Notes on polynomially bounded arithmetic

Domenico Zambella

March 8, 1994

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

0 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 where all quantifiers are of the form $Qx<t$ or $QX<t$ where t is a term (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 fram 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. Interestingly, all provably recursive functions of BA are of polynomial growth. Some theorems of partial conservativity are proved for some of these theories and the connection with complexity theory is briefly discussed.

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 also well-known $I\Delta_0 + \Omega_1$. These theories are first-order strengthening of $I\Delta_0$. In the case of $I\Delta_0 + \Omega_1$ or S_2 the urge for the strengthenings 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 operations increases the code of the string superpolynomially and so, it is not provably total in $I\Delta_0$. Adding to $I\Delta_0$ an axiom (i.c., 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 theories are obtained by some 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 $\mathbf{M}'$ of S_2 corresponds a (second-order) model $\mathbf{M}''$ of BA. The first-order objects of $\mathbf{M}''$ are the logarithmic numbers of $\mathbf{M}'$ (i.e., numbers belonging to the domain of exponentiation). The sharp function guarantees that these numbers are closed under multiplication. As second-order objects we take those finite sets which have a code in $\mathbf{M}'$. In this way, Σ_i^p-formulas get transformed into Σ_i^b-formulas of Buss' language (see e.g., [3] or chapter 5 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 $\mathbf{M}''$ of BA one obtains a (first-order) model $\mathbf{M}'$ of S_2 by the inverse procedure. As domain of $\mathbf{M}'$ we take the second-order objects of $\mathbf{M}''$. In $\mathbf{M}''$ we define the primitives of S_2 as set operations. Intuitively, we think of a finite set X as the numbers $\sum_{x\in X} 2^x$ 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 the axioms of S_2 to hold in $\mathbf{M}'$. Note, parenthetically, that the cartesian product of two sets is mapped to a first-order function with the growth rate of the sharp 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 1.7. The readers who are mainly interested in S_2^i are advised to read that 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, Theorem 2.2 is a strengthening of the main theorem of [3]. Our proof is model-theoretic and, to our knowledge, differs from those existing in the literature (but 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 Theorem 2.2 is that, if $\mathcal{P}$-*def* (i.e., the $\forall\Sigma_1^p$ fragment of $\Sigma_1^p(\equiv S_2^1)$) proves $\Sigma_2^p = \Pi_2^p$, then all of BA collapses to $\mathcal{P}$-*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 3.4): in [11] Krajíček, Pudlak and Takeuti, proved that if $\mathcal{P}$-*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 $\mathcal{P}$-*def* proves Σ_1^p-*comp* does BA collapses?

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 [7].)

Theorem. The following are equivalent

(i)	$\mathcal{P}^i\text{-}def \vdash \Sigma_{i+1}^p\text{-}comp$	$T_2^i \vdash \mathcal{S}_2^{i+1}$
(ii)	$\mathcal{P}^i\text{-}def \vdash \Sigma_{i+1}^p \subseteq \Pi_{i+1}^p/poly$	$T_2^i \vdash \Sigma_{i+1}^b \subseteq \Pi_{i+1}^b/poly$
(iii)	$\mathcal{P}^i\text{-}def \vdash BA$	$T_2^i \vdash S_2$
(iv)	$\mathcal{P}^i\text{-}def + \Sigma_{i+1}^p\text{-}choice \vdash \Sigma_{i+1}^p\text{-}comp$	$T_2^i + BB\Sigma_{i+1}^b \vdash \mathcal{S}_2^{i+1}$

The implication from **(i)** to **(ii)** is Theorem 3.3. The implication from **(i)** to **(iii)** can be reconstructed from the proof of Theorem 3.2. (To read these two proofs the reader need only to rush through Section 1.) From Theorem 3.2 it actually follows that **(ii)** implies **(iii)** while in Corollary 2.3 is proved that **(iv)** implies **(i)**.

Acknowledgments. The numerous discussions with Rineke Verbrugge, Harry Buhrman and Volodya Shavrukov have been pleasant and stimulating. When the first draft of this manuscript was ready I had interesting discussions with Sam Buss. I owe him interesting observations and various corrections. Buss independently proved that condition **(i)** above implies **(ii)** and **(iii)**). He observed that from **(i)** follows that PH (provably) collapses to $Boole(\Sigma_{i+2}^p)$. His result inspired our interpolation theorem 3.1. This work is part of my Ph.D. thesis at the University of Amsterdam. The supervision of Dick de Jongh and Albert Visser has assisted me through the numerous stadia of preparation of this work.

1 Preliminaries.

Here we introduce the necessary definitions. Lemma 1.3 provides a smooth bootstrapping. The class of polynomial time computable functions is concisely introduced in section 1.5 in a machine independent way. The (standard) comparison of strength of the various fragments are sketched in Section 1.6. In Section 1.7 the relation with Buss' S_2^i is sketched.

1.1 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 three symbols for binary relations: $<$, $\in$, $\subseteq$. Moreover, there are two sorts of variables: first and second-order. Lower case Latin letters $x, y, z, ..$ denote first-order variables and capital Latin letters $X, Y, Z, ..$ 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 formula $x{<}y$ is to be read "x is less than y" while $X{\subseteq}Y$ stands for "X is a subset of Y". 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

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

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 5 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 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 $\mathcal{F}$ of new symbols for functions. We define the (*relativized*) classes of bounded $L_2(\mathcal{F})$-formulas: $\Sigma_i^p(\mathcal{F})$, $\Pi_i^p(\mathcal{F})$, etc. similarly to those of the language L_2. (We allow terms of $L_2(\mathcal{F})$ to occur in the bounds of the quantifiers.)

The domain of an L_2 structure $\mathbf{M}$ is composed of two disjoint parts: the numbers and the sets of $\mathbf{M}$. Truth in $\mathbf{M}$ is defined as usual but first-order variables are restricted to range over numbers while second order variables range over sets. To denote elements of a model, we use the same convention as for variables so, we write $A{\in}\mathbf{M}$ for 'A is a set of $\mathbf{M}$' and $a{\in}\mathbf{M}$ for 'a is a number of $\mathbf{M}$'. For models we use bold face letters, for the class of first-order objects of a model $\mathbf{M}$ we use the corresponding lower case letter $\mathbf{m}$. The disjoint union of ω and $\mathcal{P}_{<\omega}(\omega)$ constitutes the *standard model*, functions and relations are interpreted in the natural way. We loosely denote the standard model by ω.

Computational complexity theory and second-order arithmetic are our main sources of inspiration, concrete intuition and terminology. For our digressions to computational complexity theory it is convenient to think of finite sets as strings i.e., we identify $\mathcal{P}_{<\omega}(\omega)$ 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 $\{1\}^{<\omega}$.

1.2 The axioms of second-order bounded arithmetic.

The theory Θ is axiomatized by the following formulas:

$$
\begin{array}{ll}
a+1=b+1 \to a=b & a<b \leftrightarrow \exists x.\ (a+x)+1=b \\
a+0=a & A<b \leftrightarrow (\forall x \in A).\ x<b \\
a+(b+1)=(a+b)+1 & A \subseteq B \leftrightarrow (\forall x \in A) x \in B \\
a \cdot 0 = 0 & A=B \leftrightarrow .\ A \subseteq B \wedge B \subseteq A \\
a \cdot (b+1) = (a \cdot b)+a & A \neq \emptyset \to .\ (\exists x \in A)(\forall y<x)\ y \notin A \\
a \neq 0 \leftrightarrow \exists x.\ x+1=a & \exists x.\ A<x.
\end{array}
$$

The six axioms on the left are those of Robinson arithmetic. To these we add the defining axioms for the relations $<$ and $\subseteq$, the axiom of extensionality, the least number principle and the axioms of finiteness (i.e. all sets have an upper bound). 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 $i \in \omega$. The theories Π_i^p-*comp* and $\Sigma_0^p(\Sigma_i^p)$-*comp* are defined in a similar way and are easily seen to be equivalent to Σ_i^p-*comp*.

1.3 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 $|\vec{a}, \vec{A}|$ for the least upper bound of $\{a_1, .., a_n, |A_1|, .., |A_m|\}$. It should be clear that Σ_0^p-*comp* suffices to prove the existence of $|\vec{a}, \vec{A}|$. 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 subsequent ways:

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

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 $\mathcal{R}$ be a set of new primitives, one for each (definition of a) rudimentary function. Let $\mathcal{R}$-*def* be the theory axiomatized by Θ plus the (obvious) defining axioms for the functions in $\mathcal{R}$. Clearly, Σ^p_0-*comp* suffices to prove every rudimentary function to be total. So, $\mathcal{R}$-*def* is a conservative expansion of Σ^p_0-*comp*. The following lemma ensures us that there is no danger in considering formulas of the expanded language $L_2(\mathcal{R})$ as abbreviations of L_2-formulas. In fact, the 'translation' does not increase the complexity of the formula. Namely, the following lemma shows that $\Sigma^p_0 = \Sigma^p_0(\mathcal{R})$ provably in $\mathcal{R}$-*def*.

Lemma 1.3. *For every* $\psi \in \Sigma^p_0(\mathcal{R})$*, there is* $\psi^* \in \Sigma^p_0$ *such that* $\mathcal{R}$-*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 report it in full detail. One has to unfold the definitions of the rudimentary functions inside the $\Sigma^p_0(\mathcal{R})$-formulas ψ. We can assume that ψ has only one occurrence of a single rudimentary function $F_{\varphi,p}(\vec{a}, \vec{A})$ (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 $\in$. This is done by eliminating the relations $<$ and $\subseteq$ as is suggested by the axioms of Θ. Then replace each subformula of the form $x \in F_{\varphi,p}(\vec{a}, \vec{A})$ with

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

Finally, replace subformulas of the form $x < |\vec{a}, \vec{A}|^p$ with an equivalent Σ^p_0-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 functions occur. ∎

A noteworthy corollary of this lemma is that rudimentary functions are closed under composition. From the Lemma it follows also that $\Sigma^p_i(\mathcal{R})$-*comp* $+ \mathcal{R}$-*def* is equivalent to Σ^p_i-*comp* $+ \mathcal{R}$-*def* and hence a conservative extension of Σ^p_i-*comp*.

Below, we list a few rudimentary functions that we often use.

$\langle a, b\rangle := \mu_z.\ 2z = (a+b)(a+b+1)$, the pairing function,

$A \times B := \{\langle x, y\rangle \ :\ x \in A \wedge y \in B\}$, the cartesian product,

$A^{[b]} := \{y \ :\ \langle b, y\rangle \in A\}$, the b-th row of the 'matrix' A,

$A(b) := \mu_z.\ z \in A^{[b]}$, the value of the 'function' A at b,

$[x] := \{y \ :\ y < x\}$, the set of predecessors of x,

$\{x\} := \{y \ :\ x = y\}$, the singleton of x.

1.4 Other fragments.

In this section we present some other interesting axiomatizations of BA. In the next sections we study the relative strength of their fragments. We agree that all theories we introduce in this section contain, by definition, Σ^p_0-*comp*. The theories Σ^p_i-*ind* and Σ^p_i-*dc* (i.e., of *induction*, *dependent choice* and *strong collection* for Σ_i^p-formulas) are axiomatized by the following schemas, for $\varphi \in \Sigma_i^p$.

$$\Sigma_i^p\text{-}ind: \ \varphi(0) \wedge \forall x[\varphi(x) \to \varphi(x+1)] \ \to \varphi(a),$$

$$\Sigma_i^p\text{-}dc: \ \forall x(\forall X{<}b)(\exists Y{<}b)\varphi(x, X, Y) \ \to \exists Z(\forall x{<}a)\varphi(x, Z^{[x]}, Z^{[x+1]})$$

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

(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 that dependent choice, induction and strong collection are all equivalent to comprehension. A rather intriguing role is played by the following schema of *choice*

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

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

1.5 Polynomial time computable functions.

In this section we introduce the classes of functions $\mathcal{P}^i$. These correspond to classes which have been intensively studied in computational complexity theory. 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. A definition of rudimentary function has already been given in Section 1.3. We include here a different one. It is easy to see that these two definitions define the same class of functions. The reader may consult [6] for some details.

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 and 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 $\mathcal{R}$ of *rudimentary* functions is the smallest set of functions closed under composition and under the following schemas

1 (a 0-ary function),

$F(a) = [a]$

$f(a_1, .., a_n, A_1, .., A_m) = a_i + a_j$ for $0{<}i, j \leq n$ and $0 \leq m$,

$f(a_1, .., a_n, A_1, .., A_m) = a_i \cdot a_j$ for $0{<}i, j \leq n$ and $0 \leq m$,

$F(a_1, .., a_n, A_1, .., A_m) = A_i \cup A_j$ for $0 \leq n$ and $0{<}i, j \leq m$,

$F(a_1, .., a_n, A_1, .., A_m) = A_i \setminus A_j$ for $0 \leq n$ and $0{<}i, j \leq m$,

$f(A) = \mu_x(x{\in}A)$ (for $A = \emptyset$ this is defined to be 0)

$F(\vec{a}, Y, \vec{A}) = \bigcup_{y\in Y} G(\vec{a}, y, \vec{A})$ for G in $\mathcal{R}$.

The functions defined by the first seven schemas are called *basic rudimentary*. We shall refer to the last schema as *rudimentary collection*. The class $\mathcal{P}$ is closed also under the following schema of *second-order (polynomially bounded) recursion*

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

for any G, H in $\mathcal{P}$ 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 $\mathcal{P}$ is also denoted $\mathcal{P}^0$. In general, the classes $\mathcal{P}^i$ are obtained by adding to $\mathcal{P}$ *Turing oracles* for Σ^p_i-formulas and closing under rudimentary collection and second-order recursion. Turing oracles for Σ^p_i-formulas are functions of the form

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

for φ in Σ^p_i.

Now, going back to theories of second-order arithmetic, let us use $\mathcal{R}$ and $\mathcal{P}^i$ to indicate also three sets of symbols for functions, a different symbol for each definition of a function in the corresponding class. Let $L_2(\mathcal{R})$ and $L_2(\mathcal{P}^i)$ be the corresponding expansion of L_2. Let $\mathcal{P}^i$*-def* be the theories axiomatized by Θ and the defining axioms of the functions in $\mathcal{P}^i$. We choose the obvious defining axioms of functions obtained by the basic schemas. Namely, for Turing oracles the defining axioms are those given above. If F is (the symbol of the function) obtained by rudimentary collection from $G{\in}\mathcal{R}$ we take as defining axiom of F

$$x{\in}F(\vec{a},Y,\vec{A}) \leftrightarrow (\exists y{\in}Y).\ x{\in}G(\vec{a},y,\vec{A}).$$

If F is obtained by second-order recursion from $G, H{\in}\mathcal{P}$ and $p{\in}\omega$, then the defining axiom is

$$F(0,\vec{a},\vec{A}) = G(\vec{a},\vec{A}) \quad\wedge\quad F(y+1,\vec{a},\vec{A}) = H(y,\ \vec{a},\ \vec{A},\ F(y,\vec{a},\vec{A})) \cap [|y,\vec{a},\vec{A})|^p].$$

1.6 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^p_i, Π^p_i and $\Sigma^p_0(\Sigma^p_i)$-formulas are equivalent. Also, we may contract quantifiers, so, Σ^p_{i+1}-*dc* and Σ^p_{i+1}-*choice* are respectively equivalent to Π^p_i-*dc* and Π^p_i-*choice* (these last two theories are defined in the obvious way). The theory Σ^p_{i+1}-*choice* proves that Σ^p_{i+1}-formulas are closed under first-order bounded quantification. In the schemas of Σ^p_i-*choice*, Σ^p_i-*dc* and Σ^p_i-*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.

Lemma 1.6. *For all* $i{\in}\omega$,

(i) Σ^p_{i+1}-*ind* $\implies$ Σ^p_{i+1}-*choice* $\implies$ Σ^p_i-*comp*

(ii) Σ^p_{i+1}-*comp* $\iff$ Σ^p_{i+1}-*ind* $\iff$ Σ^p_{i+1}-*dc* $\iff$ Σ^p_{i+1}-*coll*

(iii) Σ^p_{i+1}-*comp* $\implies$ $\mathcal{P}^i$-*def* $\implies$ Σ^p_i-*comp*

We understand the first inclusion of **(iii)** *as: every model of* Σ^p_{i+1}-*comp has a unique expansion to a model of* $\mathcal{P}^i$-*def*

Proof of (i). For the first inclusion, it is sufficient to prove Π^p_i-*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^p_{i+1}-*choice* proves Σ^p_i-*comp* (this is true by definition if $i=0$, for $i>0$ it follows from our induction hypothesis), we show that Σ^p_{i+2}-*choice* proves Σ^p_{i+1}-*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

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

We may apply the axiom of choice to get a set $Z\subseteq[a]\times[b]$ such that

$$(\forall Y{<}b)[\psi(x,Z^{[x]})\vee\neg\psi(x,Y)].$$

So,

$$\psi(x,Z^{[x]})\leftrightarrow\varphi(x).$$

Hence, Σ^p_i-*comp* suffices to prove the existence of the set $\{x{<}a\ :\ \varphi(x)\}$.

Proof of (ii). Since all three theories above prove Σ^p_{i+1}-*choice*, in the following proof we use without explicit mention that Σ^p_{i+1}-formulas are closed under bounded first-order quantification.

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

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

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 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 $\psi\in\Sigma^p_{i+1}$,

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

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 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.

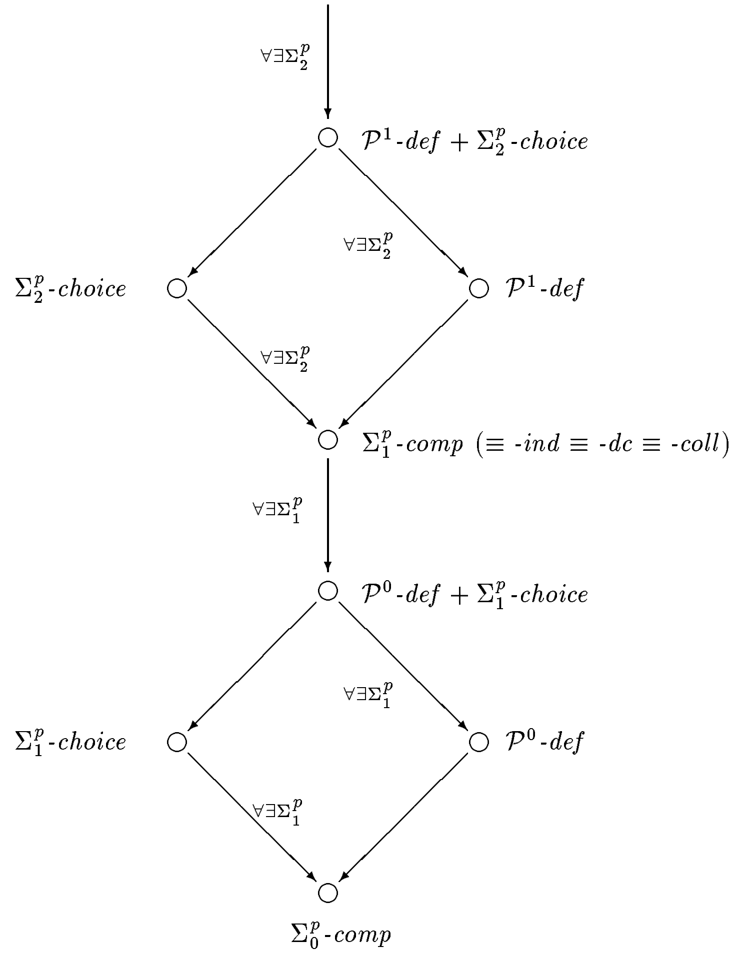
Proof of (iii). The second implication is true by definition if $i = 0$. For $i{>}0$ this holds because $\mathcal{P}^i$ contains Σ^p_i Turing oracles and is closed under rudimentary collection. For the first implication, consider first the case $i = 0$. Given a model $\mathbf{M}$ of Σ^p_1-*comp* we show that there is a unique way of defining new functions on $\mathbf{M}$ which satisfy the axioms of $\mathcal{P}$-*def*. We proceed by induction on the definition of $F{\in}\mathcal{P}$. The new primitives are added in order to have that for some Σ^p_1-formula φ

$$\mathbf{M} \models F(\vec{x}, \vec{X}) = Y \leftrightarrow \varphi(\vec{x}, \vec{X}, Y)$$

$$\mathbf{M} \models \forall \vec{x}, \vec{X}\, \exists! Y\, \varphi(\vec{x}, \vec{X}, Y)$$

The proof is actually standard and need not be reported here in detail. The key step is when F is obtained by recursion. In this case Σ^p_1-*dc* is used. For $i{>}0$ let $\mathcal{T}^i$ be the set of Turing oracles. Clearly there is a unique way to add to a model $\mathbf{M}$ new primitives for $\mathcal{T}^i$-functions and having them satisfy their defining axioms. Now, it is easily seen that, if $\mathbf{M}$ models Σ^p_{i+1}-*comp*, then it models $\Sigma^p_1(\mathcal{T}^i)$-*comp* too. At this point the proof proceeds as in the case $i = 0$. ∎

We sum the lemma up in the following table. An arrow means provability. Next to the arrow we write the partial conservativity we shall prove in sections 2.2 and 2.3.



1.7 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], [10]). 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 $\mathbf{M}_1$ be a model of S_2^i. Let $\mathbf{M}_2$ be the second-order structure having as first-order objects the elements a of $\mathbf{M}_1$ such that 2^a exists and as second-order objects those finite subsets of $\mathbf{M}_1$ which are coded in the usual way by elements of $\mathbf{M}_1$. I.e., for every $a \in \mathbf{M}_1$ we add the set A to $\mathbf{M}_2$ such that

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

Functions and relations of $\mathbf{M}_2$ are defined in the natural way. Note that multiplication of first-order elements is a total operation in $\mathbf{M}_2$. In fact if 2^a and 2^b exist in $\mathbf{M}_1$ then $2^{a \cdot b}$ exists too, since it is equal to $2^a \# 2^b$. It is easy to see that $\mathbf{M}_2$ 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 $a, A \in \mathbf{M}_2$

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

To see the other direction, we apply the inverse procedure. Let $\mathbf{M}_2$ be a model of Σ^p_i-*comp*. We think of sets of $\mathbf{M}_2$ 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 $\mathbf{M}_2$. Still, formalizing the natural algorithm for addition and multiplication of binary numbers, we may define in $\mathbf{M}_2$ some set functions $X \oplus Y$ and $X \otimes Y$ such that

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

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 $\mathcal{P}$-*def*. Let $X\#Y$ be the set $\{\ |X| \cdot |Y|\ \}$ which exists because $\mathbf{M}_2$ models Σ^p_0-*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^i_2 having as its domain the second-order elements of $\mathbf{M}_2$ and as functions and relations the ones just defined. The reader may check that the 32 axioms of BASIC hold in $\mathbf{M}_1$. Because $\mathbf{M}_2$ is a model of Σ^p_i-*ind*, it is not difficult to see that $\mathbf{M}_1$ satisfies logarithmic inductions for Σ^b_i-formulas. Hence $\mathbf{M}_1$ is a model of S^i_2.

To translate the results of section 3.3 in the language of S_2 note that second-order models of Σ^p_{i+1}-*choice* correspond to first-order models of $BB\Sigma^b_{i+1}$ (cf. chapter 5 of [7]), i.e., the schema

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

where φ is in Σ^b_{i+1}.

2 Witnessing theorems and conservativity results.

Buss was the first to give an extensive characterization of complexity classes as classes of functions definable and provably total in some weak fragment of arithmetic. 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 [12], [13]. Buss', Parsons' and Mints's proofs are proof-theoretical. Wilkie gave a model-theoretic proof (unpublished) of Buss' theorem (see [7]). Here we adapt a model-theoretical proof of Mints-Parsons' theorem given by Albert Visser (unpublished).

2.1 Closures

Let $\mathbf{M}$ be a model of Σ^p_0-*comp* and let $\mathbf{W}$ be a subset of $\mathbf{M}$. We say that $\mathbf{W}$ is closed under $\mathcal{R}$-functions if $F(\vec{c},\vec{C}), f(\vec{c},\vec{C}) \in \mathbf{W}$ for every $\vec{c},\vec{C} \in \mathbf{W}$ and $F, f \in \mathcal{R}$. The $\mathcal{R}$-closure of $\mathbf{W}$ in $\mathbf{M}$ is the minimal $\mathcal{R}$-closed subset of $\mathbf{M}$ containing $\mathbf{W}$, i.e.,

$$\langle\!\langle \mathbf{W} \rangle\!\rangle_{\mathcal{R}} := \{F(\vec{c},\vec{C}), f(\vec{c},\vec{C})\ :\ \vec{c},\vec{C} \in \mathbf{W} \text{ and } F, f \in \mathcal{R}\}.$$

We interpret $\mathcal{R}$-closed subsets as substructure in the canonical way. The functions and relations of $\mathbf{N}$ are the restriction of those of $\mathbf{M}$. In the same way we define $\mathcal{P}^i$-closed sets in models of $\mathcal{P}^i$-*def*.

We say that $\mathbf{N} \subseteq \mathbf{M}$ is a Σ^p_i-elementary substructure of $\mathbf{M}$, if for every Σ^p_i-formula φ and every

$\vec{a}, \vec{A} \in \mathbf{N}$

$$\mathbf{N} \models \varphi(\vec{a}, \vec{A}) \implies \mathbf{M} \models \varphi(\vec{a}, \vec{A})$$

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

Lemma 2.1. *(Definability of Skolem functions)*

(i) *$\mathcal{R}$-closed substructures of models of Σ_0^p-comp are Σ_0^p-elementary.*

(ii) *For every model $\mathbf{M}$ of $\mathcal{P}^i$-def and every $W \subseteq \mathbf{M}$ the $\mathcal{P}^i$-closure $\mathbf{N}$ of $\mathbf{W}$ is a $\Sigma_i^p(\mathcal{P}^i)$-elementary substructure of $\mathbf{M}$. In particular $\mathbf{N}$ is a model of $\mathcal{P}^i$-def.*

Proof. For **(i)**, observe first-order Skolem functions for Σ_0^p-formulas are in $\mathcal{R}$. This suffices. The proof of **(i)** when $i = 0$ is obvious as in the previous lemma. For $i>0$ it suffices to show that among the $\mathcal{P}^i$-functions there are Skolem functions for $\Sigma_i^p(\mathcal{P}^i)$-formulas. I.e., for every $\Sigma_i^p(\mathcal{P}^i)$-formula φ there is a function F in $\mathcal{P}^i$ such that

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

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

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

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

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

$$F(\vec{a}, \vec{A}) = G(|\vec{a}, \vec{A}|^p + 1).$$

We leave to the reader the verification that F produces a witness, if one exists, of $\exists Y < |\vec{a}, \vec{A}|^p \varphi(\vec{a}, \vec{A}, Y)$. ∎

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

Corollary 2.1. *(Witnessing theorem for $\mathcal{P}^i$-def.) Each $\forall\exists\Sigma_{i+1}^p$ sentence provable in $\mathcal{P}^i$-def has a witnessing function in $\mathcal{P}^i$.*

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

$$\mathcal{P}^i\text{-}def \vdash \forall \vec{X}, \vec{x}\ \exists Y \varphi(\vec{x}, \vec{X}, Y) \qquad \implies \qquad \mathcal{P}^i\text{-}def \vdash \forall \vec{X}, \vec{x}\ \varphi(\vec{x}, \vec{X}, F(\vec{x}, \vec{X})).$$

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 $F \in \mathcal{P}^i$

(*) $\mathcal{P}^i\text{-}def \vdash \forall \vec{X}, \vec{x}\ \varphi(\vec{x}, \vec{X}, F(\vec{x}, \vec{X}))$.

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

(**) $\mathcal{P}^i$-*def* $+ \{\neg\varphi(\vec{c}, \vec{C}, F(\vec{c}, \vec{C})) \ : \ F \in \mathcal{P}^i\}$

This theory is consistent. Otherwise by compactness, for a finite set of functions $\{F_1, .., F_n\}$ in $\mathcal{P}^i$,

$$\mathcal{P}^i\text{-}def \vdash \forall \vec{x}, \vec{X}.\ \varphi(\vec{x}, \vec{X}, F_1(\vec{x}, \vec{X})) \vee .... \vee \varphi(\vec{x}, \vec{X}, F_n(\vec{x}, \vec{X})).$$

So, since $\mathcal{P}^i$-functions are closed under definition by Σ_i^p-cases, one can combine $F_1, .., F_n$ together to find a function $F \in \mathcal{P}^i$ satisfying (*). Now, choose a model $\mathbf{M}$ of the theory (**) and let $\mathbf{N}$ be the $\mathcal{P}^i$-closure of $\vec{c}, \vec{C}$. By the previous lemma $\mathbf{N}$ is a model of $\mathcal{P}^i$-*def*. The same lemma excludes the possibility of having in $\mathbf{N}$ a set Y such that $\varphi(\vec{c}, \vec{C}, Y)$. Thus $\mathcal{P}^i$-*def* does not prove $\forall \vec{x}, \vec{X}\ \exists Y \varphi(\vec{x}, \vec{X}, Y)$ and the corollary follows. ∎

2.2 A model-theoretical version of Buss' witnessing theorem.

We derive our version of Buss witnessing theorem from the following lemma.

Lemma 2.2. *Every model $\mathbf{M}$ of $\mathcal{P}^i$-def has an $\exists\Sigma_{i+1}^p$-elementary extension to a model $\mathbf{N}$ of Σ_{i+1}^p-comp such that for every Π_i^p-formula φ there is a function $F \in \mathcal{P}^i$ with (undisplayed) parameters from $\mathbf{N}$ such that (*) below holds*

(*) $\mathbf{N} \models \forall X\ \exists Y \varphi(X, Y) \rightarrow \forall X\ \varphi(X, F(X))$.

Proof. We claim that, if we succeed in satisfying condition (*), we obtain also that $\mathbf{N}$ models Σ_{i+1}^p-*comp*. To prove the claim it is sufficient to check that in $\mathbf{N}$ the schema of dependent choices holds for Π_i^p-formulas. Assume in $\mathbf{N}$ holds $\forall x \forall X \exists Y\ \varphi(x, X, Y)$ where a bound b on X and Y is implicit in φ. Let $a \in \mathbf{N}$, we want to find a Z such that $(\forall x < a)\ \varphi(x, Z^{[x]}, Z^{[x+1]})$. By (*), for some $F \in \mathcal{P}^i$ 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):

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

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

Now, let $\mathbf{M}$ be a model of $\mathcal{P}^i$-*def*. The required model $\mathbf{N}$ is constructed as the union of an $\exists\Sigma_{i+1}^p$-elementary chain of models of $\mathcal{P}^i$-*def*,

$$\mathbf{M} = \mathbf{M}_0 \prec_{\exists\Sigma_{i+1}^p} \mathbf{M}_1 \prec_{\exists\Sigma_{i+1}^p} \mathbf{M}_2 \prec_{\exists\Sigma_{i+1}^p} ....$$

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

$$\begin{tikzcd}
& & \mathbf{W} & \\
{} \arrow[r, "\exists\Sigma^p_{i+1}"] & \mathbf{M}_s \arrow[ur] \arrow[r, "\exists\Sigma^p_{i+1}"] & \mathbf{M}_{s+1} \arrow[u, "\Sigma^p_i"'] \arrow[r, "\exists\Sigma^p_{i+1}"] & {}
\end{tikzcd}$$

Suppose $\mathbf{M}_s$ 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 $\mathbf{M}_s$. Let $(*)_s$ be $(*)$ with φ_s for φ. We shall construct a model $\mathbf{M}_{s+1}$ realizing $(*)_s$ for some function $F \in \mathcal{P}^i$. 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 $\mathbf{N}$. It is easy to choose the enumeration such that eventually all Π^p_i-formulas with parameters in $\mathbf{N}$ 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 $\mathbf{M}_s$. Finally, let φ_s be ψ^r_t for $s = \langle r, t\rangle$. To define $\mathbf{M}_{s+1}$ proceed as follows. If $(*)_s$ holds for φ_s, we do nothing, i.e. we define $\mathbf{M}_{s+1} := \mathbf{M}_s$. Otherwise, we try to make the antecedent of $(*)_s$ false in $\mathbf{M}_{s+1}$. We construct $\mathbf{M}_{s+1}$ and $C \in \mathbf{M}$ where $\exists Y \varphi_s(C, Y)$ fails. Since $(*)_s$ does not hold in $\mathbf{M}_s$, the following theory has a model $\mathbf{W}_s$

$$Diag(\mathbf{M}_s) + \{\neg\varphi_s(C, F(C)) \;:\; F \in \mathcal{P}^i \text{ with parameters in } \mathbf{M}_s\},$$

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

$$\mathbf{M}_{s+1} := \langle\!\langle \mathbf{M}_s + C \rangle\!\rangle_{\mathcal{P}^i}$$

Closure to be taken in $\mathbf{W}$. Clearly $\mathbf{M}_{s+1}$ is a Σ^p_i-elementary substructure of $\mathbf{W}_s$ which is elementary equivalent to $\mathbf{M}_s$, so, every $\exists\Sigma^p_{i+1}$-formula true in $\mathbf{M}_{s+1}$ will be true in $\mathbf{W}_s$ and hence in $\mathbf{M}_s$. In $\mathbf{M}_{s+1}$ there is no witness of $\exists Y \varphi_s(C, Y)$. This completes the proof of the lemma. ∎

Corollary 2.2. *($\forall\exists\Sigma^p_{i+1}$-conservation and witnessing theorem for Σ^p_{i+1}-comp.) Σ^p_{i+1}-comp is $\forall\exists\Sigma^p_{i+1}$-conservative over $\mathcal{P}^i$-def, therefore every $\forall\exists\Sigma^p_{i+1}$ sentence provable in Σ^p_{i+1}-comp has a witnessing function in $\mathcal{P}^i$.*

Proof. Immediate from the previous lemma and from Lemma 2.1. ∎

2.3 A model theoretical characterization of choice.

We introduce the concept of $\mathcal{R}$-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 SP_{i+1}-*choice* over Σ^p_i-*comp*. An useful application of this notion is given in the proof of the Corollary below. (The conservativity result in Corollary 2.3 **(b)** will find application in the following sections to characterize the collapse of BA.)

Let $\mathbf{M}$ and $\mathbf{N}$ be models of Σ^p_0-*comp*. Recall that their first-order parts are denoted respectively by $\mathbf{m}$ and $\mathbf{n}$. We say that $\mathbf{N}$ is an $\mathcal{R}$-*extension* of $\mathbf{M}$ if

- **(o)** $\mathbf{m}$ is cofinal in $\mathbf{n}$, i.e., for all $a \in \mathbf{N}$ there is $b \in \mathbf{M}$, such that $a < b$.
- **(i)** $\mathbf{M} \prec_{\Sigma^p_0} \mathbf{N}$.
- **(ii)** $\mathbf{N} = \langle\!\langle \mathbf{M} + \mathbf{n} \rangle\!\rangle_{\mathcal{R}}$, i.e., for every $A \in \mathbf{N}$ there are $a \in \mathbf{N}$ such that $\mathbf{N} \models A = F(a)$ for some $F \in \mathcal{R}$ with parameters in $\mathbf{M}$.

We write $\mathbf{M} \prec_{\mathcal{R}} \mathbf{N}$ when $\mathbf{N}$ is an $\mathcal{R}$-extension of $\mathbf{M}$.

Fact 2.3. *Let* $\mathbf{N}$ *be an* $\mathcal{R}$*-extension of* $\mathbf{M}$.

(a) $\mathbf{M} \prec_{\exists\Sigma^p_1} \mathbf{N}$.

(b) $\mathbf{M} \models \Sigma^p_{i+1}$*-choice* $\implies$ $\mathbf{M} \prec_{\exists\Sigma^p_{i+2}} \mathbf{N}$.

(c) $\mathbf{M} \models \Sigma^p_i$*-comp* $\iff$ $\mathbf{N} \models \Sigma^p_i$*-comp*.

(d) $\mathbf{M} \models \mathcal{P}^i$*-def* $\iff$ $\mathbf{N} \models \mathcal{P}^i$*-def*.

Proof of (a). If $\mathbf{N} \models \exists Y \varphi(Y)$ for some Σ^p_0-formula φ with parameters in $\mathbf{M}$, then for some $b \in \mathbf{M}$, and some $F \in \mathcal{R}$ with parameters in $\mathbf{M}$

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

so, by Σ^p_0-elementarity, this holds in $\mathbf{M}$ too. This proves **(a)**.

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

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

Then, clearly,

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

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

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

Finally, by Σ^p_{i+1}-*choice*,

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

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 1.6. In fact, these imply that $\mathbf{N}$ is an $\exists\Sigma^p_{i+1}$-elementary extension of $\mathbf{M}$. So, let φ be any Σ^p_i-formula with parameters in $\mathbf{N}$. By **(ii)**, we can assume that all second-order parameters $\vec{c}$ of φ belong to $\mathbf{M}$. Let $a \in \mathbf{N}$ be arbitrary. Choose in $\mathbf{M}$ a $b{>}a, \vec{c}$. Since $\mathbf{M} \models \Sigma^p_i$-*comp* there is a set $A \in \mathbf{M}$ such that

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

where the variables $\vec{y}$ replace all first-order parameters of φ. By $\exists\Sigma^p_{i+1}$-elementarity, A satisfies the same property in $\mathbf{N}$ too. So, the set of $\mathbf{N}$,

$$B = \{x{<}a\ :\ \langle x, \vec{c}\rangle {\in} A\}$$

verifies,

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

This proves that $\mathbf{N}$ 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 $\mathbf{N}$ be a model of Σ^p_{i+1}-*comp*. By induction hypothesis, $\mathbf{M}$ is a model of Σ^p_i-*comp* and by Fact **(b)**, a $\exists\Sigma^p_{i+1}$-elementary substructure of $\mathbf{N}$. Let $\varphi(x, Y)$ be a Π^p_i-formula with parameters in $\mathbf{M}$ and an implicit bound on Y. It suffices to find in $\mathbf{M}$ a set A such that

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

By Lemma 1.6, $\mathbf{N}$ models Σ^p_{i+1}-*coll* so, for some set Z

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

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

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

We claim that the set $A{\in}\mathbf{M}$ such that

$$A = \{x{<}a : \ \exists y \ \varphi(x, F(y)^{[x]})\}$$

is the required one. We only need to show that

$$(\forall x{<}a)[\exists Y \varphi(x, Y) \rightarrow x{\in}A],$$

because the converse is obvious. If $\exists Y \varphi(x, Y)$ holds in $\mathbf{M}$ for some $x{<}a$, then this will be also true in the Σ^p_i-elementary extension $\mathbf{N}$. Then $\exists y \ \varphi(x, F(y)^{[x]})$ holds in $\mathbf{N}$ and, again by Σ^p_i-elementarity, is true in $\mathbf{M}$ too. Therefore $x{\in}A$.

Proof of (d). To prove the 'left to right' direction we use Lemma 2.2. This lemma characterize models of $\mathcal{P}^i$-*def* as those having an $\exists\Sigma^p_{i+1}$-elementary extension to a model $\mathbf{M}'$ of Σ^p_{i+1}-*comp*. So, it suffices to show that there exists a model $\mathbf{W}$ satisfying the following diagram of (restricted) elementary extensions

$$\begin{tikzcd}
\mathbf{M} \arrow[r, "\exists\Sigma^p_{i+1}"] \arrow[d, "\mathcal{R}"'] & \mathbf{M}' \models \Sigma^p_{i+1}\text{-}comp \arrow[d] \\
\mathbf{N} \arrow[r, "\exists\Sigma^p_{i+1}"] & \mathbf{W}.
\end{tikzcd}$$

Consider the theory

$$Diag(\mathbf{M}') + Diag_{\Pi^p_{i+1}}(\mathbf{N}).$$

This theory has a model, otherwise, let, for a contradiction, for some $\varphi{\in}\Sigma^p_i$,

$$(\forall X{<}|\vec{c}|^p)\varphi(X, \vec{c}){\in}Diag_{\Pi^p_{i+1}}(\mathbf{N}) \quad \text{and} \quad Diag(\mathbf{M}') \vdash \neg\forall X \varphi(X, \vec{c})$$

where we assume that a bound on X is implicit in φ. Also, since $\mathbf{M} \prec_{\mathcal{R}} \mathbf{N}$, we can assume that all other parameters of φ but $\vec{c}$ are in $\mathbf{M}$. Let $a{\in}\mathbf{M}$ be such that $\vec{c}{<}a$. Replacing the constants

$\vec{c}\notin\mathbf{M}'$ with variables and quantifying we obtain

$$\mathbf{M}' \models (\forall\vec{x}{<}a)\exists X\neg\varphi(X,\vec{x}).$$

We may apply Σ^p_{i+1}-*choice* to get,

$$\mathbf{M}' \models \exists Z(\forall\vec{x}{<}a)\neg\varphi(Z^{[\vec{x}]},\vec{x})$$

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

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

Recall that $\mathbf{M}$ models Σ^p_i-*comp*, so, by **(b)**, $\mathcal{R}$-extensions of $\mathbf{M}$ are $\exists\Pi^p_i$-elementary. So,

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

Therefore,

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

A contradiction since we assumed that $\forall X\varphi(X,\vec{c})\in Diag_{\Pi^p_{i+1}}(\mathbf{N})$.

Let $\mathbf{W}'$ be a model of the theory above and let

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

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

For the converse, assume $\mathbf{N}$ is a model of $\mathcal{P}^i$-*def*. By Lemma 2.2, there is a model $\mathbf{N}'$ such that

$$\begin{tikzcd}
\mathbf{M} \arrow[d, "\mathcal{R}"'] \arrow[dr, "\exists\Sigma^p_{i+1}"] & \\
\mathbf{N} \arrow[r, "\exists\Sigma^p_{i+1}"] & \mathbf{N}' \models \Sigma^p_{i+1}\text{-}comp
\end{tikzcd}$$

where the diagonal arrow follows from **(b)** since, by **(c)**, $\mathbf{M}$ is a model of Σ^p_i. ∎

Lemma 2.3. *Every model* $\mathbf{M}$ *of* Σ^p_i-*comp has an* $\mathcal{R}$-*extension to a model* N *of* Σ^p_{i+1}-*choice.*

Proof. The proof is similar to that of Theorem 2.2. The model $\mathbf{N}$ is constructed as the union of a chain

$$\mathbf{M} = \mathbf{M}_0 \prec_{\mathcal{R}} \mathbf{M}_1 \prec_{\mathcal{R}} \mathbf{M}_2 \prec_{\mathcal{R}} \ldots$$

By the Fact above we have that we actually construct a $\exists\Sigma^p_{i+1}$-elementary chain of models of Σ_i^p-*comp*. Let $\{\varphi_s\}_{s\in\omega}$ be an enumeration with infinitely many repetitions of all formulas with parameters in $\mathbf{N}$, such that all parameters of φ_s are in $\mathbf{M}_s$ (see Theorem 2.2 for details on this enumeration). The chain is constructed so that for all $\varphi_s\in\Pi_i^p$, either (1) or (2) below holds.

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

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

Each link of the chain is constructed using a model $\mathbf{W}$ as intermediate step, as in the following diagram

$$\begin{tikzcd} & & & \mathbf{W} & \\ {} \arrow[r, "\mathcal{R}"] & \mathbf{M}_s \arrow[urr] \arrow[rr, "\mathcal{R}"] & & \mathbf{M}_{s+1} \arrow[u, "\Sigma_0^p"'] \arrow[r, "\mathcal{R}"] & {} \end{tikzcd}$$

Suppose $\mathbf{M}_s$ has already been constructed. If (1) holds in $\mathbf{M}_s$ then let $\mathbf{M}_{s+1} := \mathbf{M}_s$. Otherwise, let $\mathbf{W}$ be any model of

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

Such a model exists, otherwise, for some n

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

Using Σ_i^p-*comp* one can define a set Z in $\mathbf{M}$ 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 $\mathbf{W}$ is, up to isomorphism, an elementary superstructure of $\mathbf{M}_s$. Let $\mathbf{M}_{s+1} := \langle\!\langle \mathbf{M} + c\rangle\!\rangle_{\mathcal{R}}$ (closures to be taken in $\mathbf{W}$). To check that $\mathbf{M}_s \prec_{\mathcal{R}} \mathbf{M}_{s+1}$ note that $\mathbf{M}_{s+1}$ is a Σ_0^p substructure of $\mathbf{W}$. Also, observe that all elements of $\mathbf{M}_{s+1}$ are generated by elements of $\mathbf{M}_s$ and the first-order element $c{<}a$, so, conditions **(o)**, **(i)** and **(ii)** in the definition of $\mathcal{R}$-extension are fulfilled.

To check that (2) holds, suppose not, for a contradiction. If $\exists Y\varphi_s(c, Y)$ held in $\mathbf{M}_{s+1}$, then we would have $\varphi_s(c, F(c))$ for some $F\in\mathcal{R}$ with parameters in $\mathbf{M}_s$. We will reach a contradiction by showing that instead $\varphi_s(c, F(c))$ must fail in $\mathbf{M}_s$. By construction, we have $\neg\varphi_s(c, F(c))$ in $\mathbf{M}_{s+1}$. To pull this back to M_s we reason as follows. Since $\mathbf{M}_s$ is a model of Σ_i^p-*comp*, for some $A\in\mathbf{M}_s$,

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

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

Finally, $\mathbf{N}$ 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 announced characterization.

Theorem 2.3. *For every* $\mathbf{M} \models \Sigma_i^p$*-comp the following are equivalent*

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

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

Proof. That **(i)** implies **(ii)** has already been observed in the fact above. For the converse, suppose

$$\mathbf{M} \models (\forall x{<}a)(\exists Y{<}b)\varphi(x, Y)$$

for some $\varphi \in \Pi_i^p$. Let $\mathbf{N}$ be the $\mathcal{R}$-elementary extension of $\mathbf{M}$ to a model of Σ_{i+1}^p*-choice* as guaranteed by the Lemma above. Then, by the assumed $\exists\Sigma_{i+2}^p$-elementarity

$$\mathbf{N} \models (\forall x{<}a)(\exists Y{<}b)\varphi(x, Y).$$

Let Z in $\mathbf{N}$ be such that $(\forall x{<}a)\varphi(x, Z^{[x]})$. By the definition of $\mathcal{R}$-extension,

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

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

The following conservativity results are consequences of the lemma above.

Corollary 2.3.

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

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

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

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

2.4 Ultrapowers

In this section we present an ultrapower construction corresponding to the construction in Lemma 2.3. Let $\mathbf{M}$ be a model of Σ_0^p*-comp* and $a \in \mathbf{M}$. Let $\mathcal{U}_a$ be an ultrafilter on the set $\{b \in \mathbf{M} : M \models b{<}a\}$. We define on $\mathbf{M}$ the following equivalence relations

$$A \sim_1 B \text{ iff } \{c \in \mathbf{M} : M \models c{<}a \wedge A(c) = B(c)\} \in \mathcal{U}_a$$

$$A \sim_2 B \text{ iff } \{c{\in}\mathbf{M}:\ M \models c{<}a \wedge A^{[c]} = B^{[c]}\} \in \mathcal{U}_a$$

The definitions of $A(c)$ is given in the end of Section 1.3. The $\sim_1$ equivalence class of A is denoted with $A_{/1}$, the $\sim_2$ equivalence class with $A_{/2}$ (the filter $\mathcal{U}_a$ is usually clear from the context). We shall systematically confuse equivalence classes with their representative. Let $\mathbf{M}/\mathcal{U}_a$ be the model whose first-order elements are the $\sim_1$ equivalence classes and whose second-order elements the $\sim_2$ equivalence classes. The relations and the functions of $\mathbf{M}/\mathcal{U}_a$ are defined in the canonical way. To every element c, $C{\in}\mathbf{M}$ we associate the elements $id(c)$ and $id(C)$ of $\mathbf{M}/\mathcal{U}_a$ in the usual way,

$$id(c) = \bigcup_{x<a}\{x\} \times \{c\} \quad \text{and} \quad id(C) = \bigcup_{x<a}\{x\} \times C.$$

The map id is an embedding of $\mathbf{M}$ into $\mathbf{M}/\mathcal{U}_a$. So, as usual, we consider $\mathbf{M}$ as a substructure of $\mathbf{M}/\mathcal{U}_a$.

Fact 2.4.

(a) *If* $\mathbf{M}$ *is a model of* Σ^p_i*-comp then for every* $\Sigma^p_0(\Sigma^p_i)$*-formula* φ

$$\mathbf{M}/\mathcal{U}_a \models \varphi(\vec{B}_{/1}, \vec{C}_{/2}) \qquad \Longleftrightarrow \qquad \{d{\in}\mathbf{M}:\ \mathbf{M} \models (d{<}a) \wedge \varphi(\vec{B}(d), \vec{C}^{[d]})\} \in \mathcal{U}_a.$$

(b) $\mathbf{M}/\mathcal{U}_a$ *is an* $\mathcal{R}$*-extension of* $\mathbf{M}$.

Proof of (a). For atomic φ the lemma holds by definition. The inductive step for the Boolean connectives is immediate. We show that of the existential quantifiers. The $\Longrightarrow$ direction is again immediate. For the converse let us first consider first-order quantifiers. Suppose the lemma holds for $\varphi{\in}\Sigma^p_0(\Sigma^p_i)$ and let us show that it is holds also for $\exists y\ \varphi$, where the bound on y is implicit in φ. Let us write φ_x for $\varphi(\vec{B}(x), \vec{C}^{[x]})$ and assume

$$\{x{\in}\mathbf{M}:\ \mathbf{M} \models (x{<}a) \wedge \exists y \varphi_x(y)\} \in \mathcal{U}_a.$$

Then by Σ^p_i comprehension there is a set A in $\mathbf{M}$ such that

$$\mathbf{M} \models \forall y\ (\forall x{<}a)[\varphi_x(y) \leftrightarrow \langle x, y\rangle{\in}A]$$

so,

$$\{x{\in}\mathbf{M}:\ \mathbf{M} \models (x{<}a) \wedge \varphi_x(A(x))\} \in \mathcal{U}_a,$$

and, by induction hypothesis, $\mathbf{M}/\mathcal{U}_a$ models $\varphi(A_{/1})$ and hence $\exists y \varphi(y)$

For second-order quantifiers the proof is similar. We can assume $i{>}0$ otherwise there is nothing to prove. Suppose the lemma holds for $\varphi{\in}\Sigma^p_i$ and let us show that it is holds also for $\exists Y \varphi$, where the bound on Y is implicit in φ. If

$$\{x{\in}\mathbf{M}:\ \mathbf{M} \models (x{<}a) \wedge \exists Y \varphi_x(Y)\} \in \mathcal{U}_a,$$

by Σ^p_i comprehension, (since $i{>}0$) there is a set A in $\mathbf{M}$ such that

$$\mathbf{M} \models \forall Y\ (\forall x{<}a)[\varphi_x(Y) \leftrightarrow \varphi_x(A^{[x]})]$$

so,

$$\{x{\in}\mathbf{M}:\ \mathbf{M} \models (x{<}a) \wedge \varphi_x(A^{[x]})\} \in \mathcal{U}_a,$$

and, by induction hypothesis,$\mathbf{M}/\mathcal{U}_a$ models $\varphi(A_{/2})$ and hence $\exists Y \varphi(Y)$.

Proof of (b). From **(a)** we have immediately that $\mathbf{M}/\mathcal{U}_a \prec_{\Sigma_0^p} \mathbf{M}$. To check cofinality, observe that $A_{/1}<id(|A|)$. It remains to check condition **(ii)** in the definition of $\mathcal{R}$-extension. Let $D_{/1}$ the diagonal element of $\mathbf{M}/\mathcal{U}_a$, i.e., $D = \{\langle x,x\rangle :\ x<a\}$. All elements $A_{/2}$ of $\mathbf{M}/\mathcal{U}_a$ are such that

$$\mathbf{M}/\mathcal{U}_a \models A_{/2} = \{y : \langle D_{/1}, y\rangle \in id(A)\}$$

In fact, observe that for all first-order elements $B_{/1}$ of $\mathbf{M}/\mathcal{U}_a$,

$$\langle D_{/1}, B_{/1}\rangle = \{x<a : \langle x, \langle x, B(x)\rangle\rangle\}_{/1},$$

so, by the definition of $id(A)$, $\langle D_{/1}, B_{/1}\rangle \in id(A)$ is equivalent to

$$\{x<a : \langle x, B(x)\rangle \in A\} \in \mathcal{U}_a.$$

But this is the same as

$$\{x<a : B(x) \in A^{[x]}\} \in \mathcal{U}_a,$$

which turns out to coincide, by definition, with $B_{/1} \in A_{/2}$. So, every second-order element $A_{/2}$ of $\mathbf{M}/\mathcal{U}_a$ is Σ_0^p-definable over the first-order elemet $D_{/1}$ and the second-order element $id(A)$. The latter is identified with an element of $\mathbf{M}$ since it is the image of A via the canonical embedding of $\mathbf{M}$ into $\mathbf{M}/\mathcal{U}_a$. Thus, also condition **(ii)** is fulfilled. ∎

Theorem 2.4. *Every model* $\mathbf{M}$ *of* Σ_i^p*-comp has an* $\mathcal{R}$*-extension to a model of* Σ_{i+1}^p*-choice.*

Proof. We construct a chain of $\mathcal{R}$-extensions

$$\mathbf{M} = \mathbf{M}_0 \prec_{\mathcal{R}} \mathbf{M}_1 \prec_{\mathcal{R}} \mathbf{M}_2 \prec_{\mathcal{R}} \ldots$$

by means of ultrapowers. By Fact 2.3, the chain is automatically Σ_{i+1}^p and all models in it are models of Σ_{i+1}^p-*comp*. Let $\{\varphi_s\}_{s\in\omega}$ be an enumeration with infinitely many repetitions of all formulas with parameters in $\mathbf{N}$, such that all parameters of φ_s are in $\mathbf{M}_s$ (see Theorem 2.2 for details on this enumeration). The chain is constructed so that for all $\varphi_s \in \Pi_i^p$, either (1) or (2) below holds.

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

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

Suppose $\mathbf{M}_s$ has already been constructed. If (1) holds in $\mathbf{M}_s$ then let $\mathbf{M}_{s+1} := \mathbf{M}_s$. Otherwise let $a\in\mathbf{M}_s$ be any element witnessing the failure of (1). Consider the ultrafilter on $[a]$ generated by the sets

$$\{x<a : \mathbf{M}_s \models \neg\varphi_s(x, Z^{[x]})\}$$

for Z in M. Since $\mathbf{M}_s \models \Sigma_i^p$-*comp*, the sets above enjoy the finite intersection property, so, such an ultrafilter actually exists. Let $\mathbf{M}_{s+1} := M_s/\mathcal{U}_a$.

To check that (2) holds, suppose not for a contradiction. Let D be the diagonal in $M_s/\mathcal{U}_a$. If $\exists Y \varphi_s(D_{/1}, Y)$ held in $\mathbf{M}_{s+1}$, then, by Fact **(a)** above, we would have that for some Y in M,

$$\{x<a :\ M_s \models \varphi_s(x, Y^{[x]})\} \in \mathcal{U}_a,$$

quod non since the complement of this set is, by construction, also in $\mathcal{U}_a$.

Finally, $\mathbf{N}$ is a model of Σ^p_{i+1}-*choice*, since the truth of both formulas in (1) and in (2) is preserved along the the $\exists\Sigma^p_{i+1}$-chain. ∎

3 The collapse of BA versus the collapse of PH

It is not known whether BA collapses, i.e., if it is equal to some of its fragments. The only collapse that we are able to exclude is Σ^p_1-*choice* $= \mathcal{P}$-*def*. In fact rudimentary functions $\mathcal{R}$ are the only Σ^p_1 provably total functions of Σ^p_1-*choice* and a simple diagonalization argument shows these are strictly included in the polynomial time computable functions $\mathcal{P}$. Actually one can also see that the $\forall\Sigma^p_0$ fragment of $\mathcal{P}$-*def* strictly include that of Σ^p_0-*comp* (and, by conservativity, that of Σ^p_1-*choice*). In fact, in [2] Ajtai has constructed a model $\mathbf{M}$ of $I\Delta_0(R)$ such that

$$\mathbf{M} \models \exists x \ R : [x] \hookrightarrow [x+1]$$

i.e., R is an injection of $[x]$ into $[x+1]$. We can expand $\mathbf{M}$ to a model $\mathbf{M}'$ of Σ^p_0-*comp* taking as sets of $\mathbf{M}'$ the finite $\Delta_0(R)$-definable sets of $\mathbf{M}$. Then $\mathbf{M}'$ 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 $\mathcal{P}$-*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.

3.1 An interpolation theorem

The following is the 'bounded version' of a general interpolation theorem for classical predicate logic.

Theorem 3.1. *Let φ and ψ be $\forall\Pi^p_{i+2}$-formulas and let T be a $\forall\Pi^p_{i+2}$-axiomatized theory. If $T \vdash \varphi \to \neg\psi$ then there is a Boolean combination β of Σ^p_{i+1}-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 $\forall\Pi^p_{i+2}$-theories $U \supseteq T + \varphi$ and $V \supseteq T + \psi$ such that U and V have the same $\forall\Sigma^p_i$-consequences (we say also that they are mutually $\forall\Sigma^p_i$-conservative). In fact, we claim that, for any pair U and V of mutually $\forall\Sigma^p_i$-conservative theories which are $\forall\Pi^p_{i+2}$-axiomatizable, $U + V$ is consistent (and, actually, also has the same $\forall\Sigma^p_i$-consequences). Let us first prove this claim and then proceed to the construction of U and V. We construct a Σ^p_i-elementary chain of models,

$$\mathbf{M}_0 \prec_{\Sigma^p_i} \mathbf{M}_1 \prec_{\Sigma^p_i} ....,$$

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

$$\mathbf{M}_{2s+1} \models Diag_{\Pi_i^p}(\mathbf{M}_{2s}) + V \quad \text{and} \quad \mathbf{M}_{2s+2} \models Diag_{\Pi_i^p}(\mathbf{M}_{2s+1}) + U.$$

In fact, if we assume as induction hypothesis that $\mathbf{M}_{2s}$ is a model of U, then $Diag_{\Pi_i^p}(\mathbf{M}_{2s}) + V$ is consistent, otherwise, for some $\theta \in \Pi_i^p$

$$V \vdash \forall \vec{x}\vec{X} \neg\theta \quad \text{and} \quad \mathbf{M}_{2s} \models \exists \vec{x}\vec{X}\ \theta$$

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

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

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

Now we construct U and V. Let $\vec{X}$ be all free variables occurring in $\varphi \to \neg\psi$. Let $\mathcal{B}_{i+1}$ denote the class of formulas with free variables among $\vec{X}$ of the form $\forall Y\beta$ and such that $\forall Y{<}|\vec{X}|^p\beta$ is a Boolean combination of Σ_{i+1}^p-formulas (for $p\in\omega$). Let us say that two theories U and V are $\mathcal{B}_{i+1}$ inseparable (in the following simply inseparable) if $V + Th_{\mathcal{B}_{i+1}}(U)$ is consistent. In other words, if there is no $\forall Y\beta\in\mathcal{B}_{i+1}$ such that

$$U \vdash \forall Y\beta \quad \text{and} \quad V \vdash \neg\forall Y\beta$$

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

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

where $\forall Y\beta$ is in $\mathcal{B}_{i+1}$. 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

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

Therefore $\forall Y{<}|\vec{X}|^p\beta$ 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:

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

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 $\mathcal{B}_{i+1}$,

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

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

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

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

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

therefore,

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

But $V_s \vdash \forall Z\beta'$ so, $V_s + Th_{\mathcal{B}_{i+1}}(U_s)$ 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,

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

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

3.2 Sufficient conditions for the collapse of BA

Let us introduce some terminology. We say that a theory proves $\Pi^p_i = \Sigma^p_i$ if every Π^p_i-formula is provably equivalent to a Σ^p_i-formula (with the same free variables). In this case we also say that PH provably collapses to $\Pi^p_i = \Sigma^p_i$. We say that a theory proves $\Pi^p_{i+1} = \Sigma^p_{i+1}/poly$, if for every $\theta{\in}\Sigma^p_{i+1}$ there is a $\psi{\in}\Pi^p_{i+1}$ such that, provably in the theory

$$\exists W(\forall X{<}c)\big[\theta(X) \leftrightarrow \psi(X,W)\big].$$

The W in the formula above is usually called an *advice* (it may not occur in θ). Observe that if in a model holds that $\Pi^p_{i+1} = \Sigma^p_{i+1}/poly$ then every PH-formula is equivalent to a Σ^p_{i+1}-formula depending on additional parameters.

We mention an interesting consequence of Lemma 2.2 and Lemma 2.3.

Theorem 3.2. *The following are sufficient conditions for $\mathcal{P}^i$-def $\vdash BA$*

(a) $\mathcal{P}^i\text{-}def + \Sigma^p_{i+1}\text{-}choice \ \vdash\ \Pi^p_{i+2} = \Sigma^p_{i+2}$,

(b) $\mathcal{P}^i\text{-}def + \Sigma^p_{i+1}\text{-}choice \ \vdash\ \Pi^p_{i+1} = \Sigma^p_{i+1}/poly$.

Proof. By the Corollary 2.3 if we can show that $\mathcal{P}^i$-*def* $+ \Sigma^p_{i+1}$-*choice* proves BA we are done. In fact, then we have

$$\mathcal{P}^i\text{-}def \ \vdash\ \Sigma^p_{i+1}\text{-}comp \ \vdash\ \mathcal{P}^i\text{-}def + \Sigma^p_{i+1}\text{-}choice \ \vdash\ BA$$

Let us prove **(a)**. Every model $\mathbf{M}$ of $\mathcal{P}^i$-*def* $+ \Sigma^p_{i+1}$-*choice* has an Σ^p_{i+1}-elementary extension to a model of Σ^p_{i+1}-*comp*. By the provable collapse of PH every bounded formula is equivalent both to a Π^p_{i+2} and to a Σ^p_{i+2}-formula. Therefore every Σ^p_{i+1}-elementary extension is actually PH-elementary. So $\mathbf{M}$ is a model of Σ^p_{i+1}-*comp* too. By the interpolation lemma above every PH-formula is equivalent to a Boolean combination of Σ^p_{i+1}-formulas. For this class of formulas comprehension is provable in Σ^p_{i+1}-*comp*.

Let us prove **(b)**. We show that the choice schema holds for every bounded formula. Observe that we can write the schema of choice in order to have all quantifiers in the premises bounded:

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

By $\Pi^p_{i+1} = \Sigma^p_{i+1}/poly$, there is a Σ^p_{i+1}-formula equivalent to φ depending on some additional parameters (i.e., the advices which transform universal in existential quantifiers and vice versa). So, the required Z exists by Σ^p_{i+1}-*choice*. ∎

3.3 Necessary conditions for the collapse of BA

Here we show that if $\mathcal{P}^i$*-def* proves Σ^p_{i+1}*-comp* then it proves the collapse of PH and BA reduces to $\mathcal{P}^i$*-def*. We need the following lemma of [11] which is known as the KPT witnessing theorem.

Lemma 3.3. *For every $\varphi \in \Pi^p_i$ if $\mathcal{P}^i$-def proves $\forall X \exists Y \forall Z \varphi(X, Y, Z)$, then there are $F_1,..,F_n$ in $\mathcal{P}^i$ such that $\mathcal{P}^i$-def proves*

$$\forall X Z_1, .., Z_n. \bigvee \begin{cases} \varphi(X, F_1(X), Z_1) \\ \varphi(X, F_2(X, Z_1), Z_2) \\ \dots \\ \dots \\ \varphi(X, F_n(X, Z_1, \dots, Z_{n-1}), Z_n). \blacksquare \end{cases}$$

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

$$\mathcal{P}^i\text{-}def + \{\neg\varphi(C, F_n(C, \vec{D}_n), D_n) \ : \ n\in\omega\}$$

where $\vec{D}_n$ stays for $D_1, .., D_{n-1}$. If this theory is inconsistent, our claim follows by compactness. So, we suppose for a contradiction that this theory has a model. Let $\mathbf{M}$ be the $\mathcal{P}^i$-closure of C, $\{D_n\}_{n\in\omega}$ in the model of the theory above. By Lemma 2.1

$$\mathbf{M} \models \neg\varphi(C, F_n(C, \vec{D}_n), D_n)$$

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

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

Theorem 3.3. $\mathcal{P}^i$*-def* $\vdash \Sigma^p_{i+1}$*-comp* $\implies$ $\mathcal{P}^i$*-def* $\vdash \Pi^p_{i+1} = \Sigma^p_{i+1}/poly$.

Proof. Consider an arbitrary formula of the form $\exists Z \varphi(X, Z)$ for $\varphi \in \Pi^p_i$ where a bound on Z implicit in φ. We shall find a formula $\psi \in \Pi^p_{i+1}$ such that $\mathcal{P}$*-def* proves

$$\exists W (\forall X{<}c).\ \exists Z \varphi(X, Z) \leftrightarrow \psi(X, W).$$

Since, by lemma'1.6, Σ^p_{i+1}*-comp* is equivalent to Σ^p_{i+1}*-coll*, we can assume that $\mathcal{P}$*-def* proves the following sentence

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

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

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

We can replace universal quantification with 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 $\forall X, Y, A\ \gamma$ where

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

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

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

We consider two possibilities.

- ($\circ$) Suppose there is a $Y < c$ such that $\xi(X, Y, A)$ holds for every $X < c$ and every A. Let $W = Y$. Since $\xi(X, W, A)$ holds for all X and A, then, in particular, $\exists A \varphi(X, A)$ implies $\varphi(X, F(X, W))$ and so, implies $\psi(X, W)$. The converse is obvious since, by our choice of W, the second disjunct is always false.

- ($\circ\circ$) Suppose case ($\circ$) 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, e.g., $W = \{c\}$. If $\exists A \varphi(X, A)$ does not hold then in particular $\neg\varphi(X, K(Y, X, A))$. So, for A and Y such that $\neg\xi(Y, X, A)$, $\psi(X, W)$ 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 3.3.

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

(b) $\mathcal{P}^i\text{-}def \ \vdash \ \Sigma^p_{i+1}\text{-}comp \ \Longrightarrow \ \mathcal{P}^i\text{-}def \ \vdash \ \Pi^p_3 = \Sigma^p_3$

Proof. bf (a) follows immediately from Theorem 3.2. To prove **(b)** We can assume that $\theta(A) \in \Pi^p_3$ 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_3-formula equivalent to θ. From $\Pi^p_{i+1} = \Sigma^p_{i+1}/poly$ we have that, provably in $\mathcal{P}^i\text{-}def$, for some $\psi \in \Sigma^p_{i+1}$, (omitting the bound on W)

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

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

$$(\forall X,Y,A<c).\ \varphi(X,Y,A)\leftrightarrow\psi(c,X,Y,A,W)$$

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

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

3.4 Krajícěk, Pudlak and Takeuti's method

Krajícěk, Pudlak and Takeuti have shown in [11] that if $\mathcal{P}^i$-*def* proves Σ^p_{i+1}-*comp* then $\Sigma^p_{i+1}=\mathcal{P}^i/poly$ in the standard model (and hence $\Sigma^p_2=\Pi^p_2$). We show how their result can be obtained by sharpening the reasoning of the previous section. The combinatorics used in the following proof is of a more complex nature than those needed in the previous section. It is still unknown whether this proof can be formalized in BA.

For every Σ^p_{i+1}-formula $\exists Y\varphi(X,Y)$ we construct a $\mathcal{P}^i$-function F and an $p\in\omega$ such that for all c there is some advice $W<c^p$ such that $\varphi(X,F(X,W))$ for every $X<c$. We shall say for short that $\Sigma^p_{i+1}=\mathcal{P}^i/poly$.

Theorem 3.4. *If $\mathcal{P}^i$-def + Σ^p_{i+1}-choice $\vdash$ Σ^p_{i+1}-comp then in the standard model $\Sigma^p_{i+1}=\mathcal{P}/poly$.*

Proof. By Corollary 2.3 we can as well assume that $\mathcal{P}^i$-*def* $\vdash\Sigma^p_{i+1}$-*comp*. Let $\exists Y\varphi(X,Y)\in\Sigma^p_{i+1}$. We reason as in Theorem 4.4. Assuming for readability that, for the formula considered here, the KPT witnessing theorem holds with $n=2$, we obtain that the following formula $\gamma(X,Y,A)$ is provable in $\mathcal{P}^i$-*def*,

$$\bigvee\left\{\begin{array}{l}\bigwedge\left\{\begin{array}{l}\varphi(X,A)\to\varphi(X,F(X,Y)\\ \varphi(Y,A)\to\varphi(Y,G(X,Y))\end{array}\right.\\ \\ \bigwedge\left\{\begin{array}{l}\exists B\varphi(X,B)\to\varphi(X,H(X,Y,A))\\ \exists B\varphi(Y,B)\to\varphi(Y,K(X,Y,A))\end{array}\right.\end{array}\right.$$

where the functions $F,G,H,K\in\mathcal{P}^i$ are those of the proof of Theorem 4.3.

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

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

That is, for some function $F'{\in}\mathcal{P}^i$ and some W' coding W and V,

$$(\forall X{<}c).\ \exists Y\varphi(X,Y) \leftrightarrow \varphi(X,F'(X,W')).$$

Recall the bond on $\exists Y\varphi(X,Y)$ is implicit in φ so, the size of V can be bound 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*, **24**, (1983), 1-48.

[2] M. Ajtai, The complexity of the pigeonhole principle. *IEEE*, (1988), 346-355.

[3] S. R. Buss, *Bounded arithmetic.* Bibliopolis, Naples, (1986).

[4] S. R. Buss, Axiomatizations and conservations results for fragments of bounded arithmetic. In *Logic and Computation*, (proceeding of a workshop held at Carnegie-Mellon University, 1987), Contemporary Mathematics, A.M.S., **106**, (1990), 57-84.

[5] A. Cobham, The intrinsic computational difficulty of functions. In: A.L.Seleman (ed.), Structure in complexity theory, *Lecture Notes in Computational Science*, **221**, (1986), 125-146.

[6] K. J. Devlin, *Constructibility.* Springer Verlag, Berlin, 1984.

[7] P. Hájek, 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), 278-292.

[9] J. B. Paris and L. A. S. Kirby, Σ_n-collection schemas in arithmetic. In *Logic Colloquium 77*, A. Macintyre, L. Pacholski, J. Paris (eds.). North-Holland, Amsterdam (1978), 199-209.

[10] J. Krajíček, Exponentiation and second order bounded arithmetic. *Annals of Pure and Applied Logic*, **48**, (1990), 261-276

[11] J. Krajíček, P. Pudlak, G. Takeuti, Bounded arithmetic and the polynomial time hierarchy. *Annals of Pure and Applied Logic*, **52**, (1991), 143-153.

[12] G. E. Mints, Quantifier-free and one-quantifier systems. In: Yu. V. Matijasevich and A. O. Silisenko ed., *Zapiski Nauchnykh Seminarov* **20**, (1971), 115-133. (In Russian. English translation: *Journal of Soviet Mathematics* **1**, (1973), 211-266.)

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

[14] A. Razborov, An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic, in *Proof Theory and Computational Complexity.* In: P. Clote and J. Krajíček ed., *Arithmetic, Proofs Theory and Computational Complexity.* Oxford University press, Oxford, 1993

[15] G. Takeuti, *RSUV isomorphisms.* In: P. Clote and J. Krajíček (ed.). *Arithmetic, Proofs Theory and Computational Complexity.* Oxford University press, Oxford, 1993

[16] A. J. Wilkie, Modelès non standard de l'arithmétique et complexité algorithmique. In: A. J. Wilkie and J. Ressayre, *Modelès non standard de l'arithétique et theorie des ensemble.* Publications Mathémetique de l'Université Paris VII, Paris 1-45.

Domenico Zambella
Faculteit der Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amstedam
The Netherlands
domenico@fwi.uva.nl