Techniques in weak analysis for conservation results

António M. Fernandes
Instituto Superior Técnico
Departamento de Matemática
Av. Rovisco Pais, 1049-001 Lisboa, Portugal
amfernandes@netcabo.pt

Fernando Ferreira
Universidade de Lisboa
Faculdade de Ciências
Departamento de Matemática
Campo Grande, Ed. C6, 1749-016 Lisboa, Portugal
fjferreira@fc.ul.pt

Gilda Ferreira
Universidade Lusófona de Humanidades e Tecnologias
Departamento de Matemática
Av. do Campo Grande, 376, 1749-024 Lisboa, Portugal
gildafer@cii.fc.ul.pt

January 26, 2013

Abstract

We review and describe the main techniques for setting up systems of weak analysis, i.e. formal systems of second-order arithmetic related to subexponential classes of computational complexity. These involve techniques of proof theory (e.g., Herbrand's theorem and the cut-elimination theorem) and model theoretic techniques like forcing. The techniques are illustrated for the particular case of polytime computability. We also include a brief section where we list the known results in weak analysis.

Keywords. Bounded arithmetic. Weak analysis. Conservation results. Cut-elimination. Forcing. Polytime computability.

1

1 Introduction

Weak analysis can be described as the formalization and development of analysis in very weak systems of second-order arithmetic. These systems, as they are ordinarily understood, are subelementary in the sense that they do not prove the totality of the exponential function. In addition, they are often related with well-known classes of computational complexity, e.g. polytime or polyspace computability. This paper is not, however, concerned with weak analysis as described in the first two lines of this introduction (nevertheless, in Section 8, we briefly review – without proofs – the state of the art in this respect). The aim of this paper is rather to describe and exemplify the fundamental techniques for setting up a system of weak analysis. In the remainder of this introductory section, we give a blueprint for defining theories of weak analysis. We first give a general blueprint and then describe it for the particular case of polytime computability and point to the sections of the paper where the blueprint is executed (for the polytime case).

Systems of analysis must be able to speak about real numbers. Therefore, they are usually framed in a second-order language and each real number is "presented" via a set of natural numbers. It is of course important to be able to define basic real numbers, to show that they are closed under basic operations and, in general, to be able to prove simple facts about the real line. This is achieved essentially by a combination of induction and set-formation. The amount of induction present in a weak theory is intrinsically related with its provably total functions (with appropriate graphs). Hence, if one is given a computational complexity class C and the goal is to set up a theory T whose provably total functions are exactly those of C, then one is immediately constrained with respect to the amount of induction permitted in the system.

The situation is also tight with respect to set formation because we allow set parameters in the induction scheme (therefore, the more sets there are, the more induction is available). There does exist, nevertheless, some leeway with regard to set formation. All the systems of weak analysis considered permit forms of recursive comprehension, i.e., a principle of the form:

$$\forall x\,(\exists y A(x, y) \leftrightarrow \forall z B(x, z)) \rightarrow \exists X \forall x\,(x \in X \leftrightarrow \exists y A(x, y))$$

where $A(x, y)$ and $B(x, z)$ are appropriate formulas (possibly with first and second-order parameters) and X does not occur in $A(x, y)$. Typically, $A(x, y)$ and $B(x, z)$ are sufficiently expressive so that the sets of the form $\{x : \exists y A(x, y)\}$ (resp., $\{x : \forall z B(x, z)\}$) give all the recursively enumerable (resp., co-recursively enumerable) sets in the standard model. The reader who is unfamiliar with the subject can be taken aback by this amount of comprehension. Shouldn't the variables y and z above be restricted in some way so that only sets in C are definable (in the standard model)? No, and this liberty simplifies very much the development of analysis. The *intuitive reason* why the above recursive comprehension is not a strong principle is that, in order to form the set $X = \{x : \exists y A(x, y)\}$, one must first establish the equivalence $\forall x\,(\exists y A(x, y) \leftrightarrow \forall z B(x, z))$. Note that only weak principles are available for doing this. In short, one can form a recursive set *if* one can show that the set is indeed recursive. The *formal reason* that makes possible the inclusion of recursive comprehension relies crucially on the availability (of forms) of bounded collection. Fortunately, it is known that under very gen-

eral conditions, the addition of bounded collection to a bounded theory of arithmetic results in a conservative extension with respect to Π^0_2-sentences. At this juncture, a second-order theory T^2 is set-up: one that has forms of recursive comprehension and bounded collection.

There is another reason why bounded collection is important. It is because of its relation with weak König's lemma. This lemma guarantees the existence of infinite paths through an infinite binary tree (curiously enough, although the path is a *set* the tree need not be a set – it only needs to be a *class* defined by a bounded formula). Weak König's lemma is a form of compactness and, e.g., is instrumental in analysis to prove the compactness of the closed unit interval (see Section 8 for some facts). The addition of weak König's lemma is first-order conservative over T^2. We use for this a forcing technique originally due to unpublished work of Leo Harrington. The proof of the density of some sets needed for the forcing argument relies crucially on bounded collection. Weak König's lemma can be strengthened to the so-called strict-Π^1_1 reflection. Roughly, this principle differs from weak König's lemma in that the binary trees permitted are constituted not by binary strings but by bounded sets. Observe that, in the absence of the totality of exponentiation, not every bounded set is given by a binary string. Strict-Π^1_1 reflection can be added to T^2 without changing the Π^0_2-consequences and, again, we use a forcing argument. However, in order to show the density of certain sets one must rely on stronger forms of bounded collection (and stronger notions of bounded formula). The authors do not know of any uses of strict-Π^1_1 reflection for the development of analysis in weak systems.

We have described a very general blueprint for setting up a weak system of analysis related with a given class C of computational complexity. In this paper, we illustrate this blueprint in a simple case: when C is the class of polytime computable functions. All the techniques needed to set up systems of weak analysis as described above are already present in this case. Most of the results of this paper have appeared elsewhere in several publications, but in here we conveniently integrate them and discuss their scope and limitations. The detailed blueprint for the polytime case, with appropriate references to the sections of the paper, is the following:

(a) We describe a universal theory (i.e., one that can be axiomatized by universal formulas) PTCA which has function symbols for every polytime computable function. Herbrand's theorem guarantees that the provably total functions (with appropriate graphs) of this theory are the polytime computable functions. PTCA is extended in order to permit induction for formulas that, in the standard model, define the NP sets (the Σ^b_1-formulas). This is done using a cut-elimination argument. We will observe in Section 4 that this extra amount of induction is essential to introduce recursive comprehension. As a matter of fact, we actually work with a simplified theory $\Sigma^b_1\text{-NIA}$ (this corresponds to the theory T in the general blueprint). These issues are treated in Section 2.

(b) In Section 3, we show that the addition of the bounded collection scheme $\mathsf{B}\Sigma^b_\infty$ to $\Sigma^b_1\text{-NIA}$ yields a Π^0_2-conservative extension. We use again an argument based on cut-elimination.

(c) We introduce the second-order theory BTFA (corresponding to T^2 in the general

blueprint) enjoying a form of recursive comprehension and show that it is first-order conservative over Σ^b_1-NIA + BΣ^b_∞. This is shown in Section 4 via a simple model theoretic argument.

(d) In the next section, we show that the addition of weak König's lemma to BTFA results in a theory which is a first-order conservative extension of BTFA. We use the forcing method to prove this result. We will point to the need of bounded collection in the forcing argument.

(e) In Section 7, we define the scheme of strict-Π^1_1 reflection and show that adding it to BTFA does not permit proving more Π^0_2-sentences. This is done via a forcing argument similar to the one in (d) above. As discussed, for this forcing argument to be successful, one needs a stronger form of bounded collection. This stronger form is formulated and discussed in the previous Section 6, and an appropriate conservation result is proved. Cut-elimination is used in proving this conservation result.

The paper has a further section where we present in a compact manner the state of the art concerning the formalization of analysis in weak systems. This last section has no proofs but provides appropriate references and mentions some open problems.

2   First-order theories for polytime computability

We start by presenting three first-order theories for polytime computability, namely PTCA, PTCA$^+$ and Σ^b_1-NIA. The former and the latter systems play, in the context of polytime computability, the same role as (first-order) PRA and Σ^0_1-IND play in the context of primitive recursive computability. The inclusion of the intermediate theory PTCA$^+$ aims at making more explicit a conservation result concerning induction. We remind that the goal of the present paper does not lie in the introduction of weak theories connected with polytime computability (already described in [11, 12, 13, 3]) but in the survey of conservation techniques, which we try to motivate and present in a simple and clear way.

When working in systems of bounded arithmetic, we must opt between two notations: *unary* or *binary*. Unary notation, the most commonly used in the literature, was the choice of Samuel Buss in his seminal thesis [3], while binary notation was used by the second author in [11]. Due to the possibility of interpreting theories in one notation into theories in the other notation (e.g. [23]), the choice has no intrinsic significance and is basically a question of taste and pragmatics. The authors share the opinion that binary notation is more intuitive and convenient for describing and dealing with weak (subexponential) systems of analysis and this explains why it is adopted in the present paper. Therefore, the language that we use aims at describing the set of finite binary words, denoted by $\{0,1\}^*$ (or $2^{<\omega}$). This is the domain of the intended *standard* model. Let us introduce some notation: ϵ denotes the empty word; for x and y elements in $\{0,1\}^*$, $x{}^\frown y$ represents the *concatenation* of x by y (we usually omit the concatenation symbol ${}^\frown$ and just write xy); $x \subseteq y$ means that x is an *initial subword* of y (x is a string prefix of y); $|x|$ denotes the *length* of the word x; $x_{|y}$ is the *truncation* of x by the length

of y ($x_{|_y}$ is x itself if $|x| \leq |y|$; otherwise, it is the prefix of x with length $|y|$); finally, $x \times y$ is the word x concatenated with itself length of y times (note that $|x \times y| = |x| \cdot |y|$).

Let $\mathcal{L}$ be the first-order language which has three constant symbols ϵ, 0 and 1, two binary function symbols ^ and $\times$ (with the standard interpretations given in the previous paragraph) and two binary relation symbols $=$ and $\subseteq$ (for *equality* and *initial subwordness*, respectively). Let $\mathcal{L}_\mathcal{P}$ be the extension of $\mathcal{L}$ by adding a function symbol for each description (given below) of a polytime computable function.

Definition 1. PTCA *(acronym for* Polynomial Time Computable Arithmetic*) is the first-order theory, in the language $\mathcal{L}_\mathcal{P}$, which has the following axioms:*

- Basic axioms

  $x\epsilon = x$, $x(y0) = (xy)0$ and $x(y1) = (xy)1$;

  $x \times \epsilon = \epsilon$, $x \times y0 = (x \times y)x$ and $x \times y1 = (x \times y)x$;

  $x \subseteq \epsilon \leftrightarrow x = \epsilon$, $x \subseteq y0 \leftrightarrow x \subseteq y \vee x = y0$ and $x \subseteq y1 \leftrightarrow x \subseteq y \vee x = y1$;

  $x0 = y0 \rightarrow x = y$ and $x1 = y1 \rightarrow x = y$;

  $x0 \neq y1$, $x0 \neq \epsilon$ and $x1 \neq \epsilon$;

- Defining axioms

  (a) Initial functions

  $C_0(x) = x0$
  $C_1(x) = x1$
  $P_i^n(x_1, ..., x_n) = x_i$, *for* $1 \leq i \leq n$
  $Q(x, y) = 1 \leftrightarrow x \subseteq y$; $Q(x, y) = 0 \vee Q(x, y) = 1$

  (b) Derived functions

  1. Composition:
  $f(\bar{x}) = g(h_1(\bar{x}), ..., h_k(\bar{x}))$,
  if f is the description of the composition from g, h_1, ..., h_k

  2. Bounded recursion on notation:
  $f(\bar{x}, \epsilon) = g(\bar{x})$
  $f(\bar{x}, y0) = h_0(\bar{x}, y, f(\bar{x}, y))_{|_{t(\bar{x},y)}}$
  $f(\bar{x}, y1) = h_1(\bar{x}, y, f(\bar{x}, y))_{|_{t(\bar{x},y)}}$,
  where t is a term of the language $\mathcal{L}$ and f is the description of the bounded recursion on notation defined from g, h_0, h_1 and t;

- Scheme of induction on notation

  $$A(\epsilon) \wedge \forall x \, (A(x) \rightarrow A(x0) \wedge A(x1)) \rightarrow \forall x A(x),$$

  where A is a polytime decidable matrix*, possibly with parameters. The class of polytime decidable matrices is the smallest class of formulas of $\mathcal{L}_\mathcal{P}$ containing the atomic formulas and closed under Boolean operations and quantifications of the form $\forall x \, (x \subseteq t \rightarrow \ldots)$ or $\exists x \, (x \subseteq t \wedge \ldots)$ (usually abbreviated by $\forall x \subseteq t \, (\ldots)$ and $\exists x \subseteq t \, (\ldots)$ respectively).*

The above definition gives simultaneously the theory PTCA and the language $\mathcal{L}_{\mathcal{P}}$ in which it is formulated: the *descriptions* of the polytime computable functions are given by (*a*) and (*b*) above. The proof that these schemes generate exactly the polytime computable functions can be found in [11]. Note that the polytime decidable matrices define exactly the polytime predicates in the standard model (initial subword quantification can be decided in polytime because it only needs a polytime computable search).

We argue that PTCA is a universal theory. This is not immediate because the induction scheme is not constituted by universal formulas. We rely on a well-known result of Łoś and Tarski that states that it is enough to prove that PTCA is preserved by substructures. Let $\mathcal{M}$ be a model of PTCA and let $\mathcal{N}$ be a substructure of $\mathcal{M}$. As we have pointed, we only need to argue that induction on notation also holds in $\mathcal{N}$. Note that the scheme of induction can be reformulated thus:

$$A(\epsilon) \wedge \forall y \subseteq a(A(y) \rightarrow A(y0) \wedge A(y1)) \rightarrow A(a).$$

Therefore, the result follows if it is shown that polytime decidable matrices are absolute between $\mathcal{M}$ and $\mathcal{N}$. This is a consequence of the following result:

Lemma 1. *For each polytime decidable matrix $A(\bar{z}, x)$ there is a function symbol g in $\mathcal{L}_{\mathcal{P}}$ such that* PTCA $\vdash \exists y \subseteq xA(\bar{z}, y) \rightarrow g(\bar{z}, x) \subseteq x \wedge A(\bar{z}, g(\bar{z}, x))$.

It is not difficult to define by bounded recursion on notation a function g whose value is the prefix y of x of smallest length such that $A(\bar{z}, y)$, if there is one such value. (The search argument should be clear, but details can be found in [12], page 141-143.) Note that, if we wanted to search along all words with length less than or equal to $|x|$, bounded recursion on notation would not be enough. Such a (exponential) search goes beyond polytime computability.

We need two auxiliary results. The first says that polytime decidable matrices can be expressed in PTCA by means of quantifier-free formulas. The second states that PTCA allows the definition of functions by cases. (These results are easy to prove; see [12].)

Lemma 2. *For each polytime decidable matrix A, there is a function symbol K_A in $\mathcal{L}_{\mathcal{P}}$ such that* PTCA $\vdash (A(\bar{x}) \rightarrow K_A(\bar{x}) = 1) \wedge (\neg A(\bar{x}) \rightarrow K_A(\bar{x}) = 0)$, *where the free variables of A are among $\bar{x}$.*

Lemma 3. *Given polytime decidable matrices $A_1(\bar{x}), \ldots, A_n(\bar{x})$ and function symbols $f_1(\bar{x}), \ldots, f_n(\bar{x}), f_{n+1}(\bar{x})$ there is a function symbol $f(\bar{x})$ such that the theory* PTCA *proves*

$$(A_1(\bar{x}) \wedge f(\bar{x}) = f_1(\bar{x})) \vee (\neg A_1(\bar{x}) \wedge A_2(\bar{x}) \wedge f(\bar{x}) = f_2(\bar{x})) \vee \ldots$$

$$\vee (\neg A_1(\bar{x}) \wedge \ldots \wedge \neg A_n(\bar{x}) \wedge f(\bar{x}) = f_{n+1}(\bar{x})).$$

By the previous lemmas and the universal axiomatizability of PTCA, the following is immediate by Herbrand's theorem:

Theorem 1. *If* PTCA $\vdash \forall \bar{x} \exists y A(\bar{x}, y)$, *where A is a polytime decidable matrix and $\bar{x}$ and y are the only free variables of A, then there is a function symbol f in $\mathcal{L}_{\mathcal{P}}$ such that* PTCA $\vdash \forall \bar{x} A(\bar{x}, f(\bar{x}))$.

We denote by $x \preceq y$ (respectively, $x \equiv y$) the formula $1 \times x \subseteq 1 \times y$ (respectively, $1 \times x = 1 \times y$). In the standard model $x \preceq y$ (respectively, $x \equiv y$) says that the length of x is less than or equal (respectively, equal) to the length of y. Quantifications of the form $\forall x (x \preceq t \rightarrow \ldots)$ and $\exists x (x \preceq t \wedge \ldots)$ (usually abbreviated by $\forall x \preceq t (\ldots)$ and $\exists x \preceq t (\ldots)$) are called *bounded quantifications*.

Let us now introduce the auxiliary theory PTCA$^+$:

Definition 2. PTCA$^+$ *is the first-order theory whose axioms are those of* PTCA *plus the following scheme of induction on notation:*

$$B(\epsilon) \wedge \forall x (B(x) \rightarrow B(x0) \wedge B(x1)) \rightarrow \forall x B(x),$$

where $B(x)$ is of the form $\exists y \preceq t\, A(y, x)$, where $A(y, x)$ is quantifier-free (possibly with parameters), and t is a term in which y does not occur.

The formulas of the form B above define exactly the NP-sets in the standard model (see [11]). The increase in induction (from polytime to non-deterministic polytime) does not change the provably total functions (with polytime graphs) of the theory. The result below should be compared with the classic result of Charles Parsons (independently obtained by Gaisi Takeuti and Grigori Mints) that says that the provably total functions of Σ_1^0-IND are the primitive recursive functions. For appropriate references to this classical result and a new proof of it, see [15].

Theorem 2. *If* PTCA$^+$ $\vdash \forall \bar{x} \exists y A(\bar{x}, y)$, *where A is a polytime decidable matrix and $\bar{x}$ and y are the only free variables of A, then* PTCA $\vdash \forall \bar{x} \exists y A(\bar{x}, y)$.

Proof. Let us consider the theory PTCA$^+$ given by a universal axiomatization $\mathcal{A}$ of PTCA (we take the formulas in $\mathcal{A}$ to be quantifier-free), together with the induction scheme of Definition 2. Now, let us formulate PTCA$^+$ in Gentzen's sequent calculus by adding to the usual initial sequents and rules for predicate logic with equality, the following initial sequents and rule:

- the initial sequents of the form $\longrightarrow A$, with A in $\mathcal{A}$;
- the induction rule

$$\frac{\Gamma, B(x) \longrightarrow \Delta, B(x0) \qquad \Gamma, B(x) \longrightarrow \Delta, B(x1)}{\Gamma, B(\epsilon) \longrightarrow \Delta, B(s)}$$

where $B(x)$ is of the form $\exists w \preceq t\, A(w, x)$, with $A(w, x)$ a quantifier-free formula (possibly with parameters), t is a term in which w does not occur, s is any term, and the variable x does not occur free in Γ or Δ (it is an eigenvariable).

Suppose that PTCA$^+$ $\vdash \forall \bar{x} \exists y A(\bar{x}, y)$, where (w.l.o.g.) A is quantifier-free. Our goal is to prove that PTCA $\vdash \forall \bar{x} \exists y A(\bar{x}, y)$. Take $\mathcal{P}$ a proof of $\longrightarrow \exists y A(\bar{x}, y)$ in the sequent calculus described above. By Gentzen's cut elimination theorem adapted to our setting (more precisely partial cut elimination, also called the free-cut elimination theorem) we know that there is a proof $\mathcal{P}'$ of $\longrightarrow \exists y A(\bar{x}, y)$, in the sequent calculus above, in which every cut formula comes from an initial sequent or from a principal formula in the induction rule. Therefore, by the subformula property of the calculus, every formula in the proof $\mathcal{P}'$ is a subformula of the conclusion or of a cut formula. In both cases, it is a quantifier-free formula or an existential formula.

7

The result follows if we manage to prove that, for every sequent $\Gamma \longrightarrow \Delta$ in the proof $\mathcal{P}'$, we have $\mathsf{PTCA} \vdash \wedge\Gamma \to \vee\Delta$ (where $\wedge\Gamma$, respectively $\vee\Delta$, denotes the conjunction, respectively disjunction, of the formulas in Γ, respectively in Δ). The proof is by induction on the number of lines of $\mathcal{P}'$. The only case requiring attention is the induction rule. Suppose that the result holds for the two premisses of the induction rule, i.e. $\mathsf{PTCA} \vdash \wedge\Gamma \wedge B(x) \to \vee\Delta \vee B(xi)$, for $i = 0, 1$. We want to prove that it also holds for the conclusion of the rule, i.e. $\mathsf{PTCA} \vdash \wedge\Gamma \wedge B(\epsilon) \to \vee\Delta \vee B(s)$.

By Theorem 1, it is possible to show that there are function symbols h_0 and h_1 such that PTCA proves:

$$(\wedge\Gamma \wedge \neg \vee \Delta) \to \exists \bar{y}_i \forall x \forall w \, (w \preceq t(x) \wedge A(w, x) \to h_i(\bar{y}_i, x, w) \preceq t(xi) \wedge A(h_i(\bar{y}_i, x, w), xi)),$$

for $i = 0, 1$. Of course, this fact relies crucially on the fact that the formulas in Γ and Δ are either quantifier-free or existential (see [12], pages 144-147, for details).

We now reason in PTCA. Assume that we have $\wedge\Gamma$, $\neg \vee \Delta$ and $B(\epsilon)$. We want to prove $B(s)$. By the property above, we know that there are $\bar{a}_0$ and $\bar{a}_1$ satisfying

$$(\wedge\Gamma \wedge \neg \vee \Delta) \to \forall x \forall w \, (w \preceq t(x) \wedge A(w, x) \to h_i(\bar{a}_i, x, w) \preceq t(xi) \wedge A(h_i(\bar{a}_i, x, w), xi)),$$

for $i = 0, 1$. It is not difficult to define a function f, by bounded recursion on notation, such that: $f(\bar{y}_0, \bar{y}_1, u, \epsilon) = u$ and $f(\bar{y}_0, \bar{y}_1, u, xi) = h_i(\bar{y}_i, x, f(\bar{y}_0, \bar{y}_1, u, x))$, $i = 0, 1$. Since $B(\epsilon)$ holds, take c such that $c \preceq t(\epsilon)$ and $A(c, \epsilon)$. By induction on notation on x it is possible to argue that, for all x, $f(\bar{a}_1, \bar{a}_2, c, x) \preceq t(x)$ and $A(f(\bar{a}_1, \bar{a}_2, c, x), x)$. In particular we have $f(\bar{a}_1, \bar{a}_2, c, s) \preceq t(s)$ and $A(f(\bar{a}_1, \bar{a}_2, c, s), s)$, i.e. $B(s)$. $\qquad\square$

As it is well-known, it is possible to introduce in the theory $\Sigma_1^0\text{-}\mathsf{IND}$ all primitive recursive functions (this is essentially done in the famous incompleteness paper of Gödel) and, therefore, PRA can be considered a subtheory of $\Sigma_1^0\text{-}\mathsf{IND}$. Of course, given the paucity of primitive function symbols in the language of Peano arithmetic, the availability of induction for Σ_1^0-formulas is crucial in this regard (mere bounded quantification in the language of Peano arithmetic obviously does not suffice). A similar phenomenon takes place in our setting. Let us look at the situation.

Let $x \subseteq^* y$ abbreviate the formula $\exists w \subseteq y \, (wx \subseteq y)$. The meaning of this relation is clear: x is a subword (not necessarily an initial subword) of y. The class of *subword quantification formulas*, abbreviated sw.q.-formulas, is the smallest class of formulas of $\mathcal{L}$ containing the atomic formulas and closed under Boolean operations and subword quantifications, i.e. of the form $\forall x (x \subseteq^* t \to \ldots)$ or $\exists x (x \subseteq^* t \wedge \ldots)$, where t is a term in which x does not occur. As usual, subword quantifications can be abbreviated by $\forall x \subseteq^* t (\ldots)$ and $\exists x \subseteq^* t (\ldots)$, respectively. The reader should note that the sets of the standard model defined by sw.q.-formulas are polytime computable (but by no means exhaust this class). This is clear because the number of subwords of a word is quadratic in the length of the given word (therefore, the needed searches are polytime computable). The following definition is important:

Definition 3. *A Σ_1^b-formula is a formula of the form $\exists x (x \preceq t(\bar{z}) \wedge A(\bar{z}, x))$, usually written as $\exists x \preceq t(\bar{z}) \, A(\bar{z}, x)$, where A is a sw.q.-formula and x does not occur in the term t. Π_1^b-formulas are defined dually.*

It is possible to show that the Σ_1^b-formulas define exactly the NP-sets in the standard model. (This is somewhat reminiscent of the fact that the Σ_1^0-formulas define the recursively enumerable sets.) The reason for this lies in the fact that sw.q.-formulas are expressive enough to describe computations of Turing machines (see [11] for details).

Definition 4. Σ_1^b-NIA *is the first-order theory,*[1,2] *formulated in the language $\mathcal{L}$, which has the following axioms:*

- *The* basic axioms *of Definition 1.*

- *The* scheme of induction on notation

$$A(\epsilon) \wedge \forall x\,(A(x) \rightarrow A(x0) \wedge A(x1)) \rightarrow \forall x A(x),$$

  where A is a Σ_1^b-formula, possibly with other free variables besides x.

In [11], it was shown that the class of polytime decidable matrices is closed under subword quantification (modulo equivalence in PTCA). Hence Σ_1^b-NIA is a subtheory of PTCA$^+$. On the other hand, it is possible (and relatively easy) to present for each $f(\overline{x}) \in \mathcal{L}_{\mathcal{P}}$ a Σ_1^b-formula $F_f(\overline{x}, y)$ in the language $\mathcal{L}$ such that Σ_1^b-NIA $\vdash \forall \overline{x}\,\exists^1 y\, F_f(\overline{x}, y)$ and which has the defining properties of f (as given by the axioms in Definition 1). The proof is by induction on the complexity of the description of f (the details can be found in [12]). We can subsume the above discussion by the following result:

Proposition 1. *Every model of Σ_1^b-NIA can be extended to a model of PTCA$^+$ by defining the interpretation of each function symbol $f \in \mathcal{L}_{\mathcal{P}}$ via F_f.*

3   Adding bounded collection

In this section we are going to enrich the theory Σ_1^b-NIA with a bounded collection scheme. As already discussed, this principle plays a pivotal role in setting up systems of weak analysis. Once more, we are going to use a cut-elimination technique to prove that the enriched theory is conservative over Σ_1^b-NIA concerning Π_2^0-formulas.

The *bounded formulas* of $\mathcal{L}$ consist of the smallest class of formulas containing the atomic formulas and closed under Boolean connectives and bounded quantifications. The *principle of bounded collection*, denoted by BΣ_∞^b, is the following scheme:

$$\forall x \leq a\,\exists y A(x, y) \rightarrow \exists z \forall x \leq a\,\exists y \leq z A(x, y),$$

where A is a bounded formula (possibly with parameters) and z is a new variable.

For technical reasons pertaining to the formulation of an efficient calculus of sequents, in this section (and in Section 6) we consider that the language $\mathcal{L}$ has *primitive bounded quantifiers*. I.e., if A is a formula of $\mathcal{L}$, we introduce the formulas $\forall x \leq t\,A$ and $\exists x \leq t\,A$ (with t a term where x does not occur) as new formulas, instead of mere abbreviations of $\forall x\,(x \leq t \rightarrow A)$ and $\exists x\,(x \leq t \wedge A)$, respectively.

---

[1]This theory was originally named Σ_1^b-PIND (see [11, 12]). The current denomination stands for *Notation Induction Axiom* and follows the terminology in [2].

[2]This theory is defined in the spirit of Buss's seminal theory S_2^1 ([3]).

In analogy with the formulation of PTCA^+ given in the proof of Theorem 2, we formulate Σ_1^b-NIA in Gentzen's sequent calculus with the corresponding rule for induction on notation (for Σ_1^b-formulas). We add the following rules for the bounded quantifiers:

$$\frac{\Gamma, A(t) \longrightarrow \Delta}{\Gamma, t \leq s, \forall x \leq sA(x) \longrightarrow \Delta} \ \forall_{\leq} : l \qquad \frac{\Gamma, b \leq t \longrightarrow \Delta, A(b)}{\Gamma \longrightarrow \Delta, \forall x \leq tA(x)} \ \forall_{\leq} : r$$

$$\frac{\Gamma, b \leq t, A(b) \longrightarrow \Delta}{\Gamma, \exists x \leq tA(x) \longrightarrow \Delta} \ \exists_{\leq} : l \qquad \frac{\Gamma \longrightarrow \Delta, A(t)}{\Gamma, t \leq s \longrightarrow \Delta, \exists x \leq sA(x)} \ \exists_{\leq} : r$$

where b is an eigenvariable (it is not free in either Γ, Δ or t). Of course, with these rules it is possible to prove the equivalences $\forall x \leq tA \leftrightarrow \forall x\,(x \leq t \to A)$ and $\exists x \leq tA(x) \leftrightarrow \exists x\,(x \leq t \wedge A)$.

Theorem 3. *The theory Σ_1^b-$\mathsf{NIA} + B\Sigma_\infty^b$ is Π_2^0- conservative over the theory Σ_1^b-NIA.*

Proof. The theory Σ_1^b-$\mathsf{NIA} + B\Sigma_\infty^b$ can be formulated in the sequent calculus described above together with the following rule for bounded collection:

$$\frac{\Gamma \longrightarrow \Delta, \forall x \leq t\exists yA(x, y)}{\Gamma \longrightarrow \Delta, \exists z\forall x \leq t\exists y \leq zA(x, y)}$$

where A is a bounded formula.

Suppose that Σ_1^b-$\mathsf{NIA} + B\Sigma_\infty^b \vdash \forall x\exists yA(x, y)$ with A a bounded formula. Then, there is a proof of $\longrightarrow \exists yA(x, y)$ in the sequent calculus above. The free-cut elimination theorem ensures that there is a proof $\mathcal{P}$ of $\longrightarrow \exists yA(x, y)$ without free cuts. As a consequence, all formulas occurring in the sequents $\Gamma \longrightarrow \Delta$ in $\mathcal{P}$ are Σ_1^0-formulas, i.e. of the form $\exists yB(x, y)$, with B a bounded formula.

Let $\Gamma \longrightarrow \Delta$ be a sequent in $\mathcal{P}$, where Γ is $\exists x_1 B_1(x_1, x), \ldots, \exists x_n B_n(x_n, x)$ and Δ is $\exists y_1 C_1(y_1, x), \ldots, \exists y_k C_k(y_k, x)$, with $B_1, \ldots, B_n, C_1, \ldots, C_k$ bounded formulas (we admit the absence of existential quantifiers to accommodate bounded formulas in the sequent). It can be proved, by induction on the number of lines of the proof $\mathcal{P}$, that from bounds of the antecedents we can get (in Σ_1^b-NIA) bounds for the consequents in the following way:

$$\Sigma_1^b\text{-}\mathsf{NIA} \vdash \forall u\exists v\forall x \leq u\,(\Gamma^{\leq u} \to \Delta^{\leq v}),$$

where $\Gamma^{\leq u}$ abbreviates $\exists x_1 \leq uB_1(x_1, x) \wedge \ldots \wedge \exists x_n \leq uB_n(x_n, x)$ and $\Delta^{\leq v}$ abbreviates $\exists y_1 \leq vC_1(y_1, x) \vee \ldots \vee \exists y_k \leq vC_k(y_k, x)$. The proof of this is not difficult. We do not give a proof because the situation will reappear in a stronger context in Section 6.

If we apply the above result to the last sequent of $\mathcal{P}$, we get

$$\Sigma_1^b\text{-}\mathsf{NIA} \vdash \forall u\exists v\forall x \leq u\exists y \leq vA(x, y).$$

It follows that Σ_1^b-$\mathsf{NIA} \vdash \forall x\exists yA(x, y)$. $\qquad\qquad\square$

The above result (and proof-technique) is due to Samuel Buss [4]. For model-theoretic proofs see also [4] and [14]. This latter paper has a very general formulation of the above theorem. For a proof using the bounded functional interpretations see [19].

10

4   A theory of analysis for polytime computability

In this section we define the basic second-order theory for polytime computability. Let $\mathcal{L}_2$ be the second-order language (a two-sorted language) which is the result of adding to $\mathcal{L}$ second-order variables X, Y, Z, ... (intended to vary over subsets of $\{0, 1\}^*$) and a binary relation symbol $\in$ which infixes between a term of $\mathcal{L}$ and a second-order variable. The terms of $\mathcal{L}_2$ are the same as the terms of $\mathcal{L}$ and we have similar definitions of bounded, Σ_1^b, and Π_1^b-formulas: we just have to take into account that in the present setting we have new atomic formulas of the form $t \in X$ (set parameters are permitted).

One needs to be clear about the semantics for second-order theories. The semantics of this paper (as well as of the ordinary studies of subsystems of analysis, weak or strong) is the so-called *Henkin semantics*. This means that a structure for $\mathcal{L}_2$ consists of a first-order structure $\mathcal{M}$ for the first-order part of the language and a subset S of the power set of the domain of $\mathcal{M}$ for the range of the second-order variables. Note that S need not be the full power set of the domain of $\mathcal{M}$. As it is well-known, the semantics with the full power set is not axiomatizable whereas Henkin semantics is essentially a first-order semantics (enjoying a completeness and compactness theorem, for instance).

The theory defined below was introduced by the second author in [13], where some conservation results were proved (like the theorem of this section). The system can play the role of a *feasible* base theory for *reverse mathematics* in analogy with RCA_0 which is commonly chosen as the base system for reverse mathematics [26] in the primitive recursive environment. (At this point, we must refer to the system RCA_0^* studied in the paper [27] which has some similitudes to weak systems with regard to the treatment of bounded quantifications. It is, however, a system with exponentiation.) In Section 8, we briefly discuss these matters.

Definition 5. BTFA *(acronym for* Base Theory for Feasible Analysis*) is the second-order theory, in the language* $\mathcal{L}_2$*, whose axioms are those of* $\Sigma_1^b\text{-}\mathsf{NIA} + \mathsf{B}\Sigma_\infty^b$ *plus the following comprehension scheme:*

$$\forall x \, (\exists y A(x, y) \leftrightarrow \forall z B(x, z)) \to \exists X \forall x \, (x \in X \leftrightarrow \exists y A(x, y))$$

where A is a Σ_1^b*-formula and B is a* Π_1^b*-formula, possibly with first and second-order parameters, and X does not occur in A or B.*

In the definition above, we could have required that the formulas A and B be sw.q.-formulas because first-order bounded quantifications can be absorbed into (plain unbounded) first-order quantifications of the same type. We choose the *definition* above for conceptual clarity since the simplified situation is peculiar to polytime computability (nevertheless, we work with the simplified version in the proof of the theorem below). For systems related to stronger complexity classes (e.g., polyspace computability) one must also work with second-order bounded quantifications (see Section 6) and these cannot be absorbed into first-order quantifications.

We will need the following technical lemma. It states that subword quantifications do not lead to formulas outside the Σ_1^b-class. The result is similar to other cases in logic and the proof does not present difficulties (see [12]). Therefore, we omit it.

Lemma 4. *Let $F(x, y)$ be a Σ_1^b-formula, possibly with (first or second-order) parameters. Then the theory* BTFA *proves*

$$\forall x \subseteq^* a \, \exists y \le w \, F(x, y) \to \exists u \le w \times a1 \times a1 \, \forall x \subseteq^* a \, \exists y \subseteq^* u \, (y \le w \wedge F(x, y)).$$

The proof of the next result follows familiar lines. Its idea is the same as when one proves model-theoretically that the theory RCA_0 is first-order conservative over Σ_1^0-IND: one can always enrich a given first-order model of the latter theory by declaring that the second-order domain consists of all its recursive sets (i.e., simultaneously defined by Σ_1^0 and Π_1^0-formulas). The resulting second-order structure is a model of RCA_0. Therefore, if a first-order sentence fails in some model of Σ_1^0-IND it also fails in some model of RCA_0. By the completeness theorem, this shows that RCA_0 is a first-order conservative extension of Σ_1^0-IND. For a reference, see [26]. In the proof below, we focus on the role of bounded collection and on the need for Σ_1^b-induction on notation (as opposed to mere induction on notation for polytime decidable matrices).

Theorem 4. BTFA *is first-order conservative over* Σ_1^b-NIA $+$ BΣ_∞^b.

Proof. Let $\mathcal{M}$ be a model of Σ_1^b-NIA $+$ BΣ_∞^b. Denote by M the domain of $\mathcal{M}$. Let S be the class of all subsets X of M which can be defined in $\mathcal{M}$ simultaneously by formulas of the form $\exists y A(x, y)$ and $\forall z B(x, z)$, with $A(x, y)$ and $B(x, z)$ sw.q.-formulas (possibly with parameters from M). We show that the second-order structure $(\mathcal{M}, S)$, obtained from $\mathcal{M}$ by adjoining S as the second-order domain, is a model of BTFA. We first argue that, to each sw.q.-formula $C(\overline{x})$ of $\mathcal{L}_2$ with designated free first-order variables $\overline{x}$ (possibly with parameters from M and S), we can associate two formulas $C_\Sigma(\overline{x})$ and $C_\Pi(\overline{x})$ of $\mathcal{L}$ of the form $\exists y A(\overline{x}, y)$ and $\forall z B(\overline{x}, z)$ (respectively), with $A(\overline{x}, y)$ and $B(\overline{x}, y)$ sw.q.-formulas (possibly with parameters from M), such that $\mathcal{M} \models \forall \overline{x} \, (C_\Sigma(\overline{x}) \leftrightarrow C_\Pi(\overline{x}))$ and $(\mathcal{M}, S) \models \forall \overline{x} \, (C(\overline{x}) \leftrightarrow C_\Sigma(\overline{x}))$. It is clear that the existence of these formulas implies that the scheme of comprehension holds in $(\mathcal{M}, S)$. The construction of C_Σ and C_Π is by induction on the complexity of C. For example, in the simple atomic case $C :\equiv x \in X$, we take $C_\Sigma(x)$ and $C_\Pi(x)$ as being, respectively, the formulas $\exists y A(x, y)$ and $\forall z B(x, z)$, where $A(x, y)$ and $B(x, y)$ are as in the defining formulas of the parameter X of S. The Boolean cases are not difficult to deal and subword quantification only poses a difficulty in the two cases of unmatching types of quantification. So, let us consider the case $C(x, v) :\equiv \forall u \subseteq^* v \, D(x, u)$. The construction of $C_\Sigma(x, v)$ relies on the previous lemma and on BΣ_∞^b. Let us analyze the situation. By induction hypothesis, let $D_\Sigma(x, u)$ be $\exists y A(x, u, y)$, with $A(x, u, y)$ a sw.q.-formula. A simple application of BΣ_∞^b shows the following equivalence: $C(x, v) \leftrightarrow \exists w \forall u \subseteq^* v \exists y \le w \, A(x, u, y)$. By Lemma 4, the right-hand side of the above equivalence can be put in the form of an existential quantification followed by a sw.q.-formula. This gives our formula $C_\Sigma(x, v)$.

Let us now argue that induction on notation for Σ_1^b-formulas holds in $(\mathcal{M}, S)$. Suppose that $(\mathcal{M}, S) \models A(\epsilon) \wedge \neg A(a)$, with $a \in M$ and $A(x)$ a Σ_1^b-formula. We want to find a $c \in M$ such that $(\mathcal{M}, S) \models A(c) \wedge \neg A(ci)$ (i=0 or i=1) and $ci \subseteq a$. Let $A(x)$ be $\exists w \le t \, B(x, w)$, with $B(x, w)$ a sw.q.-formula. Let $B_\Sigma(x, w) :\equiv \exists y B_1(x, w, y)$ and $B_\Pi(x, w) :\equiv \forall z B_2(x, w, y)$ as above, with $B_1(x, w, y)$ and $B_2(x, w, z)$ sw.q.-formulas satisfying the expected conditions. In particular, we have

$$\mathcal{M} \models \forall x \subseteq a \forall w \le t \, (\exists y B_1(x, w, y) \leftrightarrow \forall z B_2(x, w, z)).$$

12

We claim that there is $b \in M$ such that

$$\mathcal{M} \models \forall x \subseteq a \forall w \preceq t \, (\exists y B_1(x, w, y) \leftrightarrow \exists y \preceq b B_1(x, w, y)).$$

The argument is easy and uses $\mathsf{B}\Sigma^b_\infty$. It follows from what we have that

$$\mathcal{M} \models \forall x \subseteq a \forall w \preceq t \, \exists y, z \, (B_2(x, w, z) \rightarrow B_1(x, w, y)).$$

Hence, by $\mathsf{B}\Sigma^b_\infty$, there is b such that

$$\mathcal{M} \models \forall x \subseteq a \forall w \preceq t \, \exists y, z \preceq b \, (B_2(x, w, z) \rightarrow B_1(x, w, y)).$$

The reader can argue that this b does the job.

It follows from the claim above that, for x a subword of a, $\exists w \preceq t \, B_\Sigma(x, w)$ is equivalent to a Σ^b_1-formula. (Note that a bounded quantifier "$\exists y \preceq b$" intrudes at this point even if we were only considering induction for polytime decidable matrices.) It is now clear that we can get the witness c to the failure of the hypothesis of the (notation) induction principle by applying induction on notation for Σ^b_1-formulas in $\mathcal{M}$. (Given the intrusion of the bounded existential quantification discussed above, the extension from induction on notation for polytime decidable matrices to Σ^b_1-formulas, given by Theorem 2, is necessary for this part of the argument.)

It remains to see that $\mathsf{B}\Sigma^b_\infty$ holds in $(\mathcal{M}, S)$. The proof follows easily from an extension of the construction of C_Σ and C_Π to bounded formulas C (now with *bounded* formulas A and B). The extension uses heavily the $\mathsf{B}\Sigma^b_\infty$ scheme available in $\mathcal{M}$. $\qquad\square$

5 Adding weak König's lemma

In this section, we are going to add a nonconstructive scheme to BTFA, namely (a version) of *weak König's lemma*. Given A a formula of $\mathcal{L}_2$ and x a (first-order) designated variable, we denote by $Tree(A_x)$ the formula:

$$\forall x \forall y \, (A(x) \wedge y \subseteq x \rightarrow A(y)) \wedge \forall u \exists x \equiv u A(x).$$

The second condition is the so-called infinity or limitless condition. Given X a second-order variable, we denote by $Path(X)$ the formula:

$$Tree((x \in X)_x) \wedge \forall x \forall y \, (x \in X \wedge y \in X \rightarrow x \subseteq y \vee y \subseteq x).$$

Weak König's lemma for trees defined by bounded formulas, denoted by Σ^b_∞-WKL, is the following scheme:

$$Tree(A_x) \rightarrow \exists X \, (Path(X) \wedge \forall x \, (x \in X \rightarrow A(x))),$$

where A is a bounded formula and X is a new variable.

The aim of this section is to prove the following theorem:

Theorem 5. BTFA $+ \Sigma^b_\infty$-WKL *is first-order conservative over* BTFA.

We use the method of forcing to prove this theorem. The argument, in the traditional context of RCA_0, is due to unpublished work of Leo Harrington (recently, [17] presented a proof-theoretic proof of this conservation result in the traditional context). The main lemma is the following:

Lemma 5. *Let $(\mathcal{M}, S)$ be a countable model of* BTFA *and let A be a bounded formula (possibly with parameters in the domain of $\mathcal{M}$ and in S) with a designated variable x such that $(\mathcal{M}, S) \models Tree(A_x)$. There is a subset G of the domain of $\mathcal{M}$ such that $(\mathcal{M}, S \cup \{G\})$ is a model of Σ_1^b-$\mathsf{NIA} + \mathsf{B}\Sigma_\infty^b$ and*

$$(\mathcal{M}, S \cup \{G\}) \models Path(G) \wedge \forall x\,(x \in G \rightarrow A(x)).$$

Proof. Let $\mathbb{T}$ be the set of all (limitless) subtrees of A defined by a bounded formula (possibly with parameters in the domain M of $\mathcal{M}$ and in S). The elements of $\mathbb{T}$ are our *forcing conditions*. We order $\mathbb{T}$ by inclusion. If $T, Q \in \mathbb{T}$ we write $T \leqslant Q$ instead of $T \subseteq Q$. Let $\mathbb{G} \subseteq \mathbb{T}$ be a *generic filter* for a sufficiently rich countable class of dense sets.[3] We put $G := \bigcap \mathbb{G}$ and claim that G is indeed a path throught the tree given by A (a so-called generic path).

Fact 1. Let n be a tally element of the domain of $\mathcal{M}$. The set

$$\mathbb{D}_n = \{T \in \mathbb{T} : (\mathcal{M}, S) \models \exists^1 x\,(x \equiv n \wedge x \in T)\}$$

is dense.

Proof of fact 1. Let n be a tally sequence and $T \in \mathbb{T}$. We have to show that some subtree of T is a member of $\mathbb{D}_n$. The following cannot happen:

$$(\mathcal{M}, S) \models \forall x \equiv n\,\exists m\,(n \leq m \wedge \forall z \equiv m\,(x \subseteq z \wedge z \equiv m \rightarrow z \notin T)).$$

Otherwise, by bounded collection, there is a tally m such that all elements of T have length smaller than m, contradicting the limitlessness of T. It easily follows that there is x, with $x \equiv n$, such that $\{z \in T : z \subseteq x \vee x \subseteq z\}$ is limitless. This set is obviously a subtree of T and is clearly in $\mathbb{D}_n$. □ (of fact 1)

Given a tally n, since $\mathbb{G}$ is generic, $\mathbb{G} \cap \mathbb{D}_n \neq \emptyset$. Take $T \in \mathbb{G} \cap \mathbb{D}_n$ and let σ_n be the unique element of T of length n. Using the fact that $\mathbb{G}$ is a filter, it is now clear that $\sigma_n \in \bigcap \mathbb{G}$. By the arbitrariness of n, this entails that G is indeed a (limitless) path.

It is not difficult to argue that Σ_1^b-NIA holds in the generic extension $(\mathcal{M}, S \cup \{G\})$. Actually, this does not depend on the genericity of G. We use the following simple observation (which will be used frequently in the sequel). Let $B(x, p, P, G)$ be a bounded formula with parameters $p \in M$, $P \in S$ (to ease the notation we only consider one parameter of each type) and the generic set G. There is a term $t_B(x, p)$ such that, for

---

[3]A set $\mathbb{D}$ of forcing conditions is called *dense* if, for each forcing condition T, there is a forcing condition Q with $Q \in \mathbb{D}$ and $Q \leqslant T$. The sufficiently rich countable class of dense sets is usually given by the *definable* sets in an extension of the language of set theory containing the *forcing language* (defined later in the proof) and constants for each forcing condition. A *filter* of forcing conditions contains the tree given by A, is closed upwards and, if T and Q are in the filter then there is a forcing condition R in the filter with $R \leqslant T$ and $R \leqslant Q$. A filter is called *generic* if it intersects all the given dense sets. Since the class of dense sets is countable, it is a known fact that for any forcing condition T there is always a generic filter $\mathbb{G}$ such that $T \in \mathbb{G}$.

any element $a \in M$, we have the following equivalence: For all elements $x \le a$ and for all $y \in G$ with $t_B(a, p) \le y$,

$$(\mathcal{M}, S \cup \{G\}) \models B(x, p, P, G) \text{ if, and only if, } (\mathcal{M}, S) \models B^*(x, p, P, y),$$

where $B^*(x, p, P, y)$ is the bounded formula obtained from $B(x, p, P, G)$ by replacing every atomic formula of the form $q \in G$ by $q \subseteq y$. The observation is correct because, to decide a bounded formula, one only has to check below a certain point (the formal proof is straightforward, by induction on the complexity of the formula B). Note that the term t_B does not depend on G.

In order to check that Σ_1^b-NIA holds in the generic extension, take $B(x, G)$ (we omit the parameters of the ground model) a Σ_1^b-formula and $a \in M$ such that $B(a, G)$ is false in $(\mathcal{M}, S \cup \{G\})$. Take $y \in G$ with $t_B(a) \le y$. By the above claim, $(\mathcal{M}, S) \models \neg B^*(a, y)$. Since Σ_1^b-NIA holds in the ground model, either $(\mathcal{M}, S) \models \neg B^*(\epsilon, y)$ or there is $x \subset a$ such that $(\mathcal{M}, S) \models B^*(x, y) \wedge \neg B^*(xi, y)$, where $i \in \{0, 1\}$ is such that $xi \subseteq a$. It is clear that either counterexample lifts to the generic extension.

It remains to check that $B\Sigma_\infty^b$ holds in $(\mathcal{M}, S \cup \{G\})$. It is at this stage that we use the *forcing theorem*. Let us briefly review the basic facts of forcing in our setting. The *forcing language* is the extension of the language of $\mathcal{L}_2$ by addition of new constants for the elements of M and of S together with a constant C (for the generic path). We identify the former constants with the elements themselves. The *forcing relation* is a relation involving forcing conditions and sentences of the forcing language. The definition of the forcing relation (at the atomic level) is as follows:

1. $T \Vdash x = y$ iff $x = y$;

2. $T \Vdash x \in X$ iff $x \in X$;

3. $T \Vdash x \in C$ iff $(\mathcal{M}, S) \models \exists m \forall w \equiv m \, (w \in T \Rightarrow x \subseteq w)$;

for x, y in the domain M, $X \in S$ and T a forcing condition.

Fact 2. If F is an atomic sentence of the forcing language and T is a forcing condition then $T \Vdash F$ if, and only if, $\forall Q \le T \, \exists R \le Q \, (R \Vdash F)$.

Proof of fact 2. We need only discuss the case of atomic sentences $x \in C$. The left to right direction is clear. Assume that $T \nVdash x \in C$. Then, $Q := \{y \in T : x \nsubseteq y\}$ is a *limitless* subtree of T, i.e., $Q \le T$. Obviously, for no $R \le Q$ one has $R \Vdash x \in C$.

$\square$ (of fact 2)

The above fact shows that we are in the presence of a *weak forcing notion*. The definition of the forcing relation to arbitrary sentences is done according to the following recursive scheme:

4. $T \Vdash F \wedge G$ if $T \Vdash F$ and $T \Vdash G$;

5. $T \Vdash \neg F$ if, for all conditions Q with $Q \le P$, $Q \nVdash F$;

6. $T \Vdash \forall x \, F(x)$ if, for all elements $p \in M$, $T \Vdash F(p)$;

7. $T \Vdash \forall X\, F(X)$ if $T \Vdash F(C)$ and, for all $P \in S$, $T \Vdash F(P)$.

As it is well-known, all logical axioms are generically forced (i.e., forced by every condition) and the rules of logical inference are preserved by forcing (in the sense that if a condition forces the premisses then it forces the conclusion). We state this fact just by saying that "weak forcing preserves classical logic". In the remainder of the proof of the lemma, we will use the forcing theorem. It says that, for every formula $F(V)$ of the language (possibly with parameters in the ground model) and every forcing condition T, the condition $T \Vdash F(C)$ holds if, and only if, for *every* generic filter $\mathbb{H}$ such that $T \in \mathbb{H}$, $(\mathcal{M}, S \cup \{H\}) \models F(H)$, where $H = \bigcap \mathbb{H}$.

Fact 3. Let $B(x, X)$ be a bounded formula, possibly with parameters in the ground model, and consider a forcing condition T. The condition $T \Vdash \exists x B(x, C)$ holds if, and only if,

$$(\mathcal{M}, S) \models \exists m \forall y \equiv m\,(y \in T \rightarrow \exists x \leq m\,(t_B(x) \leq m \wedge B^*(x, y))).$$

Proof of fact 3. Assume that the latter condition holds. Let $\mathbb{H}$ be an arbitrary generic filter such that $T \in \mathbb{H}$. By the forcing theorem, we only need to show that the existential statement $\exists x B(x, H)$ holds in $(\mathcal{M}, S \cup \{H\})$. By hypothesis, there is a (tally) element m in M and $x \leq m$ such that

$$(\mathcal{M}, S) \models t_B(x) \leq m \wedge B^*(x, y_0),$$

where y_0 is the truncation of the path H at length m. Of course, this x witnesses the existential statement.

Suppose, now, that the latter condition fails. Let

$$Q = \{y \in T : (\mathcal{M}, S) \models \forall x \leq y\,(t_B(x) \leq y \rightarrow \neg B^*(x, y))\}.$$

It is clear that Q is a tree (it is a limitless one by the assumption). Hence Q is a forcing condition with $Q \leqslant T$. Take a generic filter $\mathbb{H}$ such that $Q \in \mathbb{H}$ and put $H = \bigcap \mathbb{H}$. We claim that

$$(\mathcal{M}, S \cup \{H\}) \models \forall x \neg B(x, H).$$

Note that, by the forcing theorem, this fact entails $T \nVdash \exists x B(x, C)$. To show the claim, consider an arbitrary $x \in M$. Take $y \in H$ with $t_B(x) \leq y$ and $x \leq y$. Since $H \subseteq Q$, by definition of Q, $(\mathcal{M}, S) \models \neg B^*(x, y)$. The claim follows. $\qquad \square$ (of fact 3)

We can now prove that $\mathsf{B}\Sigma^b_\infty$ is forced by every condition T and, as a consequence (forcing theorem), that $\mathsf{B}\Sigma^b_\infty$ holds in every generic extension. An instance of $\mathsf{B}\Sigma^b_\infty$ is a conditional statement. To see that a condition T forces a conditional statement, one must show that if a stronger condition $Q \leqslant T$ forces the antecedent then there is a yet stronger condition $R \leqslant Q$ which forces the consequent. Hence, suppose that $Q \leqslant T$ and $Q \Vdash \forall w \leq a \exists x\, B(w, x)$, where B is a bounded formula of the forcing language (and a comes from M). Then, for every w with $w \leq a$, $Q \Vdash \exists x\, B(w, x)$. According to Fact 3, for every w with $w \leq a$, we have

$$(\mathcal{M}, S) \models \exists m \forall y \equiv m\,(y \in Q \rightarrow \exists x \leq m\,(t_B(x) \leq m \wedge B^*(w, x, y))).$$

Therefore, $(\mathcal{M}, S) \models \forall w \le a \exists m \forall y \equiv m \, (y \in Q \to \exists x \le m \, (t_B(x) \le m \land B^*(w, x, y)))$. Since $B\Sigma_\infty^b$ holds in the ground model, there is a (tally) element m_0 in M such that

$$(\mathcal{M}, S) \models \forall w \le a \forall y \equiv m_0 \, (y \in Q \to \exists x \le m_0 \, (t_B(x) \le m_0 \land B^*(w, x, y))).$$

By the density of $\mathbb{D}_{m_0}$, take a forcing condition R with $R \le Q$ and $R \in \mathbb{D}_{m_0}$. We get

$$(\mathcal{M}, S) \models \forall w \le a \exists x \le m_0 \, (t_B(x) \le m_0 \land B^*(w, x, y_0)),$$

where y_0 is the unique element of R of length m_0. It easily follows from the forcing theorem that $R \Vdash \exists m \forall w \le a \exists x \le m \, B(w, x)$. $\qquad\square$

The above lemma does not provide a model of BTFA because the recursive comprehension scheme is missing. However, as in the proof of Theorem 4, it is possible to close the given model of $\Sigma_1^b\text{-NIA} + B\Sigma_\infty^b$ under this comprehension scheme. In sum, we have accomplished the following: Given a countable model $(\mathcal{M}, S)$ of BTFA and given a bounded formula A (possibly with first and second-order parameters) with designated variable x such that $(\mathcal{M}, S) \models Tree(A_x)$, there is a countable S' with $S \subseteq S' \subseteq \mathcal{P}(M)$ such that $(\mathcal{M}, S')$ is a model of BTFA and

$$(\mathcal{M}, S') \models \exists X \, (Path(X) \land \forall x \, (x \in X \to A(x))).$$

There are only countably many trees of $(\mathcal{M}, S)$ defined by bounded formulas (possibly with parameters in the domain M of $\mathcal{M}$ and in S). We can enumerate all these formulas $A_1, A_2, \ldots$ and get, successively, countable models $(\mathcal{M}, S^1), (\mathcal{M}, S^2), \ldots$ (with $S^1 \subseteq S^2 \subseteq \ldots$) of BTFA such that, for each positive natural number i, $(\mathcal{M}, S^i)$ has paths through the trees given by $A_1, \ldots A_i$. Let $S^\omega = \bigcup_i S^i$. It is easy to argue that $(\mathcal{M}, S^\omega)$ is still a (countable) model of BTFA and that it has paths through all the trees given by bounded formulas *with parameters in M or S*. Of course, there may be other trees: those defined by bounded formulas with second-order parameters in S^ω. However, we can repeat the above operation with ground model $(\mathcal{M}, S^\omega)$ and get a countable model $(\mathcal{M}, S^{\omega+\omega})$ which has paths for all trees defined by bounded formulas with parameters in M or in S^ω. After repeating this process ω-times, we end up with a model $(\mathcal{M}, S^{\omega \cdot \omega})$, where $S^{\omega \cdot \omega} = \bigcup_k S^{\omega \cdot k}$. This is easily seen to be a model of BTFA $+ \Sigma_\infty^b\text{-WKL}$.

We have shown that, given a countable model $(\mathcal{M}, S)$ of BTFA, it is possible to find $S^{\omega \cdot \omega}$ with $S \subseteq S^{\omega \cdot \omega} \subseteq \mathcal{P}(M)$ such that $(\mathcal{M}, S^{\omega \cdot \omega})$ is a model of BTFA $+ \Sigma_\infty^b\text{-WKL}$. Note that the first-order part remains the same. By an easy application of the completeness theorem, it follows that the theory BTFA $+ \Sigma_\infty^b\text{-WKL}$ is first-order conservative over BTFA.

6   On second-order bounded theories of arithmetic

In this section, we make a detour through a setting where the second-order part of the language has a severe restriction: the set variables denote sets which are always bounded by a term of the language. The reason for this diversion is twofold. In the next section, when studying a conservation result concerning a scheme of strict Π_1^1-reflection, we need a stronger form of collection (we need collection for formulas with

first and second-order *bounded* quantifiers). More importantly, when working in theories of bounded arithmetic connected with computational complexity classes stronger than polytime computability, e.g. polyspace computability, FCH or EXPTIME, it is convenient to work with bounded second-order variables. For polyspace computability and exponential time computability, see the theories U_2^1 and V_2^1 (respectively) defined by Buss in [3]. The class FCH is related with the *hierarchy of counting functions*, a class defined by Klaus Wagner in [28] based on an iteration procedure that stems from Leslie Valiant's well-known counting class $\sharp P$. The functions of this hierarchy are all polynomial space computable and the theory related to this class, the so-called theory TCA (theory for counting arithmetic), is contained in U_2^1. See [21] and [22].

Let $\mathcal{L}_2^b$ be the second-order language obtained by adding second-order bounded variables to $\mathcal{L}$ and the relation symbol $\in$ which infixes between a term of $\mathcal{L}$ and a second-order bounded variable.[4] The second-order bounded variables are complexes of the form X^t where X is a (second-order) variable and t is a (first-order) term. As far as the authors are aware, second-order bounded variables were introduced by Buss in his thesis [3]. The intuitive idea is that X^t has only elements x such that $x \leq t$. For ease of reading, often we write $\forall X \leq t\,(...)$ and $\exists X \leq t\,(...)$ instead of the official notation $\forall X^t\,(...)$ and $\exists X^t\,(...)$ (respectively). These quantifiers are called *bounded* second-order quantifiers.

In the following definition, we introduce an auxiliary theory Aux:

Definition 6. Aux *is the theory formulated in the language $\mathcal{L}_2^b$, whose axioms are those of* Σ_1^b-NIA + $B\Sigma_\infty^b$,

$$\forall x \forall X^t (x \in X^t \to x \leq t)$$

for any term t, and the following comprehension scheme

$$\forall x \leq t\,(A(x) \leftrightarrow B(x)) \to \exists X^t \forall x \leq t\,(x \in X^t \leftrightarrow A(x))$$

where A is a Σ_1^b-formula, B is a Π_1^b-formula, possibly with first and second-order parameters, X^t does not occur in A or B and x does not occur in the term t.

It is clear that the theory Aux can be seen as a subtheory of BTFA in a natural manner. Therefore, its provably total functions (with appropriate graphs) are still the polytime computable functions.

The theory Aux can be formulated in Gentzen's sequent calculus by adding to the corresponding formulation of Σ_1^b-NIA + $B\Sigma_\infty^b$ presented in the proof of Theorem 3 two new kinds of initial sequents:

$$s \in X^t \longrightarrow s \leq t$$

where s and t are terms, and

$$\forall x \leq t\,(A(x) \leftrightarrow B(x)) \longrightarrow \exists X^t \forall x \leq t\,(x \in X^t \leftrightarrow A(x))$$

where A is a Σ_1^b-formula, B is a Π_1^b-formula, possibly with first and second-order parameters, X^t does not occur in A or B and x does not occur in t. We also add four new rules for the second-order quantifiers:

---

[4]In this definition, $\mathcal{L}$ is the language of Section 3 with primitive bounded first-order quantifiers.

$$\frac{\Gamma, A(F^t)\longrightarrow\Delta}{\Gamma, \forall X^t A(X^t)\longrightarrow\Delta} \; \forall_{2^{nd}} : l \qquad \frac{\Gamma\longrightarrow\Delta, A(C^t)}{\Gamma\longrightarrow\Delta, \forall X^t A(X^t)} \; \forall_{2^{nd}} : r$$

$$\frac{\Gamma, A(C^t)\longrightarrow\Delta}{\Gamma, \exists X^t A(X^t)\longrightarrow\Delta} \; \exists_{2^{nd}} : l \qquad \frac{\Gamma\longrightarrow\Delta, A(F^t)}{\Gamma\longrightarrow\Delta, \exists X^t A(X^t)} \; \exists_{2^{nd}} : r$$

with F^t a second-order variable and C^t a second-order eigenvariable.

We say that a formula is in the class $\Sigma^{1,b}_\infty$ if it belongs to the smallest class of formulas containing the atomic formulas and closed under Boolean operations, bounded first-order quantifications and second-order (bounded) quantifications. These are also known as the bounded formulas in the language of $\mathcal{L}^b_2$. The principle of bounded collection for the language $\mathcal{L}^b_2$, denoted by $\mathsf{B}^1\Sigma^{1,b}_\infty$, is the following scheme:

$$\forall X \leq t \exists y A(X^t, y) \rightarrow \exists z \forall X \leq t \exists y \leq z A(X^t, y),$$

where A is a $\Sigma^{1,b}_\infty$-formula (possibly with other first and second-order free variables). It is easy to argue that this form of bounded collection implies the principle $\mathsf{B}\Sigma^b_\infty$.

Proposition 2. $\mathsf{Aux} + \mathsf{B}^1\Sigma^{1,b}_\infty \vdash \mathsf{B}\Sigma^b_\infty$.

Proof. Suppose that $\forall x \leq t \exists y A(x, y)$, with A a bounded formula. We want to prove that $\exists z \forall x \leq t \exists y \leq z A(x, y)$. Let $B(y, X^t)$ be the $\Sigma^{1,b}_\infty$-formula, expressing that when X^t is empty or has more than one element then $y = \epsilon$, and when X^t has a unique element, say x, then y satisfies $A(x, y)$. Formally, $B(y, X^t)$ is

$$(y = \epsilon \wedge \forall x \leq t \; x \notin X^t) \vee (y = \epsilon \wedge \exists x, x' \leq t \, (x \neq x' \wedge x, x' \in X^t)) \vee$$

$$\exists x \leq t \, (A(x, y) \wedge x \in X^t \wedge \forall x' \leq t \, (x \neq x' \rightarrow x' \notin X^t)).$$

By definition of $B(y, X^t)$, we have $\forall X^t \exists y B(y, X^t)$. Applying $\mathsf{B}^1\Sigma^{1,b}_\infty$, we conclude that $\exists z \forall X^t \exists y \leq z B(y, X^t)$. Fix such a z. But then $\forall x \leq t \exists y \leq z A(x, y)$. Just think of the y which corresponds to the singleton set $X^t :\equiv \{x\}$. $\qquad\square$

Theorem 6. *The theory $\mathsf{Aux} + \mathsf{B}^1\Sigma^{1,b}_\infty$ is conservative over the theory Aux with respect to formulas of the form $\forall x \exists y A(x, y)$, with A a $\Sigma^{1,b}_\infty$-formula.*

Proof. The theory $\mathsf{Aux} + \mathsf{B}^1\Sigma^{1,b}_\infty$ can be formulated in Gentzen's sequent calculus (as above), making use of the following new inference rule, we call $\mathsf{B}^1\Sigma^{1,b}_\infty$-*rule*:

$$\frac{\Gamma\longrightarrow\Delta, \exists y A(y, C^t)}{\Gamma\longrightarrow\Delta, \exists z \forall X \leq t \exists y \leq z A(y, X^t)}$$

where A is a $\Sigma^{1,b}_\infty$-formula (possibly with other free variables), C^t is a second-order eigenvariable, and y does not occur in the term t.

Suppose that $\mathsf{Aux} + \mathsf{B}^1\Sigma^{1,b}_\infty \vdash \forall x \exists y A(x, y)$, with A a $\Sigma^{1,b}_\infty$-formula. Then, there is a proof of $\longrightarrow \exists y A(x, y)$ in the sequent calculus above. Applying the free-cut elimination theorem, we know that there is a proof $\mathcal{P}$ of $\longrightarrow \exists y A(x, y)$ without free cuts. Therefore

19

all formulas occurring in the sequents $\Gamma \longrightarrow \Delta$ in $\mathcal{P}$ are of the form $\exists y B(y, x, X^p)$, with B a $\Sigma_\infty^{1,b}$-formula. As usual, the existential quantifier can be absent.

Let $\Gamma \longrightarrow \Delta$ be a sequent in $\mathcal{P}$, where Γ is $\exists x_1 B_1(x_1, x, X^{p(x)}), \ldots, \exists x_n B_n(x_n, x, X^{p(x)})$ and Δ is $\exists y_1 C_1(y_1, x, X^{p(x)}), \ldots, \exists y_k C_k(y_k, x, X^{p(x)})$, where $B_1, \ldots, B_n, C_1, \ldots, C_k$ are $\Sigma_\infty^{1,b}$-formulas. To ease reading, we show only a first-order free variable x and a second-order bounded variable $X^{p(x)}$, instead of tuples of such. Also, we have the same term $p(x)$ for every formula (this can be assumed without loss of generality). We are also only displaying the variable x in the term $p(x)$.

Let us prove, by induction on the number of lines of $\mathcal{P}$, that from bounds of the antecedents we can get (in Aux) bounds for the consequents in the following way:

$$\text{Aux} \vdash \forall u \exists v \forall x \le u \forall X^{p(x)}(\Gamma^{\le u} \to \Delta^{\le v}),$$

where $\Gamma^{\le u}$ abbreviates $\exists x_1 \le u B_1(x_1, x, X^{p(x)}) \wedge \ldots \wedge \exists x_n \le u B_n(x_n, x, X^{p(x)})$ and $\Delta^{\le v}$ abbreviates $\exists y_1 \le v C_1(y_1, x, X^{p(x)}) \vee \ldots \vee \exists y_k \le v C_k(y_k, x, X^{p(x)})$. Note that applying this result to the last sequent of $\mathcal{P}$, we conclude that Aux proves $\forall u \exists v \forall x \le u \exists y \le v A(x, y)$. Thus $\text{Aux} \vdash \forall x \exists y A(x, y)$.

The proof above is going to be illustrated by considering the cut-rule, the $\exists{:}\,r$-rule, the $\forall_{\le}{:}\,r$-rule and the $\text{B}^1\Sigma_\infty^{1,b}$-rule. The other cases are trivial (including the initial sequents and the rules for the second-order bounded quantifiers) or similar to the ones presented; the rules for $\forall{:}\,e$ and $\forall{:}\,d$ do not occur in $\mathcal{P}$ and there is no need to analyze the rule for $\text{B}\Sigma_\infty^b$ because we have shown that this principle is derivable from $\text{B}^1\Sigma_\infty^{1,b}$.

Cut-rule:

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

If A is a $\Sigma_\infty^{1,b}$-formula the result is immediate taking $v :\equiv v_1 \hat{\ } v_2$, where v_1 and v_2 the bounds that exist by induction hypothesis.

Suppose that A is of the form $\exists z D(z, x, X^{p(x)})$ with D a $\Sigma_\infty^{1,b}$-formula. By induction hypothesis we have:

1) $\text{Aux} \vdash \forall u \exists v \forall x \le u \forall X^{p(x)}(\Gamma^{\le u} \to \Delta^{\le v} \vee \exists z \le v D(z, x, X^{p(x)}))$

2) $\text{Aux} \vdash \forall u \exists v \forall x \le u \forall X^{p(x)}(\exists z \le u D(z, x, X^{p(x)}) \wedge \Gamma^{\le u} \to \Delta^{\le v})$.

We want to prove that $\text{Aux} \vdash \forall u \exists v \forall x \le u \forall X^{p(x)}(\Gamma^{\le u} \to \Delta^{\le v})$.

Fix u. By 1) there is v_1 such that $\forall x \le u \forall X^{p(x)}(\Gamma^{\le u} \to \Delta^{\le v_1} \vee \exists z \le v_1 D(z, x, X^{p(x)}))$. Assume that $u \le v_1$ (if not just replace v_1 by $v_1 \hat{\ } u$ that the assertion above remains valid). By 2), there is v_2 such that $\forall x \le v_1 \forall X^{p(x)}(\exists z \le v_1 D(z, x, X^{p(x)}) \wedge \Gamma^{\le v_1} \to \Delta^{\le v_2})$. We get $\forall x \le u \forall X^{p(x)}(\exists z \le v_1 D(z, x, X^{p(x)}) \wedge \Gamma^{\le u} \to \Delta^{\le v_2})$, using the fact that if $u \le u'$ then $\Gamma^{\le u} \to \Gamma^{\le u'}$. Let $v :\equiv v_1 \hat{\ } v_2$. We conclude that $\forall x \le u \forall X^{p(x)}(\Gamma^{\le u} \to \Delta^{\le v})$.

$\exists{:}\,r$-rule:

$$\frac{\Gamma \longrightarrow \Delta, A(t)}{\Gamma \longrightarrow \Delta, \exists x A(x)}$$

Fix u. By induction hypothesis, there is v_1 so that $\forall x \leq u \forall X^{p(x)}(\Gamma^{\leq u} \to \Delta^{\leq v_1} \vee A(t))$. Note that by the construction of $\mathcal{P}$, A is a $\Sigma^{1,b}_\infty$-formula. We want to prove that there is v such that $\forall x \leq u \forall X^{p(x)}(\Gamma^{\leq u} \to \Delta^{\leq v} \vee \exists x \leq v A(x))$. Just take v as being $v_1 \hat{\ } t(u)$.

$\forall_\leq : r$-rule:

$$\frac{a \leq t, \Gamma \longrightarrow \Delta, A(a)}{\Gamma \longrightarrow \Delta, \forall y \leq t A(y)}$$

with a an eigenvariable and A a $\Sigma^{1,b}_\infty$-formula.

We want to prove that $\mathsf{Aux} \vdash \forall u \exists v \forall x \leq u \forall X^{p(x)}(\Gamma^{\leq u} \to \Delta^{\leq v} \vee \forall y \leq t A(y))$. Fix u. Let $u' :\equiv t(u) \hat{\ } u$. By induction hypothesis, there is v' such that

$$\forall x \leq u' \forall X^{p(x)} \forall y \leq u'(y \leq t \wedge \Gamma^{\leq u'} \to \Delta^{\leq v'} \vee A(y)).$$

Thus, $\forall x \leq u \forall X^{p(x)} \forall y \leq u'(y \leq t \wedge \Gamma^{\leq u} \to \Delta^{\leq v'} \vee A(y))$. Just let v be v'.

$\mathsf{B}^1 \Sigma^{1,b}_\infty$-rule:

$$\frac{\Gamma \longrightarrow \Delta, \exists y A(y, C^t)}{\Gamma \longrightarrow \Delta, \exists z \forall Y \leq t \exists y \leq z A(y, Y^t)}$$

By induction hypothesis we know that

$$\mathsf{Aux} \vdash \forall u \exists v \forall x \leq u \forall X^{p(x)} \forall Y^{t(x)}(\Gamma^{\leq u} \to \Delta^{\leq v} \vee \exists y \leq v A(y, Y^{t(x)})).$$

To prove, as we want, that

$$\mathsf{Aux} \vdash \forall u \exists v \forall x \leq u \forall X^{p(x)}(\Gamma^{\leq u} \to \Delta^{\leq v} \vee \exists z \leq v \forall Y^{t(x)} \exists y \leq z A(y, Y^{t(x)})),$$

consider an arbitrary u, take v as the element that exists by induction hypothesis, and let $z :\equiv v$.

The complete proof, in a slightly different context, is given in [20]. □

Theorem 7. *The theory* $\mathsf{BTFA} + \mathsf{B}^1 \Sigma^{1,b}_\infty$ *is conservative over the theory* $\mathsf{Aux} + \mathsf{B}^1 \Sigma^{1,b}_\infty$ *with respect to sentences of the form* $\forall x \exists y A(x, y)$, *where* $A \in \Sigma^{1,b}_\infty$.

Proof. The proof uses a strategy similar to the one applied in Theorem 4 for dealing with the comprehension scheme. Let $\mathcal{M}$ be a model of $\mathsf{Aux} + \mathsf{B}^1 \Sigma^{1,b}_\infty$ with first-order domain M and second-order domain S_b. Let S be the class of all subsets $X \subseteq M$ which can be defined in $\mathcal{M}$ simultaneously by formulas of the form $\exists y A(x, y)$ and $\forall y B(x, y)$, with A a Σ^b_1-formula and B a Π^b_1-formula (possibly with first and second-order parameters from $\mathcal{M}$). Using $\mathsf{B} \Sigma^b_\infty$, it can be proved that $S_b = \{X^a : X \in S \wedge a \in M\}$ (where $X^a = \{x \in X : x \leq a\}$). It can also be argued that the second-order structure $\mathcal{M}^*$, obtained from $\mathcal{M}$ by keeping the same first-order domain and replacing the second-order domain S_b by S, is a model of $\mathsf{BTFA} + \mathsf{B}^1 \Sigma^{1,b}_\infty$. The argument uses the following fact: if $F(x, X)$ is a $\Sigma^{1,b}_\infty$-formula, there is a term $t(x)$ such that, for $c \in M$ and $C \in S$, we have $\mathcal{M}^* \models F(c, C)$ if and only if $\mathcal{M} \models F(c, C^b)$, whenever $t(c) \leq b$.[5] □

---

[5] For the details (in a slightly different context, but easily adapted to the present case), see [20], pp 65-70.

7 Adding strict Π_1^1-reflection

In this section, we go back to the (unbounded) second-order setting and add to BTFA a principle that, in the presence of the totality of the exponential function, is equivalent to weak König's lemma. The principle in question, called *strict Π_1^1-reflection*, is defined by the following scheme:

$$\forall X \exists x A(x, X) \rightarrow \exists u \forall X \exists x \leq u A(x, X),$$

with A a $\Sigma_\infty^{1,b}$-formula (possibly with parameters) in which u does not occur. It is sometimes convenient to present the strict Π_1^1-reflection scheme in its contrapositive form:

$$\forall u \exists X \forall x \leq u \, A(x, X) \rightarrow \exists X \forall x \, A(x, X),$$

with A in the conditions above.

The original version of strict Π_1^1-reflection was introduced by Jon Barwise in the context of admissible set theory (see chapter VIII of [1]). This is perhaps a good place to remark that fragments of arithmetic (weak arithmetic) have similarities with admissibility (the preface of [24] calls attention to these similarities). Strict Π_1^1-reflection was first considered in the weak context by Andrea Cantini in [5]. In this paper, Cantini asks whether strict Π_1^1-reflection is equivalent to weak König's lemma (Cantini shows that the former implies the latter).[6] We conjecture that it is not. The following observation is (essentially) due to Cantini [5]:

Proposition 3. *The theory* BTFA + strict Π_1^1-reflection *proves* $\mathsf{B}^1\Sigma_\infty^{1,b}$.

Proof. Let us reason in BTFA + strict Π_1^1-reflection. Suppose that $\forall X \leq t \exists y A(X, y)$, with A a $\Sigma_\infty^{1,b}$-formula (possibly with parameters). Of course, $\forall X \exists y \tilde{A}(X, y)$, where $\tilde{A}(X, y)$ is the $\Sigma_\infty^{1,b}$-formula $A(X^t, y)$. By strict Π_1^1-reflection, $\exists z \forall X \exists y \leq z \tilde{A}(X, y)$. Such a z satisfies $\forall X \leq t \exists y \leq z A(X, y)$. $\qquad\square$

So, $\mathsf{B}^1\Sigma_\infty^{1,b}$ is a consequence of BTFA + strict Π_1^1-reflection. The next theorem says that, in a sense, the formulas of $\mathsf{B}^1\Sigma_\infty^{1,b}$ are the only non-trivial consequences of *strict Π_1^1-reflection* which do not have second-order unbounded quantifiers.

Theorem 8. *The theory* BTFA + strict Π_1^1-reflection *is conservative over* BTFA + $\mathsf{B}^1\Sigma_\infty^{1,b}$ *with respect to formulas without second-order unbounded quantifiers.*

Proof sketch. Let $(\mathcal{M}, S)$ be a countable model of BTFA + $\mathsf{B}^1\Sigma_\infty^{1,b}$ and $A(x, X)$ be a $\Sigma_\infty^{1,b}$-formula (possibly with first and second-order parameters) such that

$$(\mathcal{M}, S) \models \forall u \exists X \forall x \leq u \, A(x, X).$$

---

[6]Our formulation of strict Π_1^1-reflection is incomparable with Cantini's formulation. On the one hand, it admits a matrix of $\Sigma_\infty^{1,b}$-formulas, instead of just Σ_∞^b-formulas. On the other hand, the form of Cantini's formulation is more general. With his formulation of strict Π_1^1-reflection, Cantini shows that this principle is a Π_2^0-conservative extension of BTFA. For a detailed analysis of a generalization of Cantini's reflection scheme see [8].

We are going to show that there is a subset G of the domain M of $\mathcal{M}$ such that the structure $(\mathcal{M}, S \cup \{G\})$ is a model of Σ_1^b-NIA + $B^1\Sigma_\infty^{1,b}$ in which $\forall x\, A(x, G)$ holds. It is possible to close $S \cup \{G\}$ under our form of recursive comprehension by the argument of the proof of Theorem 7. Let us denote this closure structure by $(\mathcal{M}, S^1)$: this structure is again a model of $BTFA + B^1\Sigma_\infty^{1,b}$ and, moreover, has the same bounded sets as $(\mathcal{M}, S)$. (I.e., the sets of the form X^a with a an element of M coincide for X ranging in S or in S^1). Now, using a chain argument as in the last part of the proof of Theorem 5, there is $S^{\omega\cdot\omega}$, with $S^1 \subseteq S^{\omega\cdot\omega} \subseteq \mathcal{P}(M)$ such that the structure $(\mathcal{M}, S^{\omega\cdot\omega})$ is a model of $BTFA + B^1\Sigma_\infty^{1,b} + \text{strict } \Pi_1^1\text{-reflection}$ with the same bounded sets as the initial structure. This fact, of course, entails our result.

The adjoining of G mimics the forcing construction of the proof of Theorem 5. However, we now use a different notion of tree. In Theorem 5, the forcing conditions are (limitless) trees defined by bounded formulas. The elements of these trees are, of course, the 0-1 strings of the model $\mathcal{M}$ (i.e., the elements of M). Roughly, in our case, the bounded sets of S play the role of the 0-1 strings. One should intuitively view a bounded set as a very long 0-1 string (the "characteristic function" of the bounded set) along the linear order $\leq_l$ defined by

$$x \leq_l y :\Leftrightarrow (x \leq y \wedge x \not\equiv y) \vee (x \equiv y \wedge \exists z \subseteq x(z0 \subseteq x \wedge z1 \subseteq y)) \vee (x = y).$$

Note that $\leq_l$ is defined first according to length and, within the same length, lexicographically. (In the presence of the totality of the exponential function such "long strings" can be obtained from the usual ones.)

After this interlude, take the given $\Sigma_\infty^{1,b}$-formula $A(x, X)$. In analogy to similar properties in other contexts, it is easy to show that there is a term $t_A(x)$ such that, for all a and $x \leq a$, the equivalence between $A(x, X)$ and $A(x, X^b)$ holds in second-order structures of Σ_1^b-NIA for b such that $t_A(a) \leq b$. For simplicity, we write t instead of t_A and we assume, without loss of generality, that $x \leq t(x)$.

We can now describe our forcing conditions. These are sets T of the form

$$\{(a, D^{t(a)}) : a \in M, D \in S \text{ and } (\mathcal{M}, S) \models B(a, D^{t(a)})\},$$

where $B(x, X)$ is a $\Sigma_\infty^{1,b}$-formula (possibly with first and second-order parameters), such that:

1. $(\mathcal{M}, S) \models \forall x \exists X B(x, X^{t(x)})$;

2. $(\mathcal{M}, S) \models \forall X \forall x\, (B(x, X^{t(x)}) \rightarrow \forall y \leq_l x\, B(y, X^{t(y)}))$;

3. $(\mathcal{M}, S) \models \forall x \forall X\, (B(x, X^{t(x)}) \rightarrow \forall u \leq x\, A(u, X^{t(x)}))$.

Intuitively, the first two conditions say that the formula B defines some kind of limitless tree. The third condition just says that T is a subtree of the (limitless, by assumption!) tree associated with the formula A.

Given conditions T and Q, we say that $Q \leq T$ if $Q \subseteq T$. We can now take a generic filter $\mathbb{G}$ of forcing conditions and define:

$$G := \{x \in M : \forall T \in \mathbb{G}\, \exists a \in M, D \in S\, (x \in D \wedge x \leq t(a) \wedge (\mathcal{M}, S) \models (a, D^{t(a)}) \in T)\}.$$

By the genericity of $\mathbb{G}$, it can be shown that, for all $x \in M$, $(\mathcal{M}, S) \models \forall u \leq x\, A(u, G^{t(x)})$. We use the density of the sets $\mathbb{D}_x$ whose members are the forcing conditions containing a single member of the form $(x, X^{t(x)})$. Of course, the proof of the density property of these sets uses the scheme of $\mathsf{B}^1\Sigma_\infty^{1,\mathsf{b}}$.

As before, the forcing language has constants for each element of M and of S and an extra constant C (standing for the generic set G). We define the forcing relation for the relevant atomic sentences, i.e., for sentences of the form $s \in C$. We say that $T \Vdash s \in C$ if

$$(\mathcal{M}, S) \models \exists x \forall X^{t(x)}((x, X^{t(x)}) \in T \rightarrow s \in X^{t(x)}).$$

It is easy to verify that the above is a good weak forcing notion. The forcing relation is extended to all sentences of the forcing language in the standard way. Note that $T \Vdash s \in C$ is a $\exists \Sigma_\infty^{1,\mathsf{b}}$-formula.

It can be shown that the structure $(\mathcal{M}, S \cup \{G\})$ is a model of $\Sigma_1^{\mathsf{b}}\text{-NIA} + \mathsf{B}^1\Sigma_\infty^{1,\mathsf{b}}$ in which $\forall x\, A(x, G)$ holds. The reader can check the details in [8] (there is also related information in [6] and [21]). □

8 Weak analysis digest

In [25], Wilfried Sieg posed the following question: to find a mathematically significant subsystem of analysis whose class of provably recursive functions consists only of the computationally feasible ones. In the last part of his Ph.D. dissertation [11], the second author made a first attempt at investigating mathematics in a weak setting. He considered some basic theorems of analysis in the Cantor space setting. In fact, the discussion of these theorems (e.g., the Heine/Borel covering theorem) is very natural in the Cantor space setting (the case of the closed unit interval poses some minor technical difficulties). Pursuing this line of research, in the mid-nineties the theory BTFA of Section 4 was defined and a few years later, in collaboration with the first author, the paper "Groundwork for weak analysis" [9] was written. As the title suggests, the paper aims at giving the groundwork for developing analysis in a weak setting – in our case in BTFA. The paper defines the real number system and the notion of a real-valued continuous function of a real variable. It proves the intermediate value theorem and, as a consequence, it is shown that the reals form a real closed ordered field. In the last section of the paper, it is shown that BTFA is interpretable in Robinson's theory of arithmetic Q and, as a corollary, one obtains that Tarski's theory of real closed ordered fields is interpretable in Q (a result independently due to Harvey Friedman). It is an open question whether $\text{BTFA} + \Sigma_\infty^{\mathsf{b}}\text{-WKL}$ is interpretable in Q. We conjecture that it is. The same question can be posed for the principle of strict Π_1^1-reflection.

The paper [10] investigates the role of weak König's lemma over BTFA. As discussed in Section 5, the adjunction of $\Sigma_\infty^{\mathsf{b}}\text{-WKL}$ results in a theory that is a first-order conservative extension of BTFA. In [10] it is shown that, over BTFA, the Heine/Borel covering theorem for the closed unit interval is equivalent to weak König's lemma for trees defined by Π_1^{b}-formulas. The Heine/Cantor theorem (which says that every real-valued continuous function on the closed unit interval is uniformly continuous) was also investigated. It was shown that the Heine/Cantor theorem implies weak König's

lemma for *set* trees and is implied by weak König's lemma for trees defined by Π_1^b-formulas. The authors were not able to close the gap.

In reverse mathematics over RCA_0, it is well known that weak König's lemma is sufficient to guarantee that real-valued continuous functions defined on the closed unit interval have a supremum and attain it (see [26]). However, over BTFA, weak König's lemma does not seem to be sufficient to guarantee the existence of the supremum because this fact implies the so-called "slow" principle of induction for Σ_1^b-predicates, where "slow" induction is the following form of induction:

$$A(\epsilon) \land \forall x\, (A(x) \to A(S(x))) \to \forall x A(x).$$

Here, the "successor function" S is defined thus: $S(\epsilon) = 0, S(x0) = x1$ and $S(x1) = S(x)0$. The successor of x is the *next* element after x in the ordering $\leq_l$ of the previous section. In the unary framework of Buss, the above scheme of "slow" induction corresponds to the ordinary "+1" scheme of induction for Σ_1^b-formulas (the mark of Buss' theory T_2^1 of [3]). The paper [10] shows that, over $\mathsf{BTFA} + \Sigma_\infty^b\text{-WKL}$, the scheme of slow induction for Σ_1^b-formulas is equivalent to the existence of the maximum for real-valued continuous functions defined on the closed unit interval. In [29], Takeshi Yamazaki considers the stronger principle $(\star)$: given a real-valued continuous function F defined in $[0,1] \times [0,1]$, there exists a real-valued continuous function G defined on the closed unit interval such that, for all $x \in [0,1]$, $G(x) = \sup_{0 \leq y \leq x} F(x,y)$. Yamazaki, however, uses a different notion of continuous function. Our notion is an adaptation of the usual notion given in [26] to our weak setting. Yamazaki's notion defines a continuous function by approximations of piecewise linear functions with a *modulus of approximation* (see [29] for details). This is a stronger notion than our notion and, in particular, a continuous function in the sense of Yamazaki is automatically uniformly continuous. With this form of continuity, Yamazaki shows that $(\star)$ is equivalent to comprehension for bounded formulas.

On a different direction, the first author considers in [7] a *variation* of the base theory BTFA and shows (by a forcing argument) that a version of Baire's category theorem is first-order conservative over the base theory considered.

The Ph.D. dissertation of the third author [21], as well as [18], studies Riemann integration for real-valued continuous functions defined in closed bounded intervals. It is shown that in the theory TCA^2, a theory related to the computational "counting class" FCH (see the beginning of Section 6), it is possible to define and develop Riemann integration, up to the fundamental theorem of calculus, for continuous functions with a modulus of uniform continuity. It does not seem possible to develop Riemann integration over a weaker base (for instance, over BTFA). The reason is the following: the existence of the Riemann integral implies the possibility of counting the number of elements of a bounded polytime decidable set. This is shown in [16]. Note that the possibility of this counting goes beyond polytime computability (unless certain classes of computational complexity collapse). Nevertheless, it may be possible to define Riemann integration in BTFA using Yamazaki's definition of continuous function, or a related definition (e.g., where the approximating functions are polynomials). It would be nice to see if this is possible, specially if the class of continuous functions considered is sufficiently robust (e.g., contains many analytic functions). Of course, this restricted

class of continuous functions does not seem to coincide with the wider class (the one based on the standard definition in [26]). We believe that this is related to the eventual failure of Weierstrass' approximation theorem in weak settings. Indeed, we conjecture that this theorem is equivalent to the totality of the exponential function over BTFA.

References

[1] J. Barwise. *Admissible sets and structures*. Perspectives in Mathematical Logic. Springer-Verlag, 1975.

[2] W. Buchholz and W. Sieg. A note on polynomial time computable arithmetic. *Contemporary Mathematics*, 106:51–55, 1990.

[3] S. R. Buss. *Bounded arithmetic*. PhD thesis, Princeton University, Princeton, New Jersey, 1985. A revision of this thesis was published by Bibliopolis (Naples) in 1986.

[4] S. R. Buss. A conservation result concerning bounded theories and the collection scheme. *Proceedings of the American Mathematical Society*, 100:109–116, 1987.

[5] A. Cantini. Asymmetric interpretations for bounded theories. *Mathematical Logic Quarterly*, 42(1):270–288, 1996.

[6] A. M. Fernandes. *Investigações em sistemas de análise exequível* (in Portuguese). PhD thesis, Universidade de Lisboa, 2001.

[7] A. M. Fernandes. The Baire category theorem over a feasible base theory. In Stephen Simpson, editor, *Reverse Mathematics 2001*, volume 21 of *Lecture Notes in Logic*, pages 164–174. A K Peters, Massachusetts, 2005.

[8] A. M. Fernandes. Strict Π_1^1-reflection in bounded arithmetic. *Archive for Mathematical Logic*, 49(1):17–34, 2010.

[9] A. M. Fernandes and F. Ferreira. Groundwork for weak analysis. *The Journal of Symbolic Logic*, 67(2):557–578, 2002.

[10] A. M. Fernandes and F. Ferreira. Basic applications of weak König's lemma in feasible analysis. In Stephen Simpson, editor, *Reverse Mathematics 2001*, volume 21 of *Lecture Notes in Logic*, pages 175–188. A K Peters, Massachusetts, 2005.

[11] F. Ferreira. *Polynomial time computable arithmetic and conservative extensions*. PhD thesis, Pennsylvania State University, USA, 1988.

[12] F. Ferreira. Polynomial time computable arithmetic. *Contemporary Mathematics*, 106:137–156, 1990.

[13] F. Ferreira. A feasible theory for analysis. *The Journal of Symbolic Logic*, 59(3):1001–1011, 1994.

[14] F. Ferreira. A note on a result of Buss concerning bounded theories and the collection scheme. *Portugaliae Mathematica*, 52:331–336, 1995.

[15] F. Ferreira. A simple proof of Parson's theorem. *Notre Dame Journal of Formal Logic*, 46:83–91, 2005.

[16] F. Ferreira and G. Ferreira. Counting as integration in feasible analysis. *Mathematical Logic Quaterly*, 52(3):315 – 320, 2006.

[17] F. Ferreira and G. Ferreira. Harrington's conservation theorem redone. *Archive for Mathematical Logic*, 47(2):91–100, 2008.

[18] F. Ferreira and G. Ferreira. The Riemann integral in weak systems of analysis. *Journal of Universal Computer Science*, 14(6):908–937, 2008.

[19] F. Ferreira and P. Oliva. Bounded functional interpretation and feasible analysis. *Annals of Pure and Applied Logic*, 145:115–129, 2005.

[20] G. Ferreira. *Aritmética Computável em Espaço Polinomial* (in Portuguese). Master thesis, Universidade de Lisboa, 2001.

[21] G. Ferreira. *Sistemas de Análise Fraca para a Integração* (in Portuguese). PhD thesis, Universidade de Lisboa, 2006.

[22] G. Ferreira. The counting hierarchy in binary notation. *Portugaliae Mathematica*, 66:81–94, 2009.

[23] G. Ferreira and I. Oitavem. An interpretation of S^1_2 in Σ^b_1-NIA. *Portugaliae Mathematica*, 63(4):427–450, 2006.

[24] G. Sacks. *Higher Recursion Theory*. Perspectives in Mathematical Logic. Springer-Verlag, 1990.

[25] W. Sieg. Hilbert's program sixty years later. *The Journal of Symbolic Logic*, 53:338–348, 1988.

[26] S. G. Simpson. *Subsystems of Second Order Arithmetic*. Perspectives in Mathematical Logic. Springer, Berlin, 1999.

[27] S. G. Simpson and R. Smith. Factorization of polynomials and Σ^0_1 induction. *Annals of Pure and Applied Logic*, 31:289–306, 1986.

[28] K. W. Wagner. Some observations on the connection between counting and recursion. *Theoretical Computer Science*, 47(2):131–147, 1986.

[29] T. Yamazaki. Reverse mathematics and basic feasible systems of 0-1 strings. In Stephen Simpson, editor, *Reverse Mathematics 2001*, volume 21 of *Lecture Notes in Logic*, pages 394–401. A K Peters, Massachusetts, 2005.