists Y<a)\varphi(X,Y)$. A direct application of induction on $r\leq p$ to the quasi-linear formula,

$$(*)\quad (\forall X<a)(\exists Z<a\cdot r)\,[Z^{[0]}=X\wedge(\forall w<r)\varphi(Z^{[w]},Z^{[w+1]})],$$

shows the existence for all $X<a$ of a Z such that $Z^{[0]}=X$ and for all $w<p$, $\varphi(Z^{[w]},Z^{[w+1]})$. By the $<_2$-least number principle there is a quasi-linear function that takes $X<a$ as input and outputs the $<_2$-minimal Z satisfying the formula (*) above (with p for r). So, $(\circ)$ for $n=1$ follows immediately.

Now, assume that for some $n>0$, $(\circ)$ holds for all quasi-linear formulas. To prove the claim for $n+1$ consider the quasi-linear formula

$$\psi(X,Y)\ :\equiv\ F(0,X)=X\ \wedge\ F(p^n,X)=Y\ \wedge\ (\forall w<p^n)\varphi(F(w,X),F(w+1,X)),$$

where F is obtained by the induction hypothesis. W.l.o.g. we can assume that $(\forall X<a)(\exists Y<a)$ $\varphi(X,Y)$. Now, applying the induction hypothesis for $n=1$, we can find G such that $G(0,X)=$

X and $\psi(G(w,X),G(w{+}1,X))$ for all $w{<}p$. It is easy to check that the following quasi-linear function H satisfy $(\circ)$ with $n{+}1$ for n.

$$H(w,X) := F\left(w - \left\lfloor \frac{w}{p^n} \right\rfloor \cdot p^n, G(\left\lfloor \frac{w}{p^n} \right\rfloor, X)\right)$$

(this means: take $\lfloor w/p^n \rfloor$ large steps with G and do the fine tuning with F). ∎

We show that from this last lemma follows that $\mathfrak{M}_R$ is a model of Σ_0^p-*rec*. Fix a quasi-linear formula $\varphi(x,y)$ (so, in particular, a Σ_0^p-formula), fix $a,b{\in}\mathfrak{M}_R$ and $x{<}a$. Assume that in $\mathfrak{M}_R$ holds $(\forall x{<}a)(\exists y{<}a)\varphi(x,y)$. Define the formula

$$\tilde{\varphi}(X,Y) \stackrel{def}{\longleftrightarrow} (\exists x,y{<}q)\Big[(X = \operatorname{Log} x) \wedge (Y = \operatorname{Log} y) \wedge \varphi(x,y)\Big],$$

where q is an arbitrary element of $\mathfrak{M}_L \setminus \mathfrak{M}_R$. Observe that $(\forall X{<}\log a)(\exists Y{<}\log a)\ \tilde{\varphi}(X,Y)$. We can apply the lemma above because $(\log a)^2{\downarrow}{\in}\mathfrak{M}_L$. Lemma 7 yields a set Z such that

$$(\forall w{<}b)\ \tilde{\varphi}(Z^{[w]}, Z^{[w+1]}).$$

To complete the proof of the theorem we just need to go back from Logarithms to numbers. ∎

Finally, let us observe that, by the very definition of the model $\mathfrak{M}_R$, the set Z, whose existence has been proved in the lemma above, is definable by a linear formula. So, Lemma 7 can be read as a metatheorem on linear (i.e., Δ_0) definability.

6 Two conservativity results

Let us conclude this article by presenting some relations between Σ_0^p-*rec* and the (sometimes easier to handle) theory Σ_1^p-(*rec*+*choice*). It is open whether our end extension theorem can be strengthened to this theory. We show that the existence of a model of Σ_0^p-*rec* and $\Sigma_1^p \neq \Pi_1^p$ is equivalent to the existence of a model of Σ_1^p-(*rec*+*choice*) and $\Sigma_1^p \neq \Pi_1^p$ (see Lemma 11). Finally, we see how the existence of this model relates to the existence of models where Σ_1^p-*comp* fails (see Theorem 12). We begin with recalling the definition of the theory Σ_1^p-*choice*. It is axiomatized by Σ_0^p-*comp* and the following schema for φ ranging over the Σ_1^p formulas where Z does not occur free,

$$(\forall x{<}a)(\exists Y{<}b)\varphi(x,Y) \rightarrow \exists Z\ (\forall x{<}a)\varphi(x,Z^{[x]}),$$

where $Z^{[x]}$ is the set $\{y : \langle x,y\rangle{\in}Z\}$.

Let me recall also the definition of rudimentary extension of a model. (The definition is taken from [10] Section 2.3 but here it is presented in a more concise way.) Let $\mathfrak{M}$ and $\mathfrak{N}$ be a models of Σ^p_0-*comp*. We say that $\mathfrak{N}\supseteq\mathfrak{M}$ is a rudimentary extension of $\mathfrak{M}$ if it is Σ^p_0 elementary and for all A in $\mathfrak{N}$ there is an B in $\mathfrak{M}$ such that $\mathfrak{N}\models\exists x\,(A=B^{[x]})$. Roughly speaking: all sets of $\mathfrak{N}$ are 'relatively constructible' from $\mathfrak{M}$.

Lemma 8 The theory Σ^p_0-*rec* is preserved under rudimentary extension.

Proof. Let $\mathfrak{M}$ be a model of Σ^p_0-*rec* and let $\mathfrak{N}$ be a rudimentary extension of $\mathfrak{M}$. Fix G, a and b in $\mathfrak{N}$. Assume that $(\forall x{<}a)(\exists y{<}a)\,\big(\langle x,y\rangle{\in}G\big)$. We claim there is a Z such that $\langle Z(w),Z(w{+}1)\rangle$ is in G for all $w{<}b$. Observe that rudimentary implies cofinality, so, there are some $\tilde{a}{>}a$ and $\tilde{b}{>}b$ in $\mathfrak{M}$. Clearly it is enough to prove the claim with $\tilde{a}$, $\tilde{b}$ and $\tilde{G}:=G\cup\{\langle x,0\rangle : a\le x{<}\tilde{a}\}$ substituted for a, b and G. By the definition of rudimentary extension, $\tilde{G}=H^{[c]}$ for some c in $\mathfrak{N}$ and some H in $\mathfrak{M}$. Take any $\tilde{c}{>}c$ in $\mathfrak{M}$. Using Σ^p_0 finite comprehension we can easily construct a set $\tilde{H}$ such that $\tilde{H}^{[c]}=H^{[c]}$ and

$$(\forall z{<}\tilde{c})(\forall x{<}a)(\exists y{<}a)\;\big(\langle x,y\rangle{\in}H^{[z]}\big).$$

Let us define a graph K as the sets of those pairs $\big\langle\langle x,z,w\rangle,\langle y,\hat{z},\hat{w}\rangle\big\rangle$ such that one of the following hold

$$(1)\;\;\langle x,y\rangle{\in}\tilde{H}^{[z]},\quad z=\hat{z},\quad w{+}1=\hat{w}\le b{+}1$$

$$(2)\;\;\hat{z}=z{+}1,\quad w=b{+}1,\quad \hat{w}=0$$

Finally let $\tilde{K}$ be obtained stating that $\langle x,z,w\rangle$ is in relation with $\langle 0,0,0\rangle$ whenever $\langle x,z,w\rangle$ is not in the domain of K. Let $Z{\in}\mathfrak{M}$ be a path of length $b{\cdot}\tilde{c}$ through $\tilde{K}$. The reader may check that Z walks b consecutive steps through the graph $\tilde{H}^{[z]}$ and than it jumps to $\tilde{H}^{[z+1]}$. This for every $z{<}\tilde{c}$. (Σ^p_0 is indeed sufficient to prove this.) This may be said in a Σ^p_0 way, so, it will be true in $\mathfrak{N}$ too. The lemma follows. ∎

Lemma 9 Every model of Σ^p_0-*comp* has a rudimentary extension to a model of Σ^p_1-*choice*. This extension is $\forall\Pi^p_1$ elementary. (Actually, all rudimentary extensions are $\forall\Pi^p_1$ elemenary.)

Proof. This is (the easy case of) Lemma 2.3 of [10]. ∎

Lemma 10 Σ^p_0-*rec* is equivalent to Σ^p_1-*rec* over Σ^p_1-*choice*.

Proof. Assume $(\forall x{<}a)(\exists y{<}a)\psi(x,y)$ for some Σ^p_1 formula ψ. W.l.o.g. we can suppose that ψ has the form $\exists Y\,\varphi(x,y,Y)$ for some Σ^p_0 sormula φ. Use Σ^p_1-*choice* to find a W such that $(\forall x{<}a)(\exists y{<}a)\varphi(x,y,W^{[x]})$. Apply Σ^p_0-*rec* to find a Z coding a path through $\varphi(x,y,W^{[x]})$. Clearly, Z is also a path through ψ. ∎

Lemma 11 Σ^p_1-(*rec+choice*) is $\forall\exists\Sigma^p_1$ conservative over Σ^p_0-*rec*. Moreover, if Σ^p_1-(*rec+choice*) proves Σ^p_1-*comp* then also Σ^p_0-*rec* proves it.

Proof. The first claim follows from Lemma 9. Let $\mathfrak{M}$ be an arbitrary model of Σ^p_0-*rec*. If Σ^p_1-(*rec+choice*) proves Σ^p_1-*comp*, then, by the previous lemmas, there is a rudimentary extension $\mathfrak{N}$ of $\mathfrak{M}$ to a model of Σ^p_1-*comp*. We show that also $\mathfrak{M}$ models Σ^p_1-*comp*. Let $\exists Y\,\varphi(x,Y)$ be a Σ^p_1 formula for some Σ^p_0 formula φ with parameters in $\mathfrak{M}$. Fix an $a{\in}\mathfrak{M}$. We want to prove the existence in $\mathfrak{M}$ of the set $\{x{<}a : \exists Y\,\varphi(x,Y)\}$. Let A be such that

$$\mathfrak{N} \models (\forall x{<}a)[x{\in}A \leftrightarrow \exists Y\,\varphi(x,Y)]$$

It is not difficult to see that Σ^p_1 finite comprehension sufficies to prove the existence of a set Z coding all witnesses of $\exists Y\,\varphi(x,Y)$ whenever they exists, i.e.,

$$\mathfrak{N} \models (\forall x{<}a)[\varphi(x,Z^{[x]}) \leftrightarrow \exists Y\,\varphi(x,Y)]$$

By rudimentarity $Z = W^{[b]}$ for some $b{\in}\mathfrak{N}$. We claim that

$$\mathfrak{M} \models (\forall x{<}a)[\exists Y\,\varphi(x,Y) \leftrightarrow \exists y\,\varphi(x,W^{[y],[x]})],$$

so, the lemma follows by Σ^p_0-*comp*. To prove the claim assume $\exists Y\,\varphi(x,Y)$ in $\mathfrak{M}$. By Σ^p_0 elementarity there is an x in $\mathfrak{N}$ such that $\varphi(x,W^{[b],[x]})$. Hence, $\exists y\,\varphi(x,W^{[y],[x]})$ holds in $\mathfrak{N}$ and, by Σ^p_0 elementarity, in $\mathfrak{M}$. This proves the claim; the lemma follows. ∎

Theorem 12 Σ^p_0-*rec* proves Σ^p_1-*comp* iff it proves $\Sigma^p_1 = \Pi^p_1/poly$

Proof. The 'ony if' direction is a weaker version of a theorem of Buss [1] and Zambella [10]. For the converse, observe that if $\Sigma^p_1 = \Pi^p_1/poly$ follows from Σ^p_1-(*rec+choice*) then Σ^p_1-*comp* is provable there (actually choice for all bounded formulas follows). The theorem follows from the lemma above. ∎

The theorem above offers some support to the conjecture that Σ^p_0-*rec* $\neq$ Σ^p_1-*comp*. But it should be observed that, though the assumption looks stronger than that of [1] and [10] (that is: "Σ^p_1-*comp* is axiomatizable by a set of $\forall\Pi^p_2$ sentences"), the conclusion is essentially the same. We do not know how to improve this.

References

[1] S. R. Buss, Relating the bounded arithmetic and polynomial time hierarchies. *Annals of Pure and Applied Logic*, vol. 75 (1995) pp. 67–77

[2] A. Berarducci and B. Intrigila, Combinatorial principles in elementary number theory. *Annals of Pure and Applied Logic*, vol. 55 (1991) pp. 35–50

[3] P. Hájek and P. Pudlák, *Metamathematics of First-order Arithmetic.* Springer-Verlag (1993)

[4] J. Krajíček, *Bounded arithmetic, propositional logic and complexity theory*, Cambridge University Press, in print.

[5] G.Takeuti, RSUV isomorphism. In *Arithmetic, Proof Theory and Computational Complexity*, eds. P.Clote and J.Krajíček, Oxford University Press (1993) pp. 364–368

[6] A.J. Wilkie and J.B. Paris, On the scheme of induction for bounded arithmetic formulas. *Annals of Pure and Applied Logic*, vol. 35 (1987) pp. 261–302

[7] A.J. Wilkie and J.B. Paris, Counting Δ_0 sets, *Fundaments Mathematica*, vol. 127 (1987) pp. 67–76

[8] A.J. Wilkie and J.B. Paris, On the existence of end extensions of models of bounded arithmetic. In: J.E. Fenstad et al., (eds), *Methodology and Philosophy of Science VIII*, Elsevier Science Publisher BV (1989) pp.143–161

[9] J.B. Paris, A.J. Wilkie and A.R. Woods, Provability of the pigeonhole principle and the existence of infinitely many primes. *The Journal of Symbolic Logic*, vol 53 (1988) pp.1235–1244

[10] D. Zambella, Notes on polynomially bounded arithmetic. To appear in *the Journal of Symbolic Logic*.