UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Notes on polynomially bounded arithmetic

Zambella, D.

DOI
10.2307/2275794
Publication date
1996

Published in
Journal of Symbolic Logic

Link to publication

Citation for published version (APA):
Zambella, D. (1996). Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, *61*, 942-966. https://doi.org/10.2307/2275794

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:23 Aug 2022

Notes on Polynomially Bounded Arithmetic

Domenico Zambella

The Journal of Symbolic Logic, Vol. 61, No. 3. (Sep., 1996), pp. 942-966.

Stable URL:
http://links.jstor.org/sici?sici=0022-4812%28199609%2961%3A3%3C942%3ANOPBA%3E2.0.CO%3B2-Y

The Journal of Symbolic Logic is currently published by Association for Symbolic Logic.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/asl.html.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is an independent not-for-profit organization dedicated to creating and preserving a digital archive of scholarly journals. For more information regarding JSTOR, please contact support@jstor.org.

http://www.jstor.org/
Wed Sep 27 02:33:44 2006

THE JOURNAL OF SYMBOLIC LOGIC
Volume 61, Number 3, Sept. 1996

NOTES ON POLYNOMIALLY BOUNDED ARITHMETIC

DOMENICO ZAMBELLA

Abstract. We characterize the collapse of Buss' bounded arithmetic in terms of the provable collapse of the polynomial time hierarchy. We include also some general model-theoretical investigations on fragments of bounded arithmetic.

Contents

§1. Introduction and motivation. In every model of $I\Delta_0$ numbers code finite sets. Sets coded by numbers are Δ_0-definable. In general, the converse is not true. Weak theories, which do not prove the totality of exponentiation, do not prove the existence of a code for every finite Δ_0-definable set. So, a natural way of strengthening $I\Delta_0$ is by adding to the language second-order variables X, Y, Z, etc. ranging over finite sets of numbers and introducing axioms of finite comprehension ensuring the existence of sets of the form $\{x < a : \varphi(x)\}$ for $\varphi(x)$ ranging over some class of second-order formulas. Interesting theories arise when we restrict the schema of finite comprehension to bounded formulas. These are formulas

Received March 21, 1994; revised July 5, 1995.
Research partially supported by the Nederlands Foundation for Scientific Research (NWO) grant PGS 22-262.

© 1996, Association for Symbolic Logic
0022-4812/96/6103-0014/$3.50

where all quantifiers are of the form $Qx < t$ or $QX < t$ where t is a first-order term (i.e., a polynomial). Note that second-order bounded quantifiers range over sets whose elements are bounded by t, so, by the absence of exponentiation, their nature is radically different from that of first-order quantifiers. We introduce the classes Σ_i^p and Π_i^p counting alternations of (polynomially) bounded second-order quantifiers. Restricting the strength of the schema of finite comprehension to formulas of a certain complexity one obtains the hierarchy of theories that we call Σ_i^p-*comp*. The union of all these theories (i.e., finite comprehension for all bounded second-order formulas) is called second-order bounded arithmetic *BA*. We study the relative strength of various fragments of *BA* and in particular their provably total functions.

In the last decades two subsystems of arithmetic, $I\Delta_0$ and S_2, have been studied especially for their connections with complexity theory (see e.g., [16] and [3] or [7]). In particular, Buss' S_2 is the most extensively studied. The theory S_2 coincides with (an extension by definition of) the equally well-known $I\Delta_0 + \Omega_1$. These theories are first-order strengthenings of $I\Delta_0$. In the case of $I\Delta_0 + \Omega_1$ or S_2 the motivation for the strengthening is somehow technical; it arises from metamathematical and/or syntactical considerations. In fact, in order to have a reasonable formalization of computation and/or syntax one needs to be able to perform operations on strings such as the substitution of substrings. Such an operation increases the code of the string superpolynomially and so, it is is not provably total in $I\Delta_0$. Adding to $I\Delta_0$ an axiom (i.e., Ω_1) asserting the totality of this function one obtains a stronger theory in which it is possible to formalize almost all basic notions of metamathematics. Buss introduced a hierarchy of theories S_2^i whose union is S_2. These fragments of S_2 are obtained by weakening of the axiom of induction (while introducing sufficiently many new primitives to allow smooth bootstrapping).

It is not surprising that *BA* coincides with Buss' S_2, modulo an appropriate translation. Namely, to each (first-order) model $\mathfrak{M}'$ of S_2 corresponds a (second-order) model $\mathfrak{M}''$ of *BA*. The first-order objects of $\mathfrak{M}''$ are the logarithmic numbers of $\mathfrak{M}'$ (i.e., numbers belonging to the domain of exponentiation). The smash function guarantees that these numbers are closed under multiplication. The second-order objects of $\mathfrak{M}'$ are those finite sets which have a code in $\mathfrak{M}'$. In this way, Σ_i^p-formulas get transformed into Σ_i^b-formulas of Buss' language (see e.g., [3] or chapter V of [7]) in a very natural way, so, the constructed second-order model verifies finite comprehension for all bounded formulas. Vice versa, from a model $\mathfrak{M}''$ of *BA* one obtains a (first-order) model $\mathfrak{M}'$ of S_2 by the inverse procedure. As domain of $\mathfrak{M}'$ we take the second-order objects of $\mathfrak{M}''$. In $\mathfrak{M}''$ we define the primitives of S_2 as set operations. Intuitively, we think of a finite set X as the number $\sum_{x \in X} 2^x$ and define operations lead by this idea. We shall see that *BA* disposes over enough second-order recursion to formalize these operations and to prove that the axioms of S_2 hold in $\mathfrak{M}'$. Note, parenthetically, that the cartesian product of two sets is mapped to a first-order function with the growth rate of the smash function.

This procedure actually maps models of Σ_i^p-*comp* into models of S_2^i and vice versa (for all $i > 0$). A few details on this isomorphism (which was discovered in different ways by many authors) are contained in Section 2.7. Readers who are mainly interested in S_2^i are advised to read this section first. In fact, afterwards they will be able to translate most of the results reported here into theorems about

fragments of S_2. In particular, Lemma 3.2 is a strengthening of the main theorem of [3]. Our proof is model-theoretic and it is formally identical to an unpublished model-theoretic argument for the conservativity of $I\Sigma_1$ over *PRA* by Albert Visser. In fact, formal similarities between $I\Sigma_1$ and Σ_i^p-*comp* are apparent when primitive recursive functions are replaced by polynomial time computable functions. Other conservativity results are obtainable with the same method. The author's personal motivation for using a second-order framework is that this approach allows economy of primitives, natural definitions and (again in the author's opinion) a clear heuristic.

In the hierarchy of fragments of *BA* very few inclusions are known to be strict. In general the problem of proving inclusions to be strict seems to be a very difficult one. A more realistic goal is to characterize the collapse of theories in terms of the provable collapse of some complexity classes. A corollary of Lemma 3.2 is that, if $\mathscr{P}$-*def* (i.e., the $\forall\Sigma_1^p$ fragment of Σ_1^p-*comp*) proves $\Sigma_2^p = \Pi_2^p$, then *BA* collapses to $\mathscr{P}$-*def*. So, a very satisfactory result would be to prove the converse. One of the best known results in this direction is the celebrated KPT theorem (see Theorem 4.4): in [10] Krajíček, Pudlák and Takeuti, proved that if $\mathscr{P}$-*def* proves Σ_1^p-*comp*, then in the standard model the polynomial time hierarchy collapses to the second level. Unfortunately, it is still unclear whether their proof is formalizable in *BA*, so, their result cannot be used to answer questions like: if $\mathscr{P}$-*def* proves Σ_1^p-*comp* does *BA* collapse?

The main achievement of this paper is the following theorem. It gives a satisfactory characterization of the collapse of *BA* in terms of the provable collapse of *PH*. (On the right hand side we include the translation into Buss' language. For uniformity, we set $T_2^0 := PV_1$. For the definition of $BB\Sigma_{i+1}^b$ see Section 2.7.)

THEOREM. *The following are equivalent*

(i) $\mathscr{P}_i$-*def* $\vdash \Sigma_{i+1}^p$-*comp*	$T_2^i \vdash S_2^{i+1}$
(ii) $\mathscr{P}_i$-*def* $\vdash \Sigma_{i+1}^p \subseteq \Pi_{i+1}^p$/*poly*	$T_2^i \vdash \Sigma_{i+1}^b \subseteq \Pi_{i+1}^b$/*poly*
(iii) $\mathscr{P}_i$-*def* $\vdash$ *BA*	$T_2^i \vdash S_2$
(iv) $\mathscr{P}_i$-*def* $+ \Sigma_{i+1}^p$-*choice* $\vdash \Sigma_{i+1}^p$-*comp*	$T_2^i + BB\Sigma_{i+1}^b \vdash S_2^{i+1}$.

The implication from (i) to (ii) is Theorem 4.3. The implication from (i) to (iii) can be reconstructed from the proof of Theorem 4.2. (To read these two proofs the reader needs only to rush through Section 2.) From Theorem 4.2 it actually follows that (ii) implies (iii) while in Corollary 3.3 is proved that (iv) implies (i).

ACKNOWLEDGMENTS. The numerous discussions with Rineke Verbrugge, Harry Buhrman and Volodya Shavrukov have been pleasant and stimulating. I also wish to thank Franco Montagna for corrections. When the first draft of this manuscript was ready I had interesting discussions with Sam Buss. I owe him various observations and corrections. Buss [5] independently proved that condition (i) above implies (ii) and (iii). He observed that from (i) it follows that *PH* (provably) collapses to *Boole*(Σ_{i+2}^p). His result inspired the interpolation theorem of Section 4.1. The supervision of Dick de Jongh and Albert Visser has assisted me through the numerous stadia of preparation of this work. ⊣

§2. Preliminaries. Here we introduce the necessary definitions. Lemma 2.3 provides a smooth bootstrapping. The class of polynomial time computable functions

is concisely introduced in Section 2.5 in a machine independent way. The (standard) comparison of strength of the various fragments is sketched in Section 2.6. In Section 2.7 the relation with Buss' S_2^i is sketched.

2.1. The polynomially bounded hierarchy. We define the analogue of the analytical hierarchy for finite sets. The language L_2 is the language of second-order arithmetic; it 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. Lower case Latin letters $x, y, z, \ldots$ denote first-order variables and capital Latin letters $X, Y, Z, \ldots$ second-order variables. 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 of L_2 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 either of these contexts are called **(polynomially) bounded quantifiers**. The class of bounded formulas is denoted by PH. Note that first-order quantifiers range over elements of sets while second-order quantifiers range over subsets of sets. Here, first-order bounded quantifiers play the role that **sharply bounded quantifiers** have in first-order bounded arithmetic (see e.g., [3] or Chapter V of [7]).

A formula is **(polynomially) bounded** if all of its quantifiers are. Counting alternations of second-order quantifiers we classify bounded formulas in the **(polynomially) bounded hierarchy**. We use either one of the symbols Π_0^p or Σ_0^p for formulas containing only bounded first-order quantifiers. We define inductively Σ_{i+1}^p as the minimal class of formulas containing Π_i^p, closed under disjunction, conjunction and bounded existential quantification. The class Π_{i+1}^p is the minimal class of formulas containing Σ_i^p, closed under disjunction, conjunction and bounded universal quantification. So, PH equals $\bigcup_{i\in\omega} \Sigma_i^p$ and $\bigcup_{i\in\omega} \Pi_i^p$.

The class $\Sigma_0^p(\Sigma_i^p)$ is the smallest set of formulas containing Σ_i^p, closed under Boolean operations and bounded first-order quantification. Sometimes we add to the language L_2 some set $\mathscr{F}$ of new symbols for functions. We define the (relativized) classes of bounded $L_2(\mathscr{F})$-formulas: $\Sigma_i^p(\mathscr{F})$, $\Pi_i^p(\mathscr{F})$, etc. similarly to those of the language L_2. (We allow terms of $L_2(\mathscr{F})$ to occur in the bounds of the quantifiers.)

The domain of an L_2 structure $\mathfrak{M}$ is composed of two disjoint parts: the numbers and the sets of $\mathfrak{M}$. To denote elements of a model, we use the same convention as for variables, so, we write $A \in \mathfrak{M}$ for 'A is a set of $\mathfrak{M}$' and $a \in \mathfrak{M}$ for 'a is a number of $\mathfrak{M}$'. For models we use Gothic capitals, for the class of first-order objects of a model $\mathfrak{M}$ we use the corresponding lower case letter $\mathfrak{m}$. The disjoint union of ω and $\mathscr{P}_{<\omega}(\omega)$ constitutes the **standard model**, functions and relations are interpreted in the natural way. We loosely denote the standard model by ω.

For our digressions to computational complexity theory it is convenient to think of finite sets as strings i.e., we identify $\mathscr{P}_{<\omega}(\omega)$ and $2^{<\omega}$. So, sets of finite sets may be identified with languages. The actual form of the isomorphism is immaterial. We stipulate that the length of the string associated to a finite set $X \subseteq \omega$ equals (up to some additive constant) the least upper bound of the set X which we henceforth

denote by $|X|$. To begin with, the reader may wish to check that Σ_1^p-formulas define languages in *NP*, i.e., if $\varphi(X) \in \Sigma_1^p$ then the language $\{X : \omega \models \varphi(X)\}$ is in *NP*. Vice versa for every language $L \subseteq 2^{<\omega}$ in *NP* there is a formula $\varphi(X)$ in Σ_1^p such that L is $\{X : \omega \models \varphi(X)\}$. In the same way, Π_1^p-formulas coincide with *coNP* languages and, in general, each level of the bounded hierarchy coincides with one of the Meyer-Stockmeyer polynomial time hierarchy (with the only exception of ground level $i = 0$ which corresponds to uniform-AC^0 languages). When digressing to computational complexity theory, we identify each number $x \in \omega$ with the set of its predecessors and so, with a string of ones of length x. Therefore, a formula $\varphi(x)$ with one free first-order variable defines a tally language, i.e., a language which is contained in $\{1\}^{<\omega}$.

2.2. The axioms of second-order bounded arithmetic. The theory Θ is axiomatized by the following formulas: (The expressions $a \leq b$, $A = \emptyset$ and $A \subseteq B$ stand for the usual abbreviations.)

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

These are the axioms of Robinson arithmetic plus the defining axioms for the relation $<$, the axiom of extensionality and the least upper bound principle. The theory Σ_i^p-*comp* is axiomatized by Θ and the schema of **(finite) comprehension** for Σ_i^p-formulas i.e., for all φ in Σ_i^p in which X does not occur free,

$$\Sigma_i^p\text{-}comp : (\exists X < a)(\forall x < a)\,[x \in X \leftrightarrow \varphi(x)].$$

The theory of **second-order bounded arithmetic**, *BA*, is the union of Σ_i^p-*comp* for $i \in \omega$.

2.3. Rudimentary functions. In order to keep formulas to a readable size we need to introduce new function symbols. To begin with, let us give some informal definitions. We write $|A|$ for the least upper bound of A and $|\bar{a}, \bar{A}|$ for the least upper bound of $\{1, a_1, \ldots, a_n, |A_1|, \ldots, |A_m|\}$. It should be clear that Σ_0^p-*comp* suffices to prove the existence of $|\bar{a}, \bar{A}|$. We call **rudimentary** those functions which are obtained by Σ_0^p comprehension or by Σ_0^p minimalization, i.e., those functions definable in either one of the two following ways:

$$F_{\varphi,p}(\bar{a}, \bar{A}) := \{x < |\bar{a}, \bar{A}|^p : \varphi(x, \bar{a}, \bar{A})\}, \quad f_{\varphi,p}(\bar{a}, \bar{A}) := \mu_{x<|\bar{a},\bar{A}|^p}\, \varphi(x, \bar{a}, \bar{A}),$$

for some $\varphi \in \Sigma_0^p$ and $p \in \omega$ (in the definition of $F_{\varphi,p}$ and $f_{\varphi,p}$, we have stressed that these functions are polynomially bounded).

Let $\mathscr{R}$ be a set of new primitives, one for each (definition of a) rudimentary function. Let $\mathscr{R}$-*def* be the theory axiomatized by Θ plus the defining axioms for the functions in $\mathscr{R}$. Clearly, Σ_0^p-*comp* suffices to prove every rudimentary function to be total. So, $\mathscr{R}$-*def* is a conservative expansion of Σ_0^p-*comp*. The following lemma ensures us that there is no danger in considering formulas of the expanded

language $L_2(\mathscr{R})$ as abbreviations of L_2-formulas. In fact, the 'translation' does not increase the complexity of the formula. Namely, the following lemma shows that $\Sigma_0^p = \Sigma_0^p(\mathscr{R})$ provably in $\mathscr{R}$-*def*.

LEMMA 2.3. *For every* $\psi \in \Sigma_0^p(\mathscr{R})$, *there is* $\psi^* \in \Sigma_0^p$ *such that* $\mathscr{R}$-*def* $\vdash \psi \leftrightarrow \psi^*$.

PROOF. The lemma is proved by a method which we believe to be well-known to the reader, so, we do not need to give it in full detail. One has to unfold the definitions of the rudimentary functions inside the $\Sigma_0^p(\mathscr{R})$-formula ψ. We can assume that ψ has only one occurrence of a single rudimentary function $F_{\varphi,p}(\bar{a}, \bar{A})$ (we also assume this function is a set function; the case of a number function is similar). First, one must rewrite ψ to have all occurrences of rudimentary set functions on the right of the symbol $\in$. Then replace each subformula of the form $x \in F_{\varphi,p}(\bar{a}, \bar{A})$ with

$$x < |\bar{a}, \bar{A}|^p \wedge \varphi(x, \bar{a}, \bar{A}).$$

Finally, replace subformulas of the form $x < |\bar{a}, \bar{A}|^p$ with an equivalent Σ_0^p-formula. The defining axioms of $F_{\varphi,p}$ ensure that the formula obtained is equivalent to the original ψ. In the resulting formula no rudimentary set function occurs. ⊣

A noteworthy corollary of this lemma is that rudimentary functions are closed under composition. From the lemma it follows also that $\Sigma_i^p(\mathscr{R})$-*comp* + $\mathscr{R}$-*def* is equivalent to Σ_i^p-*comp* + $\mathscr{R}$-*def* and hence an extension by definitions of Σ_i^p-*comp*. Below, we list a few rudimentary functions that we often use.

$$\begin{aligned}
\langle a, b\rangle &:= \mu_z\, 2z = (a+b)(a+b+1), \text{ the pairing function,}\\
A \times B &:= \{z : (\exists x, y \le z)[z = \langle x, y\rangle \wedge x \in A \wedge y \in B\}, \text{ the cartesian product,}\\
A^{[b]} &:= \{y : \langle b, y\rangle \in A\}, \text{ the } b\text{-th row of the 'matrix' } A,\\
A(b) &:= \mu_z\, z \in A^{[b]}, \text{ the value of the 'function' } A \text{ at } b,\\
[x] &:= \{y : y < x\}, \text{ the set of predecessors of } x,\\
\{x\} &:= \{y : x = y\}, \text{ the singleton of } x.
\end{aligned}$$

2.4. Other fragments. In this section we present some other interesting fragments of *BA*; in the next sections we shall study their relative strength. We agree that all theories we introduce in this section contain, by definition, Σ_0^p-*comp*. The theories Σ_i^p-*ind*, Σ_i^p-*dc* and Σ_i^p-*coll* (i.e., of **induction**, **dependent choices** and **strong collection** for Σ_i^p-formulas) are axiomatized by the following schemas, for $\varphi \in \Sigma_i^p$.

$$\begin{aligned}
\Sigma_i^p\text{-}ind &: \varphi(0) \wedge \forall x[\varphi(x) \to \varphi(x+1)] \to \varphi(a),\\
\Sigma_i^p\text{-}dc &: \forall x(\forall X < b)(\exists Y < b)\varphi(x, X, Y) \to \exists Z(\forall x < a)\varphi(x, Z^{[x]}, Z^{[x+1]}),\\
\Sigma_i^p\text{-}coll &: \exists Z\,(\forall x < a)\big[(\exists Y < b)\varphi(x, Y) \to \varphi(x, Z^{[x]})\big],
\end{aligned}$$

(in the last two schemas Z should not occur free in φ). The schema of dependent choices is inspired by second-order arithmetic. We show (cf. Lemma 2.6) that dependent choice, induction and strong collection are all equivalent to comprehension. A rather intriguing role is played by the following schema of **choice**

$$\Sigma_i^p\text{-}choice : (\forall x < a)(\exists X < b)\varphi(x, X) \to \exists Z\,(\forall x < a)\varphi(x, Z^{[x]}),$$

where φ is in Σ_i^p. It asserts that the Σ_i^p-formulas are closed under first-order bounded quantification.[1]

2.5. Polynomial time computable functions. In this section we introduce the classes of functions $\mathscr{P}_i$. These correspond to classes which have been intensively studied in computational complexity theory, i.e., the functions which are polynomial time computable with an oracle for Σ_i^p (also denoted in the literature by $\square_{i+1}^p$). For expository reasons we prefer to introduce them in an axiomatic way avoiding direct reference to any model of computation. Formally, our approach is self-contained.

To begin with, let us work in the standard model, i.e., natural numbers and finite sets of natural numbers. The functions we introduce are of two sorts, number functions and set functions, denoted respectively with lower case and capital letters. Functions take as inputs tuples of numbers and sets. They output either a number (number functions) or a set (set functions). Numbers, as input and/or output, are introduced merely as a useful device to express 'logarithmically many iterations'.

The class $\mathscr{P}$ is the smallest set of functions containing $\mathscr{R}$ and closed under composition and under the following schema of **second-order (polynomially bounded) recursion**

$$F(0,\bar{x},\bar{X}) = G(\bar{x},\bar{X}); \quad F(y+1,\bar{x},\bar{X}) = [|y,\bar{x},\bar{X}|^p] \cap H(y,\ \bar{x},\ \bar{X},\ F(y,\bar{x},\bar{X}))$$

for any G, H in $\mathscr{P}$ and $p \in \omega$.

The recursion schema introduced above is polynomially bounded for two reasons. We bound both the size of the output and the depth of the recursion. So, no more than polynomially many nested iterations of functions are possible.

The class $\mathscr{P}$ is also denoted $\mathscr{P}_0$. In general, the classes $\mathscr{P}_i$ are obtained by adding to $\mathscr{P}$ **Turing oracles** for Σ_i^p-formulas and closing under second-order recursion and composition. Turing oracles for Σ_i^p-formulas are functions of the form

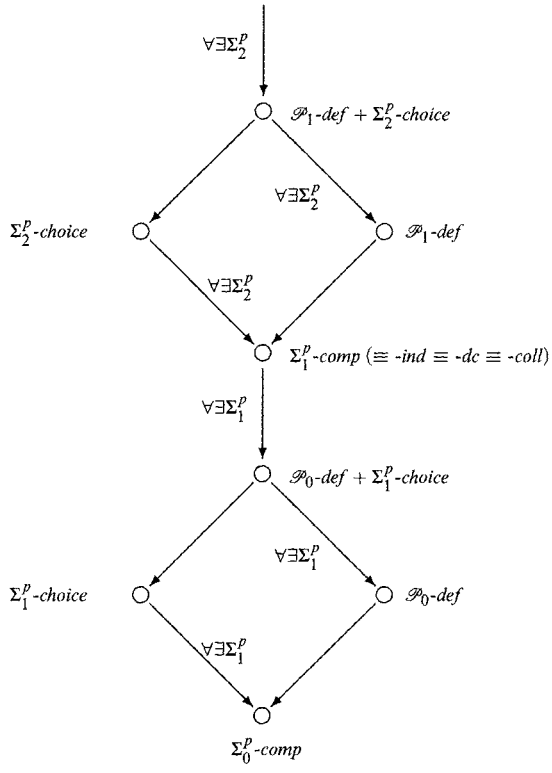
$$F(\bar{a},\bar{A}) = \begin{cases} \{0\} & \text{if } \varphi(\bar{a},\bar{A}) \\ \emptyset & \text{otherwise,} \end{cases}$$

for φ in Σ_i^p.

Now, going back to theories of second-order arithmetic, let us use $\mathscr{P}_i$ to indicate also some sets of symbols for functions, a different symbol for each definition of a function in the corresponding class. Let $L_2(\mathscr{P}_i)$ be the corresponding expansions of L_2. Let $\mathscr{P}_i$-*def* be the theories axiomatized by Θ and the defining axioms of the functions in $\mathscr{P}_i$.

2.6. Relations among fragments. We assume the reader to be familiar with fragments of first-order arithmetic (see e.g., [7]), so, we merely sketch proofs. It is easy to see that the comprehension schemas for Σ_i^p, Π_i^p and $\Sigma_0^p(\Sigma_i^p)$-formulas are equivalent. Also, we may contract quantifiers, so, Σ_{i+1}^p-*dc* and Σ_{i+1}^p-*choice* are respectively equivalent to Π_i^p-*dc* and Π_i^p-*choice* (these last two theories are defined in the obvious way). The theory Σ_{i+1}^p-*choice* proves that Σ_{i+1}^p-formulas are closed under first-order bounded quantification. In the schemas of Σ_i^p-*choice*, Σ_i^p-*dc*

[1] The notation may be a puzzle to the reader if confused with Buss'. Qua strength, *ind* correspond with Buss' LIND or PIND. Our schemas *coll* and *choice* correspond to *strong-replacement*, resp., *replacement* in Buss [3]. What is meant by 'corresponds' is explained in Section 2.7



and Σ_i^p-*coll* we can in addition require the set Z to be a subset of $[a+1]\times[b]$ without strengthening the schema. The easy proofs of these facts are left to the reader.

The content of the lemma we are going to prove in this section is summarized in the picture above. An arrow means provability. Next to the arrow we write the partial conservativity we shall prove in Sections 3.2 and 3.3.

LEMMA 2.6. *For all* $i \in \omega$,

(i) Σ_{i+1}^p-*ind* $\Longrightarrow \Sigma_{i+1}^p$-*choice* $\Longrightarrow \Sigma_i^p$-*comp*

(ii) Σ_{i+1}^p-*comp* $\Longleftrightarrow \Sigma_{i+1}^p$-*ind* $\Longleftrightarrow \Sigma_{i+1}^p$-*dc* $\Longleftrightarrow \Sigma_{i+1}^p$-*coll*

(iii) Σ_{i+1}^p-*comp* $\Longrightarrow \mathscr{P}_i$-*def* $\Longrightarrow \Sigma_i^p$-*comp*.

We understand the first inclusion of (iii) *as: every model of* Σ_{i+1}^p-*comp has a unique expansion to a model of* $\mathscr{P}_i$-*def*.

PROOF OF (i). For the first inclusion, it is sufficient to prove Π_i^p-*choice*. This is proved in a straightforward manner. By the observation above, the quantifier $\exists Z$ in the schema of choice can be bounded. So, assuming the antecedent of the implication one can prove the consequent by induction on the parameter a. The second implication is proved by induction on i. Assume that Σ_{i+1}^p-*choice* proves Σ_i^p-*comp* (this is true by definition if $i = 0$, for $i > 0$ it is taken as induction hypothesis), we show that Σ_{i+2}^p-*choice* proves Σ_{i+1}^p-*comp*. Reason in a model of

Σ^p_{i+2}-*choice*. Let $\varphi(x) \in \Sigma^p_{i+1}$. For some b and some $\psi \in \Pi^p_i$ the formula φ is equivalent to $(\exists X < b)\psi(x, X)$. We have

$$(*) \qquad (\forall x < a)\,(\exists X < b)(\forall Y < b)[\psi(x, X) \vee \neg\psi(x, Y)].$$

We may apply the axiom of choice to get a set $Z \subseteq [a] \times [b]$ such that for all $x < a$, either $\psi(x, Z^{[x]})$ or $(\forall Y < b)\neg\psi(x, Y)$. So, $\psi(x, Z^{[x]})$ is equivalent to $\varphi(x)$. Therefore, Σ^p_i-*comp* suffices to prove the existence of the set $\{x < a : \varphi(x)\}$.

PROOF OF (ii). It is immediate that Σ^p_{i+1}-*comp* contains Σ^p_{i+1}-*ind*. For the converse inclusion, reason in a model of Σ^p_{i+1}-*ind*; let $\varphi \in \Sigma^p_{i+1}$ and choose a parameter a. We want a set $X < a$ such that $x \in X \leftrightarrow \varphi(x)$ for all $x < a$. We are done if we can find a set of maximal cardinality among those such that $x \in X \rightarrow \varphi(x)$ for all $x < a$. In fact, for such an X, also the converse implication holds. Formally, we write $Y : [c] \hookrightarrow X$ for the Σ^p_0-formula saying that Y is an injection of $[c]$ into X or, in other words, that the cardinality of X is at least c. By Σ^p_1-*ind*, there exists a largest $c < a$ such that

$$(\exists X < a)(\exists Y < \langle c, a\rangle)\left[(Y : [c] \hookrightarrow X) \wedge (\forall x \in X)\varphi(x)\right].$$

The X, witnessing the existential quantifier for c maximal, is the required set satisfying $x \in X \leftrightarrow \varphi(x)$ for all $x < a$. This completes the proof of the first equivalence.

To prove that Σ^p_{i+1}-*ind* implies Σ^p_{i+1}-*dc* it is convenient to derive Π^p_i-*dc*. This is done by straightforward induction as for the schema of choice in the previous lemma. The converse implication is proved by induction on i. Reason in a model of Σ^p_{i+1}-*dc*. We show that for every $\psi \in \Sigma^p_{i+1}$,

$$(*) \qquad \psi(0) \wedge (\forall x < a)[\psi(x) \rightarrow \psi(x + 1)] \rightarrow \psi(a).$$

Without loss of generality, we may assume that $\psi(x)$ is equivalent to $(\exists X < b)$ $\varphi(x, X)$ for some $\varphi(x)$ in Π^p_i and some parameter b. Assume the antecedent of (*), then

$$(\forall x < a)(\forall X < b)(\exists Y < b)[\varphi(x, X) \rightarrow \varphi(x + 1, Y)].$$

The formula between square brackets is equivalent to a Σ^p_{i+1}-formula, so, (after a few manipulations) one can apply Σ^p_{i+1}-*dc* to get a set $Z \subseteq [a + 1] \times [b]$ such that

$$Z^{[0]} = A \wedge (\forall x < a)[\varphi(x, Z^{[x]}) \rightarrow \varphi(x + 1, Z^{[x+1]})],$$

where A is any set such that $\varphi(0, A)$. Since Σ^p_i-*ind* holds (by induction hypothesis if $i > 0$ or, by definition, if $i = 0$), we can apply induction on x to the formula $\varphi(x, Z^{[x]})$ to prove $\varphi(a, Z^{[a]})$ and hence $\psi(a)$. This completes the proof of the second equivalence.

We leave the proof that Σ^p_i-*comp* is equivalent to Σ^p_i-*coll* to the reader.

PROOF OF (iii). The proof is standard but very lengthy and it is left to the reader. ⊣

2.7. Relations with Buss' bounded arithmetic. In the introduction we mentioned that Σ_i^p-*comp* coincides with Buss' S_2^i by a suitable translation of formulas. This translation has been found independently by many authors (see e.g., [14, 15, 9]). It is not necessary to include full details here, but, to give some clue to the reader, we quickly show how to transform a model of S_2^i into a model of Σ_i^p-*comp* and vice versa.

Let $\mathfrak{M}_1$ be a model of S_2^i. Let $\mathfrak{M}_2$ be the second-order structure having as first-order objects the elements a of $\mathfrak{M}_1$ such that 2^a exists and as second-order objects those finite subsets of $\mathfrak{M}_1$ which are coded in the usual way by elements of $\mathfrak{M}_1$. I.e., for every $a \in \mathfrak{M}_1$ we add the set A to $\mathfrak{M}_2$ such that

$$a = \sum_{x \in A} 2^x.$$

Functions and relations of $\mathfrak{M}_2$ are defined in the natural way. Note that multiplication of first-order elements is a total operation in $\mathfrak{M}_2$. In fact if 2^a and 2^b exist in $\mathfrak{M}_1$ then $2^{a \cdot b}$ exists too, since it is equal to $2^a \# 2^b$. It is easy to see that $\mathfrak{M}_2$ models Σ_i^p-*comp*. In fact, it is sufficient to note that for every second-order formula $\varphi(x, X) \in \Sigma_i^p$ there is a first-order formula $\varphi^*(x, y) \in \Sigma_i^b$ such that for every $a, A \in \mathfrak{M}_2$

$$\mathfrak{M}_2 \models \varphi(a, A) \iff \mathfrak{M}_1 \models \varphi^*(a, \sum_{x \in A} 2^x).$$

To see the other direction, we apply the inverse procedure. Let $\mathfrak{M}_2$ be a model of Σ_i^p-*comp*. We think of sets of $\mathfrak{M}_2$ as representing numbers, i.e., we think of the set X as the number

$$n(X) := \sum_{x \in X} 2^x.$$

Clearly, in general such a number need not exist in $\mathfrak{M}_2$. Still, formalizing the natural algorithm for addition and multiplication of binary numbers, we may define in $\mathfrak{M}_2$ some set functions $X \oplus Y$ and $X \otimes Y$ such that

$$n(X \oplus Y) = n(X) + n(Y) \text{ and } n(X \otimes Y) = n(X) \cdot n(Y).$$

It is well known that such an algorithm is computable in polynomial time, so, $X \oplus Y$ and $X \otimes Y$ are total functions in every model of $\mathscr{P}$-*def*. Let $X \# Y$ be the set $\{ |X| \cdot |Y| \}$ which exists because $\mathfrak{M}_2$ models Σ_0^p-*comp*. Also, all other functions of the language of S_2 can be defined in a similar way. Now, one can construct a model of S_2^i having as its domain the second-order elements of $\mathfrak{M}_2$ and as functions and relations the ones just defined. The reader may check that the 32 axioms of BASIC hold in $\mathfrak{M}_1$. Since $\mathfrak{M}_2$ is a model of Σ_i^p-*ind*, it is not difficult to see that $\mathfrak{M}_1$ satisfies logarithmic induction for Σ_i^b-formulas. Hence, $\mathfrak{M}_1$ is a model of S_2^i.

We did not introduce any theory corrsponding to the direct translation of Buss' theories T_2^{i+1}. Such translation would look like

$$(*) \qquad \varphi(A) \to (\exists X \leq A)\varphi \wedge (\forall Y < X)\neg\varphi(Y)$$

where $X < Y$ stands for $X \neq Y \wedge |X \triangle Y| - 1 \in Y$ and φ is a Σ_{i+1}^p-formula. For reason of convienence we introduced the theories $\mathscr{P}_{i+1}$-*def* which correspond to

PV_{i+2}. These theories are just expansions by definitions of T_2^{i+1}. From the proof of Lemma 3.1 it is immediate to see that $\mathscr{P}_i$-*def* proves principle (*) above for φ in Σ_{i+1}^p. In fact, the function F defined there computes the minimal X in the lexicografic order satisfying φ. The proof of the converse, i.e., that $\mathscr{P}_i$-*def* is an extension by definition of (*), is omitted.

Finally, to translate the results of Section 3.3 in the language of S_2 note that second-order models of Σ_{i+1}^p-*choice* correspond to first-order models of $BB\Sigma_{i+1}^b$ (cf. Chapter V of [7]), i.e., S_2^i plus the schema

$$(\forall x < |t|)(\exists y < s)\varphi(x, y) \rightarrow \exists w(\forall x < |t|)\varphi(x, (w)_x).$$

where φ is in Σ_{i+1}^b. In [3] this schema is called Σ_{i+1}^b-*replacement*.

The schema of Σ_{i+1}^p-*coll* correspond to Σ_{i+1}^b-*strong-replacement* of [3].

§3. **Witnessing theorems and conservativity results.** Buss was the first one to give an extensive characterization of complexity classes as classes of functions definable and provably total in some weak fragment of arithmetic. Our Corollary 3.2 corresponds to the main theorem of [3]. However, the very idea of the proofs we report here goes back to the Mints-Parsons' famous partial conservativity result of $I\Sigma_1$ over *PRA* [11, 13]. Buss', Parsons' and Mints' proofs are proof-theoretical. Wilkie gave a model-theoretic proof (unpublished) of Buss' theorem (see [7]). Here we adapt a model-theoretical proof of the Mints-Parsons' theorem given by Albert Visser (unpublished).

3.1. Closures. Let $\mathfrak{M}$ be a model of Σ_0^p-*comp* and let $\mathfrak{A}$ be a subset of $\mathfrak{M}$. We say that $\mathfrak{A}$ is closed under $\mathscr{R}$-functions if $F(\bar{c}, \bar{C}), f(\bar{c}, \bar{C}) \in \mathfrak{A}$ for every $\bar{c}, \bar{C} \in \mathfrak{A}$ and $F, f \in \mathscr{R}$. The $\mathscr{R}$-closure of $\mathfrak{A}$ in $\mathfrak{M}$ is the minimal $\mathscr{R}$-closed subset of $\mathfrak{M}$ containing $\mathfrak{A}$, i.e.,

$$\langle\langle \mathfrak{A} \rangle\rangle_{\mathscr{R}} := \{F(\bar{c}, \bar{C}), f(\bar{c}, \bar{C}) \ : \ \bar{c}, \bar{C} \in \mathfrak{A} \text{ and } F, f \in \mathscr{R}\}.$$

We interpret $\mathscr{R}$-closed subsets of $\mathfrak{M}$ as substructures in the canonical way: the functions and relations of $\mathfrak{N}$ are the restriction of those of $\mathfrak{M}$. In the same way we define $\mathscr{P}_i$-closed sets in models of $\mathscr{P}_i$-*def*.

We say that $\mathfrak{N} \subseteq \mathfrak{M}$ is a Σ_i^p-elementary substructure of $\mathfrak{M}$, if for every Σ_i^p-formula φ and every $\bar{a}, \bar{A} \in \mathfrak{N}$

$$\mathfrak{N} \models \varphi(\bar{a}, \bar{A}) \Longrightarrow \mathfrak{M} \models \varphi(\bar{a}, \bar{A}).$$

We write $\mathfrak{N} \prec_{\Sigma_i^p} \mathfrak{M}$ if $\mathfrak{N}$ is a Σ_i^p-elementary substructure of $\mathfrak{M}$. A similar notation is used also for other classes of formulas.

LEMMA 3.1 (Definability of Skolem functions).

(i) *$\mathscr{R}$-closed substructures of models of Σ_0^p-comp are Σ_0^p-elementary (so, in particular, they are models of Σ_0^p-comp).*

(ii) *$\mathscr{P}_i$-closed substructures of models of $\mathscr{P}_i$-def are $\Sigma_i^p(\mathscr{P}_i)$-elementary (so, in particular, they are models of $\mathscr{P}_i$-def).*

PROOF. For (i), observe that first-order Skolem functions for Σ_0^p-formulas are in $\mathscr{R}$. The proof of (ii) when $i = 0$ is easy. For $i > 0$ it suffices to show that among

the $\mathscr{P}_i$-functions there are Skolem functions for $\Sigma_i^p(\mathscr{P}_i)$-formulas. I.e., for every $\Sigma_i^p(\mathscr{P}_i)$-formula φ there is a function F in $\mathscr{P}_i$ such that

$$\exists Y < |\bar{a}, \bar{A}|^p \varphi(\bar{a}, \bar{A}, Y) \to \varphi(\bar{a}, \bar{A}, F(\bar{a}, \bar{A})).$$

To see this we shall define a function F that, by binary search, produces the minimal (in the lexicographic order) set $Y < |\bar{a}, \bar{A}|^p$ satisfying $\varphi(\bar{a}, \bar{A}, Y)$. Let us define the function G by recursion in the following way (omitting parameters and bounds)

$$G(0, \bar{a}, \bar{A}) = \emptyset,$$

$$G(y+1, \bar{a}, \bar{A}) = \begin{cases} G(y, \bar{a}, \bar{A}) \text{ if } (\exists Y < |\bar{a}, \bar{A}|^p) \bigwedge \begin{cases} G(y, \bar{a}, \bar{A}) \cap [y] = Y \cap [y] \\ \varphi(\bar{a}, \bar{A}, Y) \\ y \notin Y \end{cases} \\ G(y, \bar{a}, \bar{A}) \cup \{y\} \text{ otherwise} \end{cases}$$

(recall that $\mathscr{P}_i$ is closed under definition by $\Sigma_i^p(\mathscr{P}_i)$-cases since it contains the characteristic functions of Σ_i^p-formulas and is closed under composition). Finally, we define

$$F(\bar{a}, \bar{A}) = G(|\bar{a}, \bar{A}|^p).$$

We leave to the reader the verification that F produces a witness of $(\exists Y < |\bar{a}, \bar{A}|^p)$ $\varphi(\bar{a}, \bar{A}, Y)$, if one exists, and is $\emptyset$ otherwise. ⊣

The class of $\mathscr{P}_i$-functions is closed under Σ_i^p-definition by cases, so, an easy compactness argument proves the following witnessing theorem for $\mathscr{P}_i$-*def*.

COROLLARY 3.1 (Witnessing theorem for $\mathscr{P}_i$-*def*). *Each* $\forall \exists \Sigma_{i+1}^p$ *sentence provable in* $\mathscr{P}_i$-*def has a witnessing function in* $\mathscr{P}_i$.

PROOF. We have to prove that, for all $\varphi \in \Sigma_{i+1}^p$, there is a function F in $\mathscr{P}_i$ such that

$$\mathscr{P}_i\text{-}def \vdash \forall \bar{X}, \bar{x}\, \exists Y \varphi(\bar{x}, \bar{X}, Y) \Longrightarrow \mathscr{P}_i\text{-}def \vdash \forall \bar{X}, \bar{x}\, \varphi(\bar{x}, \bar{X}, F(\bar{x}, \bar{X})).$$

By contraction of quantifiers it suffices to show that the implication above holds for Π_i^p-formulas. So, let φ be a Π_i^p-formula such that for no $F \in \mathscr{P}_i$

$$(*) \qquad \mathscr{P}_i\text{-}def \vdash \forall \bar{X}, \bar{x}\, \varphi(\bar{x}, \bar{X}, F(\bar{x}, \bar{X})).$$

Let $\bar{c}, \bar{C}$ be fresh constants and consider the theory

$$(**) \qquad \mathscr{P}_i\text{-}def + \{\neg \varphi(\bar{c}, \bar{C}, F(\bar{c}, \bar{C})) \,:\, F \in \mathscr{P}_i\}.$$

This theory is consistent. Otherwise by compactness, for a finite set of functions $\{F_1, \ldots, F_n\}$ in $\mathscr{P}_i$,

$$\mathscr{P}_i\text{-}def \vdash \forall \bar{x}, \bar{X} \left[\varphi(\bar{x}, \bar{X}, F_1(\bar{x}, \bar{X})) \vee \cdots \vee \varphi(\bar{x}, \bar{X}, F_n(\bar{x}, \bar{X}))\right].$$

So, since $\mathscr{P}_i$-functions are closed under definition by Σ_i^p-cases, one can combine $F_1, \ldots, F_n$ together to find a function $F \in \mathscr{P}_i$ satisfying (*). Now, choose a model $\mathfrak{M}$ of the theory (**) and let $\mathfrak{N}$ be the $\mathscr{P}_i$-closure of $\bar{c}, \bar{C}$. By the previous lemma $\mathfrak{N}$ is a model of $\mathscr{P}_i$-*def*. The same lemma excludes the possibility of having in $\mathfrak{N}$ a set

Y such that $\varphi(\bar{c}, \bar{C}, Y)$. Thus $\mathscr{P}_i$-*def* does not prove $\forall \bar{x}, \bar{X}\, \exists Y \varphi(\bar{x}, \bar{X}, Y)$ and the corollary follows. ⊣

3.2. A model-theoretical version of Buss' witnessing theorem. We derive our version of Buss' witnessing theorem from the following lemma.

LEMMA 3.2. *Every model $\mathfrak{M}$ of $\mathscr{P}_i$-def has an $\exists\Sigma^p_{i+1}$-elementary extension to a model $\mathfrak{N}$ of Σ^p_{i+1}-comp such that for every Π^p_i-formula φ there is a function $F \in \mathscr{P}_i$ with (undisplayed) parameters from $\mathfrak{N}$ such that (*) below holds*

$$(*) \qquad \mathfrak{N} \models \forall X\, \exists Y \varphi(X, Y) \to \forall X\, \varphi(X, F(X)).$$

PROOF. We claim that, if we succeed in satisfying condition (*), we obtain also that $\mathfrak{N}$ models Σ^p_{i+1}-*comp*. To prove the claim it is sufficient to check that in $\mathfrak{N}$ the schema of dependent choices holds for Π^p_i-formulas. Assume that $\forall x \forall X \exists Y\, \varphi(x, X, Y)$ holds in $\mathfrak{N}$ and that a bound b on X and Y is implicit in φ. Let $a \in \mathfrak{N}$. We want to find a Z such that $(\forall x < a)\ \varphi(x, Z^{[x]}, Z^{[x+1]})$. By (*), for some $F \in \mathscr{P}_i$ and for all x and X, $\varphi(x, X, F(x, X))$. Define the following function G by second-order recursion (F can be bounded by b):

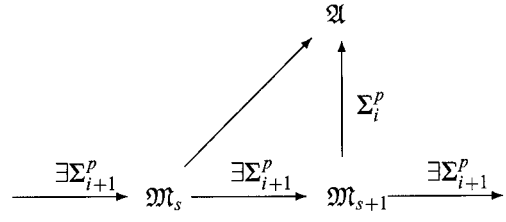
$$G(0) = \emptyset,\ G(x+1) = F(x+1,\ G(x)).$$

Finally, Z is obtained by rudimentary collection: $\bigcup_{x<a+1}\{x\} \times G(x)$. This proves our claim.

Now, let $\mathfrak{M}$ be a model of $\mathscr{P}_i$-*def*. The required model $\mathfrak{N}$ is constructed as the union of an $\exists\Sigma^p_{i+1}$-elementary chain of models of $\mathscr{P}_i$-*def*,

$$\mathfrak{M} = \mathfrak{M}_0 \prec_{\exists\Sigma^p_{i+1}} \mathfrak{M}_1 \prec_{\exists\Sigma^p_{i+1}} \mathfrak{M}_2 \prec_{\exists\Sigma^p_{i+1}} \cdots.$$

The chain is constructed by stages. Each link of the chain is constructed using a model $\mathfrak{A}$ as an intermediate step, as in the following diagram



Suppose $\mathfrak{M}_s$ has already been constructed. Let φ_s be the s-th Π^p_i-formula of an enumeration (to be specified below) of Π^p_i-formulas with parameters in $\mathfrak{M}_s$. Let $(*)_s$ be (*) with φ_s for φ. We shall construct a model $\mathfrak{M}_{s+1}$ realizing $(*)_s$ for some function $F \in \mathscr{P}_i$. Observe $(*)_s$ is a $\exists\forall\Pi^p_{i+1}$-formula, so, its truth is preserved upwards in the chain and finally inherited by the union $\mathfrak{N}$. It is easy to choose the enumeration such that eventually all Π^p_i-formulas with parameters in $\mathfrak{N}$ are considered. The details of the enumeration are as follows. At each stage s we fix an arbitrary enumeration $\{\psi^s_t\}_{t\in\omega}$ of all Π^p_i-formulas with parameters in $\mathfrak{M}_s$. Finally, let φ_s be ψ^r_t for $s = \langle r, t\rangle$. To define $\mathfrak{M}_{s+1}$ proceed as follows. If $(*)_s$ holds for φ_s, we do nothing, i.e., we define $\mathfrak{M}_{s+1} := \mathfrak{M}_s$. Otherwise, we try to make the antecedent

of $(*)_s$ false in $\mathfrak{M}_{s+1}$. We construct $\mathfrak{M}_{s+1}$ and $C \in \mathfrak{M}_{s+1}$ where $\exists Y \varphi_s(C, Y)$ fails. Since $(*)_s$ does not hold in $\mathfrak{M}_s$, the following theory has a model $\mathfrak{A}$

$$Diag(\mathfrak{M}_s) + \{\neg\varphi_s(C, F(C)) \,:\, F \in \mathscr{P}_i \text{ with parameters in } \mathfrak{M}_s\},$$

where C is a fresh constant and $Diag(\mathfrak{M}_s)$ is the elementary diagram of $\mathfrak{M}_s$ (to check the consistency, argue by compactness). $\mathfrak{A}$ is elementary equivalent to $\mathfrak{M}_s$, so, in particular, it is a model of $\mathscr{P}_i$-*def*. Define

$$\mathfrak{M}_{s+1} := \langle\langle \mathfrak{M}_s + C \rangle\rangle_{\mathscr{P}_i}.$$

Closure to be taken in $\mathfrak{A}$. Clearly, $\mathfrak{M}_{s+1}$ is a Σ_i^p-elementary substructure of $\mathfrak{A}$ which is elementary equivalent to $\mathfrak{M}_s$, so, every $\exists\Sigma_{i+1}^p$-formula true in $\mathfrak{M}_{s+1}$ will be true in $\mathfrak{A}$ and hence in $\mathfrak{M}_s$. In $\mathfrak{M}_{s+1}$ there is no witness of $\exists Y \varphi_s(C, Y)$. This completes the proof of the lemma. ⊣

COROLLARY 3.2 ($\forall\exists\Sigma_{i+1}^p$-conservation and witnessing theorem for Σ_{i+1}^p-*comp*). Σ_{i+1}^p-*comp is* $\forall\exists\Sigma_{i+1}^p$-*conservative over* $\mathscr{P}_i$-*def, therefore every* $\forall\exists\Sigma_{i+1}^p$ *sentence provable in* Σ_{i+1}^p-*comp has a witnessing function in* $\mathscr{P}_i$.

PROOF. Immediate from the previous lemma and from Lemma 3.1. ⊣

3.3. A model theoretical characterization of choice. We now introduce the concept of $\mathscr{R}$-extension. This is an extension where all second-order objects are constructible relative to the extended model. This notion may be viewed also as a second-order generalization of cofinal extension. It will be used to give a model theoretical characterization of Σ_{i+1}^p-*choice* over Σ_i^p-*comp*. An useful application of this notion is given in the proof of the corollary below. (The conservativity result in Corollary 3.3 (b) will find applications in the following sections to characterize the collapse of *BA*.)

Let $\mathfrak{M}$ and $\mathfrak{N}$ be models of Σ_0^p-*comp*. Recall that their first-order parts are denoted respectively by $\mathfrak{m}$ and $\mathfrak{n}$. We say that $\mathfrak{N}$ is an $\mathscr{R}$-**extension** of $\mathfrak{M}$ if

(o) $\mathfrak{M} \prec_{\Sigma_0^p} \mathfrak{N}$.
(i) $\mathfrak{m}$ is cofinal in $\mathfrak{n}$, i.e., for all $a \in \mathfrak{N}$ there is $b \in \mathfrak{M}$, such that $a < b$.
(ii) $\mathfrak{N} = \langle\langle \mathfrak{M} + \mathfrak{n} \rangle\rangle_{\mathscr{R}}$, i.e., for every $A \in \mathfrak{N}$ there are $a \in \mathfrak{N}$ such that $\mathfrak{N} \models A = F(a)$ for some $F \in \mathscr{R}$ with parameters in $\mathfrak{M}$.

We write $\mathfrak{M} \prec_{\mathscr{R}} \mathfrak{N}$ if $\mathfrak{N}$ is an $\mathscr{R}$-extension of $\mathfrak{M}$.

FACT 3.3. Let $\mathfrak{N}$ be an $\mathscr{R}$-extension of $\mathfrak{M}$.
(a) $\mathfrak{M} \prec_{\exists\Sigma_1^p} \mathfrak{N}$.
(b) $\mathfrak{M} \models \Sigma_{i+1}^p$-*choice* $\Longrightarrow \mathfrak{M} \prec_{\exists\Sigma_{i+2}^p} \mathfrak{N}$.
(c) $\mathfrak{M} \models \Sigma_i^p$-*comp* $\iff \mathfrak{N} \models \Sigma_i^p$-*comp*.
(d) $\mathfrak{M} \models \mathscr{P}_i$-*def* $\iff \mathfrak{N} \models \mathscr{P}_i$-*def*.

PROOF OF (a). If $\mathfrak{N} \models \exists Y \varphi(Y)$ for some Σ_0^p-formula φ with parameters in $\mathfrak{M}$, then for some $b \in \mathfrak{M}$, and some $F \in \mathscr{R}$ with parameters in $\mathfrak{M}$

$$\mathfrak{N} \models (\exists x < b)\varphi(F(x)),$$

so, by Σ_0^p-elementarity, this holds in $\mathfrak{M}$ too. This proves (a).

PROOF OF (b). Let $\mathfrak{M}$ be a model of Σ^p_{i+1}-*choice*. Let $a \in \mathfrak{M}$ and $\varphi \in \Sigma^p_i$ with parameters in $\mathfrak{M}$ and suppose $\mathfrak{N} \models \exists Y(\forall X < a)\varphi(X, Y)$. It suffices to show that the same formula holds in $\mathfrak{M}$ too. As induction hypothesis we assume $\exists\Sigma^p_{i+1}$-elementarity. Since $\mathfrak{N}$ is an $\mathscr{R}$-extension, for some $F \in \mathscr{R}$ with parameters in $\mathfrak{M}$, and some $b \in \mathfrak{M}$

$$\mathfrak{N} \models (\exists x < b)(\forall X < a)\varphi(X, F(x)).$$

Then, clearly,

$$\mathfrak{N} \models (\forall Z \subseteq \langle a, b\rangle)(\exists x < y)\varphi(Z^{[x]}, F(x)).$$

So, by $\exists\Sigma^p_{i+1}$-elementarity,

$$\mathfrak{M} \models (\forall Z \subseteq \langle a, b\rangle)(\exists x < y)\varphi(Z^{[x]}, F(x)).$$

Finally, by Σ^p_{i+1}-*choice*,

$$\mathfrak{M} \models (\exists x < b)(\forall X < a)\varphi(X, F(x)).$$

This proves (b).

PROOF OF (c). The 'left to right' direction of Fact (c) is true by definition when $i = 0$. For $i > 0$ it follows from (b) and Lemma 2.6. In fact, these imply that $\mathfrak{N}$ is an $\exists\Sigma^p_{i+1}$-elementary extension of $\mathfrak{M}$. So, let φ be any Σ^p_i-formula with parameters in $\mathfrak{N}$. By (ii), we can assume that all second-order parameters of φ belong to $\mathfrak{M}$. Let $\bar{c}$ be all first-order parameters occurring in φ and let $a \in \mathfrak{N}$ be arbitrary. Choose in $\mathfrak{M}$ a $b > a, \bar{c}$. Since $\mathfrak{M} \models \Sigma^p_i$-*comp* there is a set $A \in \mathfrak{M}$ such that

$$\mathfrak{M} \models (\forall x, \bar{y} < b)[\langle x, \bar{y}\rangle \in A \leftrightarrow \varphi(x, \bar{y})]$$

where the variables $\bar{y}$ are substituted for $\bar{c}$ in φ. By $\exists\Sigma^p_{i+1}$-elementarity, A satisfies the same property in $\mathfrak{N}$ too. So, in $\mathfrak{N}$ the set $B := \{x < a : \langle x, \bar{c}\rangle \in A\}$ verifies,

$$\mathfrak{N} \models (\forall x < a)[x \in B \leftrightarrow \varphi(x, \bar{c})].$$

This proves that $\mathfrak{N}$ is a model of Σ^p_i-*comp*.

The converse direction ('right to left') is also true by definition when $i = 0$. So, assume it true for i and let us prove it for $i + 1$. Let $\mathfrak{N}$ be a model of Σ^p_{i+1}-*comp*. By induction hypothesis, $\mathfrak{M}$ is a model of Σ^p_i-*comp* and, by Fact (b) and Lemma 2.6, a $\exists\Sigma^p_{i+1}$-elementary substructure of $\mathfrak{N}$. Let $\varphi(x, Y)$ be a Π^p_i-formula with parameters in $\mathfrak{M}$ such that $\exists Y\varphi(x, Y)$ is Σ^p_{i+1}. It suffices to find in $\mathfrak{M}$ a set A such that

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

By Lemma 2.6, $\mathfrak{N}$ models Σ^p_{i+1}-*coll*, so, for some set Z

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

Then, for some $b \in \mathfrak{N}$ and function $F \in \mathfrak{N}$ with parameters in $\mathfrak{M}$,

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

Consider, in $\mathfrak{M}$, the set $A := \{x < a : \exists y\ \varphi(x, F(y)^{[x]})\}$. We claim this is the required one. We only need to show that $(\forall x < a)[\exists Y\varphi(x, Y) \to x \in A]$, because the converse implication is obvious. If $\exists Y\varphi(x, Y)$ holds in $\mathfrak{M}$ for some $x < a$,

then this will be also true in the Σ_i^p-elementary extension $\mathfrak{N}$. Then $\exists y\ \varphi(x, F(y)^{[x]})$ holds in $\mathfrak{N}$ and, again by Σ_i^p-elementarity, is true in $\mathfrak{M}$ too. Therefore $x \in A$.

PROOF OF (d).

To prove the 'left to right' direction we use Lemma 3.2. This lemma characterizes models of $\mathscr{P}_i$-*def* as those having an $\exists\Sigma_{i+1}^p$-elementary extension to a model $\mathfrak{C}$ of Σ_{i+1}^p-*comp*. So, it suffices to show that there exists a model $\mathfrak{A}$ satisfying the following diagram of (restricted) elementary extensions

$$\begin{array}{ccc} \mathfrak{M} & \xrightarrow{\exists\Sigma_{i+1}^p} & \mathfrak{C} \models \Sigma_{i+1}^p\text{-}comp \\ \Big\downarrow \mathscr{R} & & \Big\downarrow \\ \mathfrak{N} & \xrightarrow{\exists\Sigma_{i+1}^p} & \mathfrak{A}. \end{array}$$

Consider the theory $Diag(\mathfrak{C}) + Diag_{\Pi_{i+1}^p}(\mathfrak{N})$. This theory has a model. Otherwise, suppose that for some $\varphi \in \Sigma_i^p$,

$$\forall X\varphi(X, \bar{c}) \in Diag_{\Pi_{i+1}^p}(\mathfrak{N}) \text{ and } Diag(\mathfrak{C}) \vdash \neg\forall X\varphi(X, \bar{c})$$

where we assume that a bound on X is implicit in φ. Since $\mathfrak{M} \prec_{\mathscr{R}} \mathfrak{N}$, we can assume that all other parameters of φ except $\bar{c}$ are in $\mathfrak{M}$. Let $a \in \mathfrak{M}$ be such that $\bar{c} < a$. Replacing the constants $\bar{c} \notin \mathfrak{C}$ with variables and quantifying we obtain

$$\mathfrak{C} \models (\forall \bar{x} < a)\exists X\neg\varphi(X, \bar{x}).$$

We may apply Σ_{i+1}^p-*choice* to get,

$$\mathfrak{C} \models \exists Z(\forall \bar{x} < a)\neg\varphi(Z^{[\bar{x}]}, \bar{x})$$

so, by $\exists\Sigma_{i+1}^p$-elementarity,

$$\mathfrak{M} \models \exists Z(\forall \bar{x} < a)\neg\varphi(Z^{[\bar{x}]}, \bar{x}).$$

Recall that $\mathfrak{M}$ models Σ_i^p-*comp*, so, by (b), $\mathscr{R}$-extensions of $\mathfrak{M}$ are $\exists\Sigma_{i+1}^p$-elementary. So,

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

Therefore,

$$\mathfrak{N} \models (\forall \bar{x} < a)\exists X\neg\varphi(X, \bar{x}).$$

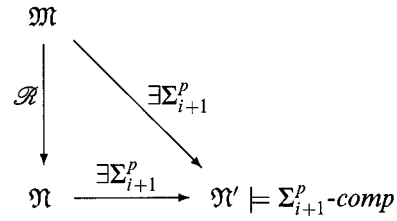
A contradiction since we assumed that $\forall X\varphi(X, \bar{c}) \in Diag_{\Pi_{i+1}^p}(\mathfrak{N})$.

Let $\mathfrak{A}'$ be a model of the theory above and let

$$\mathfrak{A} := \{a, A \in \mathfrak{A}' : a, A < b \text{ for some } b \in \mathfrak{M}\}.$$

Clearly $\mathfrak{A}'$ is a model of Σ_{i+1}^p-*comp* and consequently also $\mathfrak{A}$. To prove $\mathfrak{N} \prec_{\exists\Sigma_{i+1}^p} \mathfrak{A}$, it suffices to observe that $\mathfrak{N} \prec_{\Sigma_{i+1}^p} \mathfrak{A}'$, that $\mathfrak{A} \prec_{PH} \mathfrak{A}'$ and that $\mathfrak{N}$ is cofinal in $\mathfrak{A}$. This proves the left to right direction of (d).

For the converse, assume $\mathfrak{N}$ is a model of $\mathscr{P}_i$-*def*. By Lemma 3.2, there is a model $\mathfrak{N}'$ such that



where the diagonal arrow follows from (a) and (b) since, by (c), $\mathfrak{M}$ is a model of Σ^p_i-*comp*. ⊣

LEMMA 3.3. *Every model $\mathfrak{M}$ of Σ^p_i-comp has an $\mathscr{R}$-extension to a model N of Σ^p_{i+1}-choice.*

PROOF. The proof is similar to that of Lemma 3.2. The model $\mathfrak{N}$ is constructed as the union of a chain

$$\mathfrak{M} = \mathfrak{M}_0 \prec_{\mathscr{R}} \mathfrak{M}_1 \prec_{\mathscr{R}} \mathfrak{M}_2 \prec_{\mathscr{R}} \cdots .$$

By the fact above, we actually construct a $\exists\Sigma^p_{i+1}$-elementary chain of models of Σ^p_i-*comp*. Let $\{\varphi_s\}_s \in \omega$ be an enumeration with infinitely many repetitions of all formulas with parameters in $\mathfrak{N}$, such that all parameters of φ_s are in $\mathfrak{M}_s$ (see Theorem 3.2 for details on this enumeration). The chain is constructed so that for all $\varphi_s \in \Pi^p_i$, either (1) or (2) below holds.

(1) For every $a \in \mathfrak{M}$ there is a $Z \in \mathfrak{M}$ such that $\mathfrak{M}_s \models (\forall x < a)\varphi_s(x, Z^{[x]})$.

(2) There is a $c \in \mathfrak{M}_{s+1}$ such that $\mathfrak{M}_{s+1} \models \forall Y \neg\varphi_s(c, Y)$.

Each link of the chain is constructed using a model $\mathfrak{A}$ as an intermediate step, as in the proof of Lemma 3.2. Suppose $\mathfrak{M}_s$ has already been constructed. If (1) holds in $\mathfrak{M}_s$ then let $\mathfrak{M}_{s+1} := \mathfrak{M}_s$. Otherwise, let $\mathfrak{A}$ be any model of

$$Diag(\mathfrak{M}_s) + (c < a) + \{\neg\varphi_s(c, F(c)) \ : \ F \in \mathscr{R} \text{ with parameters in } \mathfrak{M}\}.$$

Such a model exists, otherwise, for some n

$$\mathfrak{M}_s \models (\forall x < a) \bigvee_{m=0}^{n} \varphi_s(x, F_m(x)).$$

Using Σ^p_i-*comp* one can define a set Z in $\mathfrak{M}_s$ such that for all $x < a$,

$$Z^{[x]} = F_m(x) \text{ for the minimal } m < n \text{ such that } \varphi_s(x, F_m(x)) \text{ holds.}$$

But we assumed such a set does not exist.

Clearly $\mathfrak{A}$ is, up to isomorphism, an elementary superstructure of $\mathfrak{M}_s$. Let $\mathfrak{M}_{s+1} := \langle\langle \mathfrak{M} + c \rangle\rangle_{\mathscr{R}}$ (closure to be taken in $\mathfrak{A}$). To check that $\mathfrak{M}_s \prec_{\mathscr{R}} \mathfrak{M}_{s+1}$ note that $\mathfrak{M}_{s+1}$ is a Σ^p_0 substructure of $\mathfrak{A}$. Also, observe that all elements of $\mathfrak{M}_{s+1}$ are generated by elements of $\mathfrak{M}_s$ and the first-order element $c < a$, so, conditions (o), (i) and (ii) in the definition of $\mathscr{R}$-extension are fulfilled.

To check that (2) holds, suppose not, for a contradiction. If $\exists Y\varphi_s(c, Y)$ held in $\mathfrak{M}_{s+1}$, then we would have $\varphi_s(c, F(c))$ for some $F \in \mathscr{R}$ with parameters in $\mathfrak{M}_{s+1}$. We will reach a contradiction by showing that instead $\varphi_s(c, F(c))$ must fail in $\mathfrak{M}_{s+1}$.

By construction, we have $\neg\varphi_s(c, F(c))$ in $\mathfrak{A}$. To pull this back to $\mathfrak{M}_{s+1}$ we reason as follows. Since $\mathfrak{M}_s$ is a model of Σ_i^p-*comp*, for some $A \in \mathfrak{M}_s$,

$$(\forall x < a)[x \in A \leftrightarrow \varphi_s(x, F_n(x))].$$

So, by the elementary equivalences proved above, this holds also in $\mathfrak{A}$ and in $\mathfrak{M}_{s+1}$. In $\mathfrak{A}$ we have $c \notin A$ and, by Σ_0^p equivalence this holds in $\mathfrak{M}_{s+1}$. So, $\neg\varphi_s(c, F(c))$, a contradiction.

Finally, $\mathfrak{N}$ is a model of Σ_{i+1}^p-*choice*, since the truth of both formulas in (1) and in (2) is preserved along the $\exists\Sigma_{i+1}^p$-chain. ⊣

Now we can easily prove the characterization announced above.

THEOREM 3.3. *For every* $\mathfrak{M} \models \Sigma_i^p$-*comp the following are equivalent*

(i) $\mathfrak{M} \models \Sigma_{i+1}^p$-*choice.*

(ii) *Every* $\mathscr{R}$-*elementary extension of* $\mathfrak{M}$ *is* $\exists\Sigma_{i+2}^p$-*elementary.*

PROOF. That (i) implies (ii) has already been observed in the fact above. For the converse, let $\varphi \in \Pi_i^p$ and suppose that $(\forall x < a)(\exists Y < b)\varphi(x, Y)$ holds in $\mathfrak{M}$. Let $\mathfrak{N}$ be the $\mathscr{R}$-elementary extension of $\mathfrak{M}$ to a model of Σ_{i+1}^p-*choice*. The existence of $\mathfrak{N}$ is guaranteed by the lemma above. By $\exists\Sigma_{i+2}^p$-elementarity, $(\forall x < a)(\exists Y < b)\varphi(x, Y)$ holds also in $\mathfrak{N}$. Let Z in $\mathfrak{N}$ be such that $(\forall x < a)\varphi(x, Z^{[x]})$. By the definition of $\mathscr{R}$-extension,

$$\mathfrak{N} \models (\exists y < c)(\forall x < a)\varphi(x, F(y)^{[x]})$$

for some $c \in \mathfrak{M}$ and some $F \in \mathscr{R}$ with parameters in $\mathfrak{M}$. So, by $\exists\Sigma_{i+2}^p$-elementarity this formula holds also in $\mathfrak{M}$. ⊣

The following conservativity results are consequences of the lemma above.

COROLLARY 3.3.

(a) Σ_{i+1}^p-*choice is* $\forall\exists\Sigma_{i+1}^p$-*conservative over* Σ_i^p-*comp.*

(b) $\mathscr{P}_i$-*def* $+ \Sigma_{i+1}^p$-*choice* $\vdash \Sigma_{i+1}^p$-*comp* $\Longrightarrow \mathscr{P}_i$-*def* $\vdash \Sigma_{i+1}^p$-*comp.*

(c) Σ_{i+1}^p-*choice* $\vdash \Sigma_{i+1}^p$-*comp* $\Longrightarrow \Sigma_i^p$-*comp* $\vdash \Sigma_{i+1}^p$-*comp.*

PROOF. (a) follows from the lemma and Fact (b) above. The proof of (b) and (c) are similar. Let us prove (b). Assume $\mathscr{P}_i$-*def* $+ \Sigma_{i+1}^p$-*choice* proves Σ_{i+1}^p-*comp*. Let $\mathfrak{M}$ be any model of $\mathscr{P}_i$-*def*. In particular, $\mathfrak{M}$ is a model of Σ_i^p-*comp*, so, by the lemma above, it has an $\mathscr{R}$-extension $\mathfrak{N}$ to a model of Σ_{i+1}^p-*choice*. By Fact (d) above, $\mathfrak{N}$ is also a model of $\mathscr{P}_i$-*def*. So, by our assumption, $\mathfrak{N}$ models Σ_{i+1}^p-*comp*. By Fact (c) above, $\mathfrak{M}$ is also a model of Σ_{i+1}^p-*comp*. ⊣

§4. The collapse of *BA* versus the collapse of *PH*. It is not known whether *BA* collapses, i.e., whether it is equal to some of its fragments. The only collapse that we are able to exclude is Σ_1^p-*choice* $= \mathscr{P}$-*def*. In fact, rudimentary functions $\mathscr{R}$ are the only functions with a Σ_1^p graph that are provably total in Σ_1^p-*choice*; a simple diagonalization argument shows these are strictly included in the polynomial time computable functions $\mathscr{P}$. Actually, one can also see that the $\forall\Sigma_0^p$ fragment of $\mathscr{P}$-*def* strictly includes that of Σ_0^p-*comp* (and, by conservativity, that of Σ_1^p-*choice*). In fact, in [2] Ajtai has constructed a model $\mathfrak{m}$ of $I\Delta_0(R)$ such that

$$\mathfrak{m} \models \exists x\, R : [x] \hookrightarrow [x + 1],$$

i.e., R is an injection of $[x]$ into $[x+1]$. We can expand $\mathfrak{m}$ to a model $\mathfrak{M}$ of Σ_0^p-*comp* taking as sets of $\mathfrak{M}$ the finite $\Delta_0(R)$-definable sets of $\mathfrak{m}$. Then $\mathfrak{M}$ falsifies the pigeonhole principle, i.e., the sentence

$$\forall X \ : \ \forall x \neg X : [x+1] \hookrightarrow [x],$$

while the sentence above is easily seen to be provable in $\mathscr{P}$-*def*.

For stronger fragments we can only produce relativized results. The main result of this section is to prove that the collapse of *BA* is equivalent to the provable collapse of *PH*.

4.1. An interpolation theorem. The following is the 'bounded version' of a general interpolation theorem for classical predicate logic. It entails that formulas which are both $\forall\Pi_{i+2}^p$ and $\exists\Sigma_{i+2}^p$ over a $\forall\Pi_{i+2}^p$ theory are actually provably equivalent to a Boolean combination of Σ_{i+1}^p formulas.

THEOREM 4.1. *Let φ and ψ be $\forall\Pi_{i+2}^p$-formulas and let T be a $\forall\Pi_{i+2}^p$-axiomatized theory. If $T \vdash \varphi \to \neg\psi$ then there is a Boolean combination β of Σ_{i+1}^p-formulas such that, $T \vdash \varphi \to \beta$ and $T \vdash \beta \to \neg\psi$. Moreover all free variables of β occur free in $\varphi \to \neg\psi$.*

PROOF. Let φ and ψ be as above and suppose that the required interpolant does not exist. We intend to show that $T + \varphi + \psi$ is consistent. (When the context suggests it, the free variables of $\varphi \to \neg\psi$ need to be replaced by fresh constants.) To show this, it is sufficient to show that there are two $\forall\Pi_{i+2}^p$-theories $U \supseteq T + \varphi$ and $V \supseteq T + \psi$ such that U and V have the same $\forall\Sigma_i^p$-consequences (we say also that they are mutually $\forall\Sigma_i^p$-conservative). In fact, we claim that, for any pair U and V of mutually $\forall\Sigma_i^p$-conservative theories which are $\forall\Pi_{i+2}^p$-axiomatizable, $U + V$ is consistent (and, actually, also has the same $\forall\Sigma_i^p$-consequences). Let us first prove this claim and then proceed to the construction of U and V. We construct a Σ_i^p-elementary chain of models,

$$\mathfrak{M}_0 \prec_{\Sigma_i^p} \mathfrak{M}_1 \prec_{\Sigma_i^p} \dots,$$

such that $\mathfrak{M}_{2s}$ is a model of U and $\mathfrak{M}_{2s+1}$ is a model of V. It is possible to find $\mathfrak{M}_{2s+1}$ and $\mathfrak{M}_{2s+2}$ such that

$$\mathfrak{M}_{2s+1} \models \mathit{Diag}_{\Pi_i^p}(\mathfrak{M}_{2s}) + V \text{ and } \mathfrak{M}_{2s+2} \models \mathit{Diag}_{\Pi_i^p}(\mathfrak{M}_{2s+1}) + U.$$

In fact, if we assume as induction hypothesis that $\mathfrak{M}_{2s}$ is a model of U, then V is consistent with the Π_i^p diagram of $\mathfrak{M}_{2s}$, otherwise, for some $\theta \in \Pi_i^p$

$$V \vdash \forall\bar{x}\bar{X}\neg\theta \text{ and } \mathfrak{M}_{2s} \models \exists\bar{x}\bar{X}\ \theta$$

which contradicts the $\forall\Sigma_i^p$-conservativity of V over U. The symmetric argument works for odd stages. Finally, recall that both U and V are $\forall\Pi_{i+2}^p$-theories (and hence conserved by unions of Σ_i^p-chains). So, the union of the chain

$$\mathfrak{N} := \bigcup_{s\in\omega} \mathfrak{M}_s = \bigcup_{s\in\omega} \mathfrak{M}_{2s} = \bigcup_{s\in\omega} \mathfrak{M}_{2s+1}$$

is a model of both U and V. This proves the claim.

Now we construct U and V. Let $\bar{X}$ be all free variables occurring in $\varphi \to \neg\psi$. Let $\mathscr{B}_{i+1}$ denote the class of formulas with free variables among $\bar{X}$ of the form $\forall Y\beta$ and such that $\forall Y < |\bar{X}|^p\beta$ (for $p \in \omega$) is a Boolean combination of Σ^p_{i+1}-formulas. Let us say that two theories U and V are $\mathscr{B}_{i+1}$ inseparable (in the following simply inseparable) if $V + Th_{\mathscr{B}_{i+1}}(U)$ is consistent. In other words, if there is no $\forall Y\beta \in \mathscr{B}_{i+1}$ such that $U \vdash \forall Y\beta$ and $V \vdash \neg\forall Y\beta$. Let $U_0 := T + \varphi$ and $V_0 := T + \psi$. If no interpolant exists, U_0 and V_0 are inseparable. In fact, suppose for a contradiction that

$$T + \varphi \vdash \forall Y\beta \text{ and } T + \psi \vdash \neg\forall Y\beta$$

where $\forall Y\beta$ is in $\mathscr{B}_{i+1}$. Since T is axiomatized by $\forall PH$ sentences, we can apply a well-known theorem of Parikh's, to find a $p \in \omega$ such that

$$T \vdash \forall \bar{X}\ [\psi \to \neg\forall Y < |\bar{X}|^p\beta].$$

Therefore $\forall Y < |\bar{X}|^p\beta$ would be an interpolant of φ and ψ of the required complexity. Now, we show, by induction on s that the following theories are inseparable:

$$U_{s+1} = U_s + Th_{\mathscr{B}_{i+1}}(V_s) \text{ and } V_{s+1} = V_s + Th_{\mathscr{B}_{i+1}}(U_s).$$

We have already shown the case $s = 0$. Suppose U_s and V_s are inseparable. If, for a contradiction, for some $\forall Y\beta$ in $\mathscr{B}_{i+1}$,

$$U_s + Th_{\mathscr{B}_{i+1}}(V_s) \vdash \forall Y\beta \text{ and } V_s + Th_{\mathscr{B}_{i+1}}(U_s) \vdash \neg\forall Y\beta$$

then, for some $\forall Z\beta' \in Th_{\mathscr{B}_{i+1}}(V_s)$,

$$U_s \vdash \forall Z\beta' \to \forall Y\beta.$$

Applying again Parikh's theorem, for some $p \in \omega$,

$$U_s \vdash \forall Y\ [\forall Z < |Y|^p\beta' \to \beta].$$

therefore,

$$\forall Y\ [\forall Z < |Y|^p\beta' \to \beta] \in Th_{\mathscr{B}_{i+1}}(U_s).$$

But $V_s \vdash \forall Z\beta'$, so, $V_s + Th_{\mathscr{B}_{i+1}}(U_s)$ is inconsistent. This contradicts our induction hypothesis. Finally, let $U := \bigcup_{s\in\omega} U_s$ and $V := \bigcup_{s\in\omega} V_s$. Clearly,

$$Th_{\mathscr{B}_{i+1}}(U) = Th_{\mathscr{B}_{i+1}}(V).$$

So, in particular, U and V have the same $\forall\Sigma^p_i$-consequences. ⊣

4.2. Sufficient conditions for the collapse of *BA*. Let us introduce some terminology. We say that a theory proves $\Pi_i^p = \Sigma_i^p$ if every Π_i^p-formula is provably equivalent to a Σ_i^p-formula (with the same free variables). In this case we also say that *PH* provably collapses to $\Pi_i^p = \Sigma_i^p$. We say that a theory proves $\Pi_{i+1}^p = \Sigma_{i+1}^p/poly$, if for every $\theta \in \Sigma_{i+1}^p$ there is a $\psi \in \Pi_{i+1}^p$ and $p \in \omega$ such that, provably

$$(\exists W < c^p)(\forall X < c)\Big[\theta(X) \leftrightarrow \psi(X, W)\Big].$$

(All variables are shown.) A W witnessing the existential quantifier above is usually called **(polynomial) advice**. Observe that, given any bounded formula $\varphi(X)$ and some element c of a model where $\Pi_{i+1}^p = \Sigma_{i+1}^p/poly$, there is a Σ_{i+1}^p-formula $\psi(X)$ equivalent to $\varphi(X)$ for all $X < c$. In general, such a ψ can contain extra parameters (i.e., advices which transform universal in existential quantifiers and vice versa). These parameters will depend on c. The following theorem is an interesting consequence of Lemma 3.2 and Lemma 3.3.

THEOREM 4.2. *The following are sufficient conditions for* $\mathscr{P}_i$*-def* $\vdash$ *BA*
(a) $\mathscr{P}_i$*-def* $+ \Sigma_{i+1}^p$*-choice* $\vdash \Pi_{i+2}^p = \Sigma_{i+2}^p$,
(b) $\mathscr{P}_i$*-def* $+ \Sigma_{i+1}^p$*-choice* $\vdash \Pi_{i+1}^p = \Sigma_{i+1}^p/poly$.

PROOF. By Corollary 3.3 (b), in both cases it is sufficient to show that $\mathscr{P}_i$*-def* $+$ Σ_{i+1}^p*-choice* proves *BA*. Let us prove (a). Every model $\mathfrak{M}$ of $\mathscr{P}_i$*-def* $+\Sigma_{i+1}^p$*-choice* has an $\exists\Sigma_{i+1}^p$-elementary extension to a model of Σ_{i+1}^p*-comp*. By the provable collapse of *PH* every bounded formula is equivalent both to a Π_{i+2}^p and to a Σ_{i+2}^p-formula. Therefore every $\exists\Sigma_{i+1}^p$-elementary extension is actually $\exists PH$-elementary. So $\mathfrak{M}$ is a model of Σ_{i+1}^p*-comp* too. By the interpolation lemma above every *PH*-formula is equivalent to a Boolean combination of Σ_{i+1}^p-formulas. For this class of formulas comprehension is provable in Σ_{i+1}^p*-comp*.

To prove (b) it suffices to note that the schema of choice holds for every bounded formula. In fact, as observed above, every bounded formula is provably equivalent to a Σ_{i+1}^p-formula depending on some additional parameters. ⊣

4.3. Necessary conditions for the collapse of *BA*. Here we show that if $\mathscr{P}_i$*-def* proves Σ_{i+1}^p*-comp* then it proves the collapse of *PH* and *BA* reduces to $\mathscr{P}_i$*-def*. We need the following lemma of [10] which is known as the KPT witnessing theorem.

LEMMA 4.3. *For every* $\varphi \in \Pi_i^p$ *if* $\mathscr{P}_i$*-def proves* $\forall X \exists Y \forall Z \varphi(X, Y, Z)$*, then there are* $F_0, \ldots, F_{n-1}$ *in* $\mathscr{P}_i$ *such that* $\mathscr{P}_i$*-def proves*

$$\forall X, Z_0, \ldots, Z_{n-1} \bigvee \begin{cases} \varphi(X, F_0(X), Z_0) \\ \varphi(X, F_1(X, Z_0), Z_1) \\ \ldots \\ \ldots \\ \varphi(X, F_{n-1}(X, Z_0, \ldots, Z_{n-2}), Z_{n-1}). \end{cases}$$

PROOF. Let $\{F_n\}_{n\in\omega}$ be an enumeration of all the functions in $\mathscr{P}_i$ with infinitely many repetitions. Let C, $\{D_n\}_{n\in\omega}$ be fresh constants. Consider the theory

$$\mathscr{P}_i\text{-}def + \{\neg\varphi(C, F_n(C, \bar{D}_n), D_n) \ : \ n \in \omega\}$$

where $\bar{D}_n$ stands for $D_1, \ldots, D_{n-1}$. If this theory is inconsistent, our claim follows by compactness. So, we suppose for a contradiction that this theory has a model. Let $\mathfrak{M}$ be the $\mathscr{P}_i$-closure of C, $\{D_n\}_{n\in\omega}$ in the model of the theory above. By Lemma 3.1, $\mathfrak{M}$ is a $\Sigma_i^p(\mathscr{P}_i)$-elementary substructure, so,

$$\mathfrak{M} \models \neg\varphi(C, F_n(C, \bar{D}_n), D_n).$$

But, in $\mathfrak{M}$, every possible witness of $\exists Y \forall Z \varphi(C, Y, Z)$ is of the form $F_n(C, \bar{D}_n)$. A contradiction. ⊣

For the next theorem we use ideas of [8] as we learned them from Harry Buhrman.

THEOREM 4.3. *$\mathscr{P}_i$-def $\vdash \Sigma_{i+1}^p$-comp $\Longrightarrow$ $\mathscr{P}_i$-def $\vdash \Pi_{i+1}^p = \Sigma_{i+1}^p/poly$.*

PROOF. Consider an arbitrary formula of the form $\exists Z\varphi(X, Z)$ for $\varphi \in \Pi_i^p$ where a bound on Z is implicit in φ. We shall find a formula $\psi \in \Pi_{i+1}^p$ such that $\mathscr{P}_i$-*def* proves

$$\exists W(\forall X < c)\left[\exists Z\varphi(X, Z) \leftrightarrow \psi(X, W)\right].$$

Since, by Lemma 2.6, Σ_{i+1}^p-*comp* is equivalent to Σ_{i+1}^p-*coll*, we can assume that $\mathscr{P}_i$-*def* proves the following sentence

$$\forall X \exists Y(\forall x < a)\left[\exists Z\varphi(X^{[x]}, Z) \to \varphi(X^{[x]}, Y^{[x]})\right].$$

This sentence says that for every sequence of sets $X^{[0]}, \ldots, X^{[a-1]}$ there is a sequence $Y^{[0]}, \ldots, Y^{[a-1]}$ coding witnesses, (when they exist) of $\exists Z\varphi(X^{[0]}, Z), \ldots, \exists Z\varphi(X^{[a-1]}, Z)$. So, assume this is provable in $\mathscr{P}_i$-*def*, move the quantifiers $\exists Z$ as far to the left as possible and apply the previous lemma to this formula. Fix $a = n$ and, for better readability, let us suppose $n = 2$.

$$\forall X, A, B \bigvee \begin{cases} (\forall x < 2)\left[\varphi(X^{[x]}, A) \to \varphi(X^{[x]}, F_1^{[x]}(X))\right] \\ (\forall x < 2)\left[\varphi(X^{[x]}, B) \to \varphi(X^{[x]}, F_2^{[x]}(X, A))\right]. \end{cases}$$

We can replace the universal quantifier $\forall x < 2$ with a conjunction. Also, to streamline notation, let us use two variables X, Y in place of $X^{[0]}$ and $X^{[1]}$ and introduce the functions F, G and H, K in place of the two components of F_1 and F_2. The formula above can be rewritten as $\forall X, Y, A\ \gamma(X, Y, A)$ where

$$\gamma(X, Y, A) :\equiv \bigvee \begin{cases} \bigwedge \begin{cases} \varphi(X, A) \to \varphi(X, F(X, Y)) \\ \varphi(Y, A) \to \varphi(Y, G(X, Y)) \end{cases} \\ \bigwedge \begin{cases} \exists B\varphi(X, B) \to \varphi(X, H(X, Y, A)) \\ \exists B\varphi(Y, B) \to \varphi(Y, K(X, Y, A)). \end{cases} \end{cases}$$

Let ξ stand for the first disjunct of γ, i.e., for the formula

$$\xi(X, Y, A) :\equiv \bigwedge \begin{cases} \varphi(X, A) \to \varphi(X, F(X, Y)) \\ \varphi(Y, A) \to \varphi(Y, G(X, Y)). \end{cases}$$

Now, we define the formula $\psi(X, W)$ to be

$$\bigvee \begin{cases} \varphi(X, F(X, W)) \\ c \in W \wedge (\forall Y < c)\, \forall A\, [\neg\xi(Y, X, A) \to \varphi(X, K(Y, X, A))]. \end{cases}$$

Recall that above we assumed that a polynomial bound for the quantifier $\forall A$ is implicit in φ. So, $\psi(X, W)$ is a Π^p_{i+1}-formula. To complete the proof we have to show that for every c there is advice W such that $\exists Y \varphi(X, Y) \leftrightarrow \psi(X, W)$ for every $X < c$. Let c be given, we proceed in a nonuniform way. We consider two possibilities.

(∘) Suppose there is a $Y < c$ such that $\xi(X, Y, A)$ holds for every $X < c$ and every A. Let $W = Y$. From $\xi(X, W, A)$ it follows that $\exists A \varphi(X, A)$ implies $\varphi(X, F(X, W))$ and so, $\psi(X, W)$. The converse is obvious: we have chosen a $W < c$, so the second disjunct is always false.

(∘∘) Suppose case (∘) does not obtain, i.e., (reversing the roles of X and Y) suppose for all X, $(\exists Y < c)\ \exists A\ \ \neg\xi(Y, X, A)$. We chose a W which informs us of this fact: $W = \{c\}$. If $\exists B \varphi(X, B)$ does not hold then in particular neither $\varphi(X, F(X, W))$ nor $\neg\varphi(X, K(Y, X, A))$ hold for any W, Y and A. So, $\psi(X, W)$ fails. Vice versa, assume $\exists B \varphi(X, B)$. For all Y and A such that $\neg\xi(Y, X, A)$, the second disjunct in $\gamma(Y, X, A)$ must be true. So, since $\exists B \varphi(X, B)$, we have $\varphi(X, K(Y, X, A))$. Thus the second disjunct of $\psi(X, W)$ holds.

This completes the proof under the condition $n = 2$. The general case is similar. One has to consider n cases in place of 2 and the advice W must inform of which case actually obtains for a given c. Details are left to the reader. ⊣

COROLLARY 4.3.

(a) $\mathscr{P}_i\text{-}def \vdash \Sigma^p_{i+1}\text{-}comp \Longrightarrow \mathscr{P}_i\text{-}def \vdash BA$

(b) $\mathscr{P}_i\text{-}def \vdash \Sigma^p_{i+1}\text{-}comp \Longrightarrow \mathscr{P}_i\text{-}def \vdash \Pi^p_{i+3} = \Sigma^p_{i+3}$.

PROOF. (a) follows immediately from Theorem 4.2 and the theorem above. To prove (b), we can assume that $\theta(A) \in \Pi^p_{i+3}$ has the form $(\forall X < c)(\exists Y < c)\varphi(X, Y, A)$ for some $\varphi \in \Pi^p_{i+1}$. We want a Σ^p_{i+3}-formula equivalent to $\theta(A)$ for every A. From $\Pi^p_{i+1} = \Sigma^p_{i+1}/poly$ we have that, provably in $\mathscr{P}_i\text{-}def$, for some $\psi \in \Sigma^p_{i+1}$, (omitting the bound on W)

$$\exists W (\forall X, Y, A < c) \left[\varphi(X, Y, A) \leftrightarrow \psi(X, Y, W, A)\right].$$

Note that the formula below that says that W is good advice for all $X, Y < c$,

$$(\forall X, Y, A < c) \left[\varphi(X, Y, A) \leftrightarrow \psi(X, Y, A, W)\right]$$

is Π^p_{i+2}. So, let $\zeta(W, A)$ stand for this formula. Provably in $\mathscr{P}_i\text{-}def$,

$$(\forall X < c)(\exists Y < c)\varphi(X, Y, A) \leftrightarrow \exists W [\zeta(W, A) \wedge (\forall X < c)(\exists Y < c)\psi(X, Y, W, A)].\dashv$$

4.4. Krajíček, Pudlák and Takeuti's method. Krajíček, Pudlák and Takeuti have shown in [10] that if $\mathscr{P}_i$-*def* proves Σ^p_{i+1}-*comp* then $\Sigma^p_{i+1} = \mathscr{P}_i/poly$ in the standard model (and hence $\Sigma^p_{i+2} = \Pi^p_{i+2}$). We show how their result can be obtained by sharpening the reasoning of the previous section. The combinatoral methods used in the following proof are of a more complex nature than those needed in the previous section. It is still unknown whether this proof can be formalized in *BA*.

We say that $\Sigma^p_{i+1} = \mathscr{P}_i/poly$ if for every Σ^p_{i+1}-formula $\exists Y\varphi(X, Y)$ there is a $\mathscr{P}_i$-function F such that for some $p \in \omega$,

$$(\exists W < c^p)(\forall X < c)\left[\exists Y\varphi(X, Y) \to \varphi(X, F(X, W))\right],$$

holds for every c.

THEOREM 4.4. *If* $\mathscr{P}_i$-*def* $+ \Sigma^p_{i+1}$-*choice* $\vdash \Sigma^p_{i+1}$-*comp then in the standard model* $\Sigma^p_{i+1} = \mathscr{P}/poly$.

PROOF. By Corollary 3.3 we can as well assume that $\mathscr{P}_i$-*def* $\vdash \Sigma^p_{i+1}$-*comp*. Let $\exists Y\varphi(X, Y)$ be in Σ^p_{i+1}. Reasoning as in the proof of Theorem 4.3 (so, assuming again that the KPT witnessing theorem holds with $n = 2$ for the formula under consideration) we obtain that the formula $\forall X, Y, A\ \gamma(X, Y, A)$ defined there is provable in $\mathscr{P}_i$-*def*. In particular, it holds in the standard model. For the rest of the argument let us work in ω. We say that X has information about Y if one of the following cases hold

(a) $\varphi(Y, F(Y, X))$,

(b) $\varphi(Y, K(X, Y, A))$, for all A such that $\varphi(X, A)$.

Observe that if X has information about Y, then knowing any witness of $\exists A\varphi(X, A)$ we can compute a witness of $\exists A\varphi(Y, A)$. Now, we claim that for any pair of sets $X, Y < c$ such that $\exists A\varphi(X, A)$ and $\exists A\varphi(Y, A)$ either X has information about Y or vice versa. To prove the claim, suppose X has no information about Y. In particular $\varphi(Y, F(Y, X))$ does not hold. Let A be any witness of $\exists A\varphi(Y, A)$ then, by $\gamma(Y, X, A)$, (the roles of X and Y are interchanged) $\exists B\varphi(X, B) \to \varphi(X, K(Y, X, A))$ must hold. Therefore, $\varphi(X, K(Y, X, A))$ follows, so, by (b), Y has information about X.

Consider now the class $\Omega = \{X < c : \exists A\varphi(X, A)\}$ and reason in the standard model. There is a $X \in \Omega$ such that X has information about at least half of the sets in Ω. To see this, let $i(X, Y)$ be 1 if X has information about Y, -1 otherwise. Then, by our claim above, $\sum_{X,Y\in\Omega} i(X, Y) = 0$, so, for some X in Ω, $\sum_{Y\in\Omega} i(X, Y) \geq 0$. Clearly such an X has information about at least half of the Y in Ω. Iterating the argument above, since Ω contains at most 2^c-elements, we obtain $W < \langle c, c\rangle$ such that $W^{[0]}, \ldots, W^{[c-1]}$ have information about all elements of Ω. Let V be such that $\varphi(W^{[i]}, V^{[i]})$ for $i = 0, \ldots, c-1$. Then, we have that for all $X < c$

$$\exists A\varphi(X, A) \leftrightarrow (\exists x < c)\left[\varphi(X, F(X, W^{[x]})) \vee \varphi(X, K(W^{[x]}, X, V^{[x]}))\right].$$

That is, for some function $F' \in \mathscr{P}_i$ and some W' coding W and V,

$$(\forall X < c)\left[\exists Y\varphi(X, Y) \leftrightarrow \varphi(X, F'(X, W'))\right].$$

Recall that we assumed that a bound on $\exists Y$ is implicit in φ so, the size of V can be bounded by some standard power of c. Hence $W' < c^p$ for some $p \in \omega$.

The general case (for $n > 2$) is similar. ⊣

REFERENCES

[1] M. AJTAI, Σ_1^1-*formulas on finite structures*, ***Annals of Pure and Applied Logic***, vol. 24 (1983), pp. 1–48.

[2] ———, *The complexity of the pigeonhole principle*, ***IEEE*** (1988), pp. 346–355.

[3] S. R. BUSS, ***Bounded arithmetic***, Bibliopolis, Naples, 1986.

[4] ———, *Axiomatizations and conservations results for fragments of bounded arithmetic*, ***Logic and computation***, Contemporary Mathematics, vol. 106, A.M.S., 1990, proceeding of a workshop held at Carnegie-Mellon University, 1987, pp. 57–84.

[5] ———, *Relating the bounded arithmetic and polynomial time hierarchies*, to appear.

[6] A. COBHAM, *The intrinsic computational difficulty of functions*, ***Structure in complexity theory*** (A. L. Selman, editor), Lecture Notes in Computational Science, vol. 221, 1986, pp. 125–146.

[7] P. HÁJEK and P. PUDLÁK, ***Metamathematics of first-order arithmetic***, Springer-Verlag, Berlin, 1993.

[8] J. KADIN, *The polynomial time hierarchy collapses if the Boolean hierarchy collapses*, ***IEEE*** (1988), pp. 278–292.

[9] J. KRAJÍČEK, *Exponentiation and second order bounded arithmetic*, ***Annals of Pure and Applied Logic***, vol. 48 (1990), pp. 261–276.

[10] J. KRAJÍČEK, P. PUDLÁK, and G. TAKEUTI, *Bounded arithmetic and the polynomial time hierarchy*, ***Annals of Pure and Applied Logic***, vol. 52 (1991), pp. 143–153.

[11] G. E. MINTS, *Quantifier-free and one-quantifier systems*, ***Zapiski Nauchnykh Seminarov***, vol. 20 (1971), pp. 115–133, in Russian. English translation: ***Journal of Soviet Mathematics***, vol. 1 (1973), pp. 211–266.

[12] J. B. PARIS and L. A. S. KIRBY, σ_n-*collection schemas in arithmetic*, ***Logic colloquium 77*** (A. Macintyre, L. Pacholski, and J. Paris, editors), North-Holland, Amsterdam, 1978, pp. 199–209.

[13] C. PARSONS, *On a number theoretic choice schema and its relation to induction*, ***Intuitionism and proof theory*** (Kino, Myhill, and Vesley, editors), North-Holland, Amsterdam, 1970, pp. 459–473.

[14] A. RAZBOROV, *An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic*, ***Arithmetic, proof theory and computational complexity*** (P. Clote and J. Krajíček, editors), Oxford University press, Oxford, 1993, pp. 247–277.

[15] G. TAKEUTI, *RSUV isomorphisms*, ***Arithmetic, proof theory and computational complexity*** (P. Clote and J. Krajíček, editors), Oxford University press, Oxford, 1993, pp. 364–386.

[16] A. J. WILKIE, *Modelès non standard de l'arithmétique et complexité algorithmique*, ***Modelès non standard de l'arithmétique et theorie des ensembles*** (A. J. Wilkie and J. Ressayre, editors), Publications Mathématique de l'Université Paris VII, Paris, 1983, pp. 1–45.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF AMSTERDAM
PLANTAGE MUIDERGRACHT 24
1018 TV AMSTERDAM
THE NETHERLANDS

E-mail: domenico@fwi.uva.nl