Extracting Algorithms from Intuitionistic Proofs

Fernando Ferreira[a)] *and António Marques[b)]

[a)] Departamento de Matemática, Universidade de Lisboa
Rua Ernesto de Vasconcelos, bloco C1-3, 1700 Lisboa, Portugal
[b)] Departamento de Matemática, Instituto Superior Técnico
Av. Rovisco Pais, 1096 Lisboa Codex, Portugal

Abstract. This paper presents a new method – which does not rely on the cut-elimination theorem – for characterizing the provably total functions of certain intuitionistic subsystems of arithmetic. The new method hinges on a realizability argument within an infinitary language. We illustrate the method for the intuitionistic counterpart of Buss's theory S_2^1, and we briefly sketch it for the other levels of bounded arithmetic and for the theory $I\Sigma_1$.

Mathematics Subject Classification: 03F30, 03F55, 03D15.

Key Words: Provably total functions, Intuitionism, Bounded arithmetic.

1 Introduction

Given $A(x, y)$ an arbitrary formula with two free variables x and y, an intuitionistic proof of a sentence of the form $\forall x \exists y A(x, y)$ in a given subsystem of arithmetic yields a computable function f such that $\forall x A(x, f(x))$. Moreover, if the subsystem of arithmetic is suitably expanded by definitions, the assertion $\forall x A(x, f(x))$ should be provable in the system itself. As we vary along subsystems of arithmetic (say, vary along subsystems of Heyting's arithmetic HA), the classes of witness functions become more inclusive the stronger the systems considered. For example, if the assertion $\forall x \exists y A(x, y)$ is provable in the intuitionistic counterpart of Buss's well-known system S_2^1 – the so-called system IS_2^1 defined in [2] – then f is polynomial time computable. If the assertion is provable in the intuitionistic counterpart of the theory $I\Sigma_1$, then f is primitive recursive.

The above cited result on IS_2^1 was proved by Cook and Urquhart in [3], whereas the result on the intuitionist version of $I\Sigma_1$ was recently obtained by Kai Wehmeier in [15]. The argument of Wehmeier is indirect: it reduces, via a realizability argument, the intuitionistic case to the classical case for Π_2 sentences. The proof of Cook and Urquhart hinges on a realizability argument which takes place within a higher-order version of IS_2^1 requiring the use of (feasible) functionals of higher type. At a crucial point one must use a cut-elimination theorem in order to show that this higher-order version is conservative over IS_2^1. Our argument is also a realizability argument, but it circumvents the cut-elimination theorem. Instead of enlarging to a theory of higher types, we enlarge to a theory which permits infinite disjunctions. A conspicuous case of the main axiom schema of this theory is the blatantly *false*,

$$\forall x \bigvee_n \{e\}_n(x) \downarrow \rightarrow \bigvee_n \forall x \{e\}_n(x) \downarrow$$

*This research was partially supported by CMAF and PRAXIS XXI.

where $\{e\}_n(x)\downarrow$ means that the Turing calculation of the machine with Gödel number e for the input x halts in less than $(l_1+l_2+2)^n$ steps, where l_1 and l_2 are, respectively, the lengths of the binary representations of the numbers e and x.

Although this scheme is false, the enlarged infinitary theory is consistent. Moreover, it is conservative over IS^1_2. This result is obtained by a quite simple saturation argument for Kripke-structures (this is what replaces the cut-elimination argument in our setting). The above strategy was first outlined in [5] and, suitably implemented, also yields the characterization of the provably total functions of the upper levels of intuitionistic bounded arithmetic and of the intuitionistic version of $I\Sigma_1$.

The paper is organized as follows. In the section 2 we deal with Buss's theory IS^1_2. Actually, we shall use the binary string framework of Ferreira [6], and work with the intuitionistic version of the theory Σ^b_1-NIA and its extension by definitions $PTCA^+$. To make the paper reasonably self-contained, we briefly describe these theories and leave to an appendix some peculiarities of working in intuitionistic logic. Next, we introduce an infinitary (intuitionistic) false extension $PTCA^+_\infty$ of $PTCA^+$ and define, within it, the pertinent notion of realizability. The characterization of the (intuitionistically) provably total functions of Σ^b_1-NIA is now a consequence of the soundness theorem for this notion of realizability *plus* the fact that the infinitary theory is conservative over the finitary one. The proof of this latter fact is the business of section 3. In the last section we briefly sketch how to adapt the proof of section 2 in order to obtain the (intuitionistically) provably total functions of the upper levels of Buss's hierarchy of bounded theories and of the theory $I\Sigma_1$.

2 Infinitary realizability

In the sequel we briefly describe the first-order theory Σ^b_1-NIA, which is a reformulation of Buss's well-known theory S^1_2 (see [1] or [10]). This reformulation takes place in a stringlanguage L consisting of three constant symbols ϵ, 0 and 1, two binary function symbols $\frown$ (for *concatenation*, sometimes omitted) and $\times$, and a binary relation symbol $\subseteq$ (for *initial subwordness*). There are fourteen basic open axioms:

Ax1. $x \frown \epsilon = x$

Ax2. $x \frown (y \frown 0) = (x \frown y) \frown 0$

Ax3. $x \frown (y \frown 1) = (x \frown y) \frown 1$

Ax4. $x \frown 0 = y \frown 0 \rightarrow x = y$

Ax5. $x \times \epsilon = \epsilon$

Ax6. $x \times (y \frown 0) = (x \times y) \frown x$

Ax7. $x \times (y \frown 1) = (x \times y) \frown x$

Ax8. $x \frown 1 = y \frown 1 \rightarrow x = y$

Ax9. $x \subseteq \epsilon \leftrightarrow x = \epsilon$

Ax10. $x \subseteq y \frown 0 \leftrightarrow x \subseteq y \vee x = y \frown 0$

Ax11. $x \subseteq y \frown 1 \leftrightarrow x \subseteq y \vee x = y \frown 1$

Ax12. $x \frown 0 \neq y \frown 1$

Ax13. $x \frown 0 \neq \epsilon$

Ax14. $x \frown 1 \neq \epsilon$

The standard model of these axioms is the binary tree $\{0,1\}^*$, and the interpretations of the symbols of the stringlanguage in the standard model are immediately clear, except (perhaps) for $\times$: $x \times y$ is the string x concatenated with itself length of y times. We often use $x \subseteq^* y$ for $\exists z \subseteq y\, (z \frown x \subseteq y)$, and abbreviate $1 \times x \subseteq 1 \times y$ by $x \leq y$ (the length of x is less than or equal to the length of y), and $x \subseteq y \wedge x \neq y$ by $x \subset y$. The class of *swq-formulas* ("subword quantification formulae") is the smallest class of formulae containing the atomic formulae and closed under

Boolean operations and subword quantification, i.e., quantification of the form $\forall x \subseteq^* t(\ldots)$ or $\exists x \subseteq^* t(\ldots)$, where t is a term in which the variable x does not occur. A (strict) Σ_1^b-*formula* is a formula of the form $\exists x \leq tA$, where t is a term in which the variable x does not occur and A is a swq-formula. In the standard model these formulas define exactly the sets of the complexity class NP. The theory $\Sigma_1^b - NIA$ (for *Notation Induction Axioms*) consists of the fourteen basic open axioms plus the following induction scheme:

$$F(\epsilon) \wedge \forall x(F(x) \to F(x0) \wedge F(x1)) \to \forall x F(x)$$

where F is a Σ_1^b-formula. This theory is equivalent, in a sense that could be made precise, to Buss's theory S_2^1. Buss's main theorem of his thesis [1] says that whenever $\Sigma_1^b - NIA \vdash \forall x \exists y A(x,y)$, where A is a Σ_1^b formula, there is a polynomial time computable function f such that $A(\sigma, f(\sigma))$, for all $\sigma \in \{0,1\}^*$. Moreover, Buss showed that, if suitably reformulated, the previous conclusion still holds in the theory itself. More specifically, there is a term $t(x)$ of the language L and a Σ_1^b-formula $G_f(x,y)$ such that,

1. $\Sigma_1^b - NIA \vdash \forall x \forall y \, (G_f(x,y) \to A(x,y))$
2. $\Sigma_1^b - NIA \vdash \forall x \exists y \leq t(x) \, G_f(x,y)$
3. $\Sigma_1^b - NIA \vdash \forall x \forall y \forall z \, (G_f(x,y) \wedge G_f(x,z) \to y = z)$
4. for all $\sigma \in \{0,1\}^*$, $\{0,1\}^* \models G_f(\sigma, f(\sigma))$

In fact, it is possible to extend the theory $\Sigma_1^b - NIA$ with function symbols and appropriate axioms for each (description) of a polynomial time computable function, resulting in the so-called theory $PTCA^+$. This possibility hinges on the fact that, for each polynomial time computable (description of a) function f, there is a Σ_1^b-formula $G_f(x,y)$ satisfying the above conditions 2 and 3 *plus* some simple definitional properties within the theory. This was shown in the above mentioned dissertation of Buss, and an account of the result within the framework of the stringlanguage appeared in [6]. Hence, the theory $PTCA^+$ is formulated in a language extension L_P of the L, the new open axioms describe simple definitional properties of the new function symbols, and the induction scheme consists of the notation induction axioms NIA for Σ_1^b-formulas F: in our context of the extended language L_P we may take the Σ_1^b-formulas to be of the form $\exists x \leq tA$, where t is a term in which the variable x does not occur and A is an *open* formula of L_P. Buss's theorem can be reformulated thus: if $\Sigma_1^b - NIA \vdash \forall x \exists y A(x,y)$, where A is a Σ_1^b formula, then there is a function symbol f of L_P such that $PTCA^+ \vdash \forall x A(x, f(x))$.

The point we want to make is that this extension can also be accomplished intuitionistically. In effect, the argument for the classical case is purely intuitionistic except for some uses of the law of excluded middle for swq-formulas. However, it is a theorem that these particular instances of excluded middle are provable intuitionistically in $\Sigma_1^b - NIA$ (see the appendix). [We do not rename the intuitionistic versions of classical theories. When we are working intuitionistically, this will be stated explicitly or it will show up by the use of the subscripted turnstile $\vdash_i$.] Similarly, the law of excluded middle holds for open formulas of $PTCA^+$ (see, once again, the appendix).

We often abuse language and speak of a polynomial time computable function f within the language L_P. We really mean a function symbol of L_P associated with a convenient description of the polynomial time computable function f. Similarly, we sometimes call members of $\{0,1\}^*$ *terms*. What happens is that given an element $e \in \{0,1\}^*$ there is a closed term of the language of L obtained by concatenating (*via* the function symbol $\frown$) the constants 0 and 1 according to the order of the bits in e (for determinateness, we always associate $\frown$ to the left).

We shall need an infinitary version $PTCA_\infty^+$ of the (intuitionistic) theory $PTCA^+$. The language of this version is L_P, and one extends the language of first-order logic to include denumerable disjunctions. The semantics is Kripkean, with the usual clauses of forcing for the first-order logical symbols, plus the following extra clause defining what it means for a node α of a Kripke model to force an infinitary disjunction:

$$\Vdash_\alpha \bigvee_n F_n \quad := \quad \exists m \in \omega \ \Vdash_\alpha F_m$$

The axioms of $PTCA^+_\infty$ are those of $PTCA^+$ plus the following infinitary scheme:

$$\forall x \bigvee_n F_n(x) \to \bigvee_n \forall x \bigvee_{k \leq n} F_k(x)$$

where $F_0(x), F_1(x), F_2(x), \ldots$ is any recursive enumeration of first-order formulas of L_P with only a finite number of parameters.

The following fact will be crucial in the sequel. Its proof is the business of the next section.

Theorem (Conservativity). *Let $A_0, A_1, A_2, \ldots$ be a sequence of (first-order) sentences of L_P. If*

$$PTCA^+_\infty \Vdash \bigvee_n A_n$$

then there is $m \in \omega$ such that,

$$PTCA^+ \vdash_i A_m$$

The notions $\{z\}_n(\overline{x})$ and $\{z\}_n(\overline{x}) \downarrow$ will play a central role in our definition of realizability ($\overline{x}$ abbreviates the k-tuple $x_1, \ldots, x_k$). These notions are familiar: $\{z\}_n(\overline{x})$ is the output of the Turing calculation of the machine with Gödel number z for the input $\overline{x}$, *provided* that this calculation is done in less than $(\ell_1 + \ell_2 + 2)^n$ steps, where ℓ_1 and ℓ_2 are, respectively, the lengths of z and $\overline{x}$ (when the calculation exceeds this number of steps, i.e., when $\{z\}_n(\overline{x}) \downarrow$ does not hold, the default value ϵ is given). To be completely clear, the symbolic notation of these notions requires an extra index k to show their dependence on the number of inputs; however, we will omit this. More importantly, both these notions can be formalized within intuitionistic $PTCA^+$ *via* open formulas. This is done (albeit in another notation) for the classical case in Pudlak's monograph [8]. Pudlak's construction also goes throught in the intuitionistic case since the construction only uses instances of excluded middle for open formulas (of the extended language). A remark is in order. We must be careful in defining the meaning of $\{z\}_n(\overline{x})$ when there are no variables $\overline{x}$: by stipulation, $\{z\}_n(\ )$ is the output of the Turing calculation of the machine with Gödel number z when it starts on an empty tape, provided that this calculation is done in less than $(\ell + 2)^n$ steps, where ℓ is the length of the string z (when the calculation exceeds this number of steps the default value ϵ is given).

We are now ready to define the pertinent notion of realizability for (first-order) formulas of L_P. This notion is a suitable modification of the so-called *q-realizability*, described on page 243 of [14].

Definition (q-realizability). *To every (first-order) formula A of L_p we associate a new formula $z\mathbf{q}A$ of the extended language in such a way that $FV(z\mathbf{q}A) \subseteq FV(A) \cup \{z\}$, and $z \notin FV(A)$, according to the following clauses:*

1. *$z\mathbf{q}A$ is A, if A is an open formula*;
2. *$z\mathbf{q}(A \wedge B)$ is $(z)_0\mathbf{q}A \wedge (z)_1\mathbf{q}B$;*
3. *$z\mathbf{q}(A \vee B)$ is $((z)_0 = \epsilon \to (z)_1\mathbf{q}A) \wedge ((z)_0 \neq \epsilon \to (z)_1\mathbf{q}B)$;*
4. *$z\mathbf{q}(A \to B)$ is $(A \to B) \wedge \forall x(x\mathbf{q}A \to \vee_n(\{z\}_n(x) \downarrow \wedge \{z\}_n(x)\mathbf{q}B))$;*
5. *$z\mathbf{q}\forall x A(x)$ is $\forall x \vee_n (\{z\}_n(x) \downarrow \wedge \{z\}_n(x)\mathbf{q}A(x))$;*
6. *$z\mathbf{q}\exists x A(x)$ is $(z)_0\mathbf{q}A((z)_1)$;*

where $z =< (z)_0, (z)_1 >$ is a suitable pairing coding.

The following mimics a similar result for the usual notion of q-realizability:

Theorem. *If z does not occur in A then*

$$PCTA^+_\infty \Vdash (z\mathbf{q}A) \to A$$

In order to prove a soundness theorem for our notion of realizability, we must use certain results pertaining to the notions of $\{z\}_n(\overline{x})$ and $\{z\}_n(\overline{x}) \downarrow$. All these results are true universal assertions of the language L_P which could have been introduced by *fiat* in the axiomatics of $PTCA^+$ without much ado. We concede that this would have been inelegant. In fact, the desired results are intuitionistically provable in $PTCA^+$. Results 0, 1 and 2 readily follow from Pudlak's discussions in [8], and a version of the crucial last result 5 is also discussed there. Concerning the other two results, we follow Pudlak's common sensical approach: "(...) the proofs in the standard model can be carried out in the fragments of Bounded Arithmetic. We omit the proofs since they are not difficult and contain no essential new ideas."

Result 0. *Given natural numbers $k < s$, the theory $PTCA^+$ proves the following intuitionistically,*

$$\{x\}_k(\overline{y}) \downarrow \to \{x\}_s(\overline{y}) \downarrow \wedge \{x\}_s(\overline{y}) = \{x\}_k(\overline{y})$$

Result 1. *Given f a polynomial time computable function, there is a term $e \in \{0,1\}^*$ and an element $m \in \omega$ such that the theory $PTCA^+$ proves the following intuitionistically,*

$$\forall \overline{x} \, (\{e\}_m(\overline{x}) \downarrow \wedge f(\overline{x}) = \{e\}_m(\overline{x}))$$

Result 2. *Given $n \in \omega$, there is a term $\mu_n \in \{0,1\}^*$ with the following property: for every $k \in \omega$ there is $p \in \omega$ such that the theory $PTCA^+$ proves the following intuitionistically,*

$$\{x\}_k(\overline{y}) \downarrow \to \{\mu_n\}_p(x, \overline{y}) \downarrow \wedge \{\mu_n\}_p(x, \overline{y}) = \{x\}_k(\overline{y})$$

where $\overline{y}$ is a n-tuple of variables.

Result 3. *Given $n, m \in \omega$, there is a $(n+1)$-ary polynomial time computable function $C_{n,m}$ with the following property: for every $k, s_1, \ldots, s_n \in \omega$ there is $p \in \omega$ such that the theory $PTCA^+$ proves the following intuitionistically,*

$$\{y_1\}_{s_1}(\overline{z}) \downarrow \wedge \ldots \wedge \{y_n\}_{s_n}(\overline{z}) \downarrow \wedge \{x\}_k(\{y_1\}_{s_1}(\overline{z}), \ldots, \{y_n\}_{s_n}(\overline{z})) \downarrow \to$$

$$\to \{C_{n,m}(x, y_1, \ldots, y_n)\}_p(\overline{z}) \downarrow \wedge \{C_{n,m}(x, y_1, \ldots, y_n)\}_p(\overline{z}) = \{x\}_k(\{y_1\}_{s_1}(\overline{z}), \ldots, \{y_n\}_{s_n}(\overline{z}))$$

where $\overline{z}$ is an m-tuple of variables.

The next result is a version of the so-called s-m-n-theorem:

Result 4. *Given $n \in \omega$, there is a polynomial time computable function S_n with the following property: for every $k \in \omega$ there is $p \in \omega$ such that the theory $PTCA^+$ proves the following intuitionistically,*

$$\{x\}_k(w, \overline{y}) \downarrow \to \{S_n(x, w)\}_p(\overline{y}) \downarrow \wedge \{S_n(x, w)\}_p(\overline{y}) = \{x\}_k(w, \overline{y})$$

where $\overline{y}$ is a n-tuple of variables.

Result 5. *Given $m \in \omega$ and t a term of the language L, there is a ternary polynomial time computable function $R = R_{m,t}$ with the following property: for every $n, s \in \omega$ there is $p \in \omega$ such that the theory $PTCA^+$ proves the following intuitionistically,*

$$\{v\}_n(\overline{z}) \downarrow \to \{R(v, w_0, w_1)\}_p(\overline{z}, \epsilon) \downarrow \wedge \{R(v, w_0, w_1)\}_p(\overline{z}, \epsilon) = \{v\}_n(\overline{z})$$

and

$$\{R(v, w_0, w_1)\}_p(\overline{z}, x) \downarrow \wedge \{w_0\}_s(\overline{z}, x, \{R(v, w_0, w_1)\}_p(\overline{z}, x) \mid_{t(\overline{z},x)}) \downarrow \to$$

$$\to \{R(v, w_0, w_1)\}_p(\overline{z}, x0) \downarrow \wedge \{R(v, w_0, w_1)\}_p(\overline{z}, x0) = \{w_0\}_s(\overline{z}, x, \{R(v, w_0, w_1)\}_p(\overline{z}, x) \mid_{t(\overline{z},x)})$$

and

$$\{R(v, w_0, w_1)\}_p(\overline{z}, x) \downarrow \wedge \{w_1\}_s(\overline{z}, x, \{R(v, w_0, w_1)\}_p(\overline{z}, x) \mid_{t(\overline{z},x)}) \downarrow \to$$

$$\to \{R(v, w_0, w_1)\}_p(\overline{z}, x1) \downarrow \wedge \{R(v, w_0, w_1)\}_p(\overline{z}, x1) = \{w_1\}_s(\overline{z}, x, \{R(v, w_0, w_1)\}_p(\overline{z}, x) \mid_{t(\overline{z},x)})$$

where $\overline{z}$ is a m-tuple of variables and $a \mid_b$ is the truncation of the string a at the length of b.

We are now ready to state and prove a soundness theorem about our notion of q-realizability.

Theorem (Soundness of q-realizability). *If $PTCA^+ \vdash_i A(\overline{x})$ then there is a term $e \in \{0,1\}^*$ such that*

$$PTCA^+_\infty \Vdash \forall \overline{x} \bigvee_m (\{e\}_m(\overline{x}) \downarrow \wedge \{e\}_m(\overline{x}) \mathbf{q} A(\overline{x}))$$

where the free variables of A are among the variables occurring in $\overline{x}$.

Proof : The proof is by induction on the length of deductions in $PTCA^+$. For determinateness, we work with the deductive system described on page 126 of Dummett's book [4] on intuitionism. In such a scenario we must find realizing terms in $\{0,1\}^*$ for the logical and non-logical axioms and, given a rule of the form $\Gamma \Rightarrow A$, we must be able to associate to every realization of Γ a realization of A. With the exception of the realizability of the induction axioms, the usual arguments for the HA case work for our case with some suitable modifications (remark: in these cases the infinitary axioms are not used). We shall only consider a few typical axioms and rules and, to keep the notation simple, we will usually avoid the consideration of free variables.

The logical axiom $A \to (B \to A)$ is q-realized if we can find a term $e \in \{0,1\}^*$ such that $PTCA^+_\infty$ forces

$$\forall x (x \mathbf{q} A \to (B \to A) \wedge \vee_n (\{e\}_n(x) \downarrow \wedge \forall y (y \mathbf{q} B \to \vee_p (\{\{e\}_n(x)\}_p(y) \downarrow \wedge \{\{e\}_n(x)\}_p(y) \mathbf{q} A))))$$

First note that we need not worry about the conclusion $B \to A$, since $A \to (B \to A)$ is provable and $x\mathbf{q}A$ implies A. According to result 1, there exists $e' \in \{0,1\}^*$ and $m \in \omega$ such that,

$$PTCA^+ \vdash_i \forall x \forall y (\{e'\}_m(x, y) \downarrow \wedge \{e'\}_m(x, y) = x)$$

By result 4 there is $p \in \omega$ such that $PTCA^+ \vdash_i \forall x \forall y (\{S_1(e', x)\}_p(y) \downarrow \wedge \{S_1(e', x)\}_p(y) = x)$. Using again result 1, we can take $e \in \{0,1\}^*$ and $n \in \omega$ such that,

$$PTCA^+ \vdash_i \forall x (\{e\}_n(x) \downarrow \wedge \{e\}_n(x) = S_1(e', x))$$

Thus, for $k = max\{n, p\}$,

$$PTCA^+ \vdash_i \forall x \forall y (\{e\}_k(x) \downarrow \wedge \{\{e\}_k(x)\}_k(y) \downarrow \wedge \{\{e\}_k(x)\}_k(y) = x)$$

It is easy to check that this e does the job.

Now let us consider the axiom $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$. It is enough to find a term $e \in \{0,1\}^*$ such that the following complicated condition obtains:

$$\forall a[(A \to B) \wedge \forall y(y\mathbf{q}A \to \vee_n(\{a\}_n(y) \downarrow \wedge \{a\}_n(y)\mathbf{q}B)) \to \vee_m[\{e\}_m(a) \downarrow \wedge$$

$$\wedge((A \to (B \to C)) \to (A \to C)) \wedge \forall z[z\mathbf{q}(A \to (B \to C)) \to \vee_k(\{\{e\}_m(a)\}_k(z) \downarrow \wedge$$

$$\wedge(A \to C) \wedge \forall u(u\mathbf{q}A \to \vee_s(\{\{\{e\}_m(a)\}_k(z)\}_s(u) \downarrow \wedge \{\{\{e\}_m(a)\}_k(z)\}_s(u)\mathbf{q}C)))]]]$$

where $z\mathbf{q}(A \to (B \to C))$ is the conjunction of $A \to (B \to C)$ with

$$\forall w[w\mathbf{q}A \to (B \to C) \wedge \vee_r[\{z\}_r(w) \downarrow \wedge \forall v(v\mathbf{q}B \to \vee_t(\{\{z\}_r(u)\}_t(v) \downarrow \wedge \{\{z\}_r(w)\}_t(v)\mathbf{q}C))]]$$

A judicious calculation using the above results shows the following: there exists a term $e \in \{0,1\}^*$ and there are $m, k \in \omega$ such that

$$PTCA^+ \vdash_i \forall a \forall z(\{e\}_m(a) \downarrow \wedge \{\{e\}_m(a)\}_k(z) \downarrow)$$

and such that for all $n, r, t \in \omega$ there exists $s \in \omega$ in such a way that the next implication is provable intuitionistically in $PTCA^+$,

$$\{z\}_r(u) \downarrow \wedge \{a\}_n(u) \downarrow \wedge \{\{z\}_r(u)\}_t(\{a\}_n(u)\}_t \downarrow \to$$

$$\to \{\{\{e\}_m(a)\}_k(z)\}_s(u) \downarrow \wedge \{\{\{e\}_m(a)\}_k(z)\}_s(u) = \{\{z\}_r(u)\}_t(\{a\}_n(u))$$

A careful checking shows that the above e realizes our axiom.

Let us now consider the rule *Modus Ponens*. Suppose there are $e_1, e_2 \in \{0,1\}^*$ such that the following two conditions are forced by $PTCA^+_\infty$:

$$\forall \overline{x} \bigvee_{m_1} (\{e_1\}_{m_1}(\overline{x}) \downarrow \wedge \{e_1\}_{m_1}(\overline{x})\mathbf{q}A(\overline{x}))$$

and

$$\forall \overline{x} \bigvee_{m_2} [\{e_2\}_{m_2}(\overline{x}) \downarrow \wedge \forall z\,(z\mathbf{q}A(\overline{x}) \to \bigvee_k (\{\{e_2\}_{m_2}(\overline{x})\}_k(z) \downarrow \wedge \{\{e_2\}_{m_2}(\overline{x})\}_k(z)\mathbf{q}B(\overline{x})))]$$

A straightforward calculation using the above results yields a term $e \in \{0,1\}^*$ such that, for all $m_1, m_2, k \in \omega$ there is $s \in \omega$ in such a way that the following implication is provable intuitionistically in $PTCA^+$,

$$\{e_1\}_{m_1}(\overline{x}) \downarrow \wedge \{e_2\}_{m_2}(\overline{x}) \downarrow \wedge \{\{e_2\}_{m_2}(\overline{x})\}_k(\{e_1\}_{m_1}(\overline{x})) \downarrow \to$$

$$\to \{e\}_s(\overline{x}) \downarrow \wedge \{e\}_s(\overline{x}) = \{\{e_2\}_{m_2}(\overline{x})\}_k(\{e_1\}_{m_1}(\overline{x}))$$

It is easy to check that the above e does the job for $B(\overline{x})$.

The other rule that we will consider is the rule "$C \to A(y) \Rightarrow C \to \forall x A(x)$", where y is free for x in $A(x)$, and does not occur free in C or in $A(x)$ ($A(y)$ is formed by replacing every free occurence of x in $A(x)$ by y). Hence, by hypothesis, there is a term $e \in \omega$ such that $PTCA^+_\infty$ forces,

$$\forall y \bigvee_m \; [\{e\}_m(y) \downarrow \wedge \forall z\,(z\mathbf{q}C \to \bigvee_n (\{\{e\}_m(y)\}_n(z) \downarrow \wedge \{\{e\}_m(y)\}_n(z)\mathbf{q}A(y)))]$$

In particular, using some intuitionistic logic and the fact that y does not occur free in $z\mathbf{q}C$, we get

$$\forall z(z\mathbf{q}C \to \forall y \bigvee_m \bigvee_n (\{\{e\}_m(y)\}_n(z) \downarrow \wedge \{\{e\}_m(y)\}_n(z)\mathbf{q}A(y)))$$

A straightforward calculation shows the following: there is a term $e' \in \{0,1\}^*$ and $s \in \omega$ such that,

$$PTCA^+ \vdash_i \forall z\,(\{e'\}_s(z)\downarrow)$$

and such that, for all $m, n \in \omega$, there exists $p \in \omega$ in such a way that,

$$PTCA^+ \vdash_i \{e\}_m(y)\downarrow \wedge \{\{e\}_m(y)\}_n(z)\downarrow \rightarrow \{\{e'\}_s(z)\}_p(y)\downarrow \wedge \{\{e'\}_s(z)\}_p(y) = \{\{e\}_m(y)\}_n(z)$$

This entails what we want, i.e., that $PTCA^+_\infty$ forces,

$$\forall z\,[z\mathbf{q}C \rightarrow \bigvee_s (\{e'\}_s(z)\downarrow \wedge \forall x \bigvee_p (\{\{e'\}_s(z)\}_p(x)\downarrow \wedge \{\{e'\}_s(z)\}_p(x)\mathbf{q}A(x)))]$$

Finally, we study the induction axioms,

$$F(\epsilon) \wedge \forall x(F(x) \rightarrow F(x0) \wedge F(x1)) \rightarrow \forall x F(x)$$

where F is a Σ_1^b-formula, i.e., a formula of the form $\exists w(w \leq t(x) \wedge G(x,w))$, with G an open formula of the language of L_P. These axioms are implications, and a q-realization of an implication is the conjunction of the implication itself with a certain other statement. The implication itself comes for free, since $PTCA^+_\infty$ forces the induction axioms. (Actually, it is only at this step that we use the full power of the induction axioms in $PTCA^+_\infty$; apart from this instance, in all other steps we only need induction for open formulas of L_P.) Hence, an induction axiom is q-realized if we can find a term $e \in \{0,1\}^*$ such that $PTCA^+_\infty$ forces,

$$\forall y \forall z (y\mathbf{q}F(\epsilon) \wedge z\mathbf{q}\forall x(F(x) \rightarrow F(x0) \wedge F(x1)) \rightarrow \bigvee_p (\{e\}_p(y,z)\downarrow \wedge \{e\}_p(y,z)\mathbf{q}\forall x F(x)))$$

The second conjunction in the antecedent of the main implication of the above formula is,

$$\forall x \bigvee_m (\{z\}_m(x)\downarrow \wedge \forall w(w\mathbf{q}F(x) \rightarrow \bigvee_l (\{\{z\}_m(x)\}_l(w)\downarrow \wedge \{\{z\}_m(x)\}_l(w)\mathbf{q}(F(x0) \wedge F(x1)))))$$

where we have omitted the condition $F(x) \rightarrow F(x0) \wedge F(x1)$ since it will not be needed in the sequel.

The formula "$w\mathbf{q}F(x)$" is "$(w)_1 \leq t(x) \wedge G(x,(w)_1)$"; thus, it is an open formula and, hence, decidable (see the last result of the appendix). This permits to export the disjunction "$\vee_l$" across "$w\mathbf{q}F(x)$", and get the intuitionistically equivalent,

$$\forall x \bigvee_m (\{z\}_m(x)\downarrow \wedge \forall w \bigvee_l (w\mathbf{q}F(x) \rightarrow \{\{z\}_m(x)\}_l(w)\downarrow \wedge \{\{z\}_m(x)\}_l(w)\mathbf{q}(F(x0) \wedge F(x1))))$$

At this point (with the aid of result 0) we apply the infinitary axiom scheme of $PTCA^+_\infty$ and argue intuitionistically to get,

$$\forall x \bigvee_m \bigvee_l (\{z\}_m(x)\downarrow \wedge \forall w(w\mathbf{q}F(x) \rightarrow \{\{z\}_m(x)\}_l(w)\downarrow \wedge \{\{z\}_m(x)\}_l(w)\mathbf{q}(F(x0) \wedge F(x1))))$$

By result 0, we may conflate the two infinitary "ors" into a single "or":

$$\forall x \bigvee_k (\{z\}_k(x)\downarrow \wedge \forall w(w\mathbf{q}F(x) \rightarrow \{\{z\}_k(x)\}_k(w)\downarrow \wedge \{\{z\}_k(x)\}_k(w)\mathbf{q}(F(x0) \wedge F(x1))))$$

Applying once more the infinitary axiom scheme, we conclude that,

$$\bigvee_k \forall x(\{z\}_k(x)\downarrow \wedge \forall w(w\mathbf{q}F(x) \rightarrow \{\{z\}_k(x)\}_k(w)\downarrow \wedge \{\{z\}_k(x)\}_k(w)\mathbf{q}(F(x0) \wedge F(x1))))$$

Let us remind ourselves that, in realizing an induction axiom, the aim is to obtain,

$$\bigvee_p (\{e\}_p(y,z)\downarrow \wedge \forall x \bigvee_r (\{\{e\}_p(y,z)\}_r(x)\downarrow \wedge \{\{e\}_p(y,z)\}_r(x)\mathbf{q}F(x)))$$

and, in order to accomplish this, we may use the conclusion of the discussion above.

It is easy to find a term $v \in \{0,1\}^*$ and $n \in \omega$ such that,

$$PTCA^+ \vdash \forall y \forall z\, (\{v\}_n(y,z)\downarrow \wedge \{v\}_n(y,z) = y_1)$$

A straightforward calculation shows the following: there are terms $w_0, w_1 \in \{0,1\}^*$ such that, for any $k \in \omega$, there exists $s \in \omega$ in such a way that $PTCA^+$ proves intuitionistically both

$$\{z\}_k(x)\downarrow \wedge \{\{z\}_k(x)\}_k(w)\downarrow \rightarrow \{w_0\}_s(y,z,x,w)\downarrow \wedge \{w_0\}_s(y,z,x,w) = (\{\{z\}_k(x)\}_k(<\epsilon, w>))_{01}$$

and

$$\{z\}_k(x)\downarrow \wedge \{\{z\}_k(x)\}_k(w)\downarrow \rightarrow \{w_0\}_s(y,z,x,w)\downarrow \wedge \{w_0\}_s(y,z,x,w) = (\{\{z)\}_k(x)\}_k(<\epsilon, w>))_{11}$$

where, for ease of reading, $(w)_{ij}$ abbreviates $((w)_i)_j$.

We now use result 5. Let $R = R_{2,t}(v, w_0, w_1)$. Thus, given $n, s \in \omega$ as above, there is $q \in \omega$ such that,

$$\{v\}_n(y,z)\downarrow \rightarrow \{R\}_q(y,z,\epsilon)\downarrow \wedge \{R\}_q(y,z,\epsilon) = \{v\}_n(y,z)$$

and

$$\{R\}_q(y,z,x)\downarrow \wedge \{w_0\}_s(y,z,x,\{R\}_q(y,z,x)\mid_{t(x)})\downarrow \rightarrow$$
$$\rightarrow \{R\}_q(y,z,x0)\downarrow \wedge \{R\}_q(y,z,x0) = \{w_0\}_s(y,z,x,\{R\}_q(y,z,x)\mid_{t(x)})$$

and

$$\{R\}_q(y,z,x)\downarrow \wedge \{w_1\}_s(y,z,x,\{R\}_q(y,z,x)\mid_{t(x)})\downarrow \rightarrow$$
$$\rightarrow \{R\}_q(y,z,x1)\downarrow \wedge \{R\}_q(y,z,x1) = \{w_1\}_s(y,z,x,\{R\}_q(y,z,x)\mid_{t(x)})$$

It is now easy to show, by notation induction on x, that

$$\forall x(\{R\}_q(y,z,x)\downarrow \wedge \{R\}_q(y,z,x) \leq t(x) \wedge G(x, \{R\}_q(y,z,x)))$$

A simple calculation obtains a term $e \in \{0,1\}^*$ and $p \in \omega$ such that, for any $q \in \omega$, there exists $r \in \omega$ in such a way that $PTCA^+$ proves intuitionistically,

$$\forall y \forall z\, \{e\}_p(y,z)\downarrow$$

and

$$\{R\}_q(y,z,x)\downarrow \rightarrow \{\{e\}_p(y,z)\}_r(x)\downarrow \wedge \{\{e\}_p(y,z)\}_r(x) = <\epsilon, \{R\}_q(y,z,x)>$$

Clearly, this e does the job. □

Corollary (Cook & Urquhart [3]). *Suppose that $\Sigma_1^b - NIA \vdash_i \forall \overline{x} \exists y A(\overline{x}, y)$, where A is an arbitrary formula of the language L whose free variables are among $\overline{x}$ and y. Then there is a polynomial time computable function f such that,*

$$PTCA^+ \vdash_i \forall \overline{x}\, A(\overline{x}, f(\overline{x}))$$

Proof : Suppose $\Sigma_1^b - NIA \vdash_i \exists y\, A(\overline{x}, y)$ and, *a fortiori*, $PTCA^+ \vdash_i \exists y\, A(\overline{x}, y)$. By the soundness theorem, there is a term $e \in \{0,1\}^*$ such that,

$$PTCA^+_\infty \Vdash \forall \overline{x} \bigvee_m (\{e\}_m(\overline{x}) \downarrow \wedge (\{e\}_m(\overline{x}))_0 \mathbf{q} A(\overline{x}, (\{e\}_m(\overline{x}))_1))$$

Since the q-realizability of a formula implies that formula, we may conclude that,

$$PTCA^+_\infty \Vdash \forall \overline{x} \bigvee_m (\{e\}_m(\overline{x}) \downarrow \wedge A(\overline{x}, (\{e\}_m(\overline{x}))_1))$$

Notice that the disjuncts of the above infinitary disjunction are first-order formulas. Hence, by result 0 and the infinitary axiom of $PTCA^+_\infty$,

$$PTCA^+_\infty \Vdash \bigvee_m \forall \overline{x}\, (\{e\}_m(\overline{x}) \downarrow \wedge A(\overline{x}, (\{e\}_m(\overline{x}))_1))$$

By the conservativeness result there is $n \in \omega$ such that,

$$PTCA^+ \vdash_i \forall \overline{x}\, (\{e\}_n(\overline{x}) \downarrow \wedge A(\overline{x}, (\{e\}_n(\overline{x}))_1))$$

Thus, we may put $f(\overline{x}) := (\{e\}_n(\overline{x}))_1$. □

Corollary. *Suppose that*

$$\Sigma_1^b - NIA \vdash_i \forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_n \exists y_n A(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$$

where A is an arbitrary formula of the language L whose free variables are among $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$. Then there are polynomial time computable functions $f_1, f_2, \ldots, f_n$ such that,

$$PTCA^+ \vdash_i \forall x_1 \forall x_2 \ldots \forall x_n\, A(x_1, f(x_1), x_2, f(x_1, x_2), \ldots, x_n, f(x_1, x_2, \ldots, x_n))$$

Proof : This corollary is a consequence of n applications of the previous corollary. □

3 The saturation argument

The aim of this section is to prove the conservativeness result stated on the previous section. The method of proof is best explained by the words of Dirk van Dalen [13]: “If one looks at a Kripke model from the outside, then it appears as a complicated concoction of classical structures, and hence as a classical structure itself. Such a structure has its own language and we can handle it by ordinary, classical, model-theoretic means.” With a view of establishing the relevant notation, we will briefly sketch the procedure that associates a classical structure to a given Kripke structure. For more details, the reader is referred to the above mentioned work of van Dalen.

Unless otherwise stated, our Kripke structures have a least element, usually denoted by 0. Let $\mathcal{M}$ be a Kripke structure for a certain language $\mathcal{L}$. We will associate to $\mathcal{M}$ a classical structure $\mathcal{M}^c$, formulated in a certain language $\mathcal{L}^c$, according to the following specifications. The language

$\mathcal{L}^c$ is two-sorted: one sort $\alpha, \beta, \gamma, \ldots$ for referring to the nodes of $\mathcal{M}$, and the other sort $x, y, z, \ldots$ for referring to the elements of the worlds of $\mathcal{M}$. This two-sorted language is obtained from $\mathcal{L}$ by replacing each n-ary predicate symbol P (each function symbol f, respectively) by an $(n+1)$-ary predicate symbol P^c (by an $(n+1)$-ary function symbol f^c, respectively), and by adding two new binary predicate symbols $\leq$ and D and a constant 0. The structure $\mathcal{M}^c$ validates the following laws (referred to by Θ):

1. $0 \leq \alpha \wedge \alpha \leq \alpha$
2. $\alpha \leq \beta \wedge \beta \leq \gamma \rightarrow \alpha \leq \gamma$
3. $\alpha \leq \beta \wedge \beta \leq \alpha \rightarrow \alpha = \beta$
4. $D(\alpha, x) \wedge \alpha \leq \beta \rightarrow D(\beta, x)$
5. $P^c(\alpha, \overline{x}) \wedge \alpha \leq \beta \rightarrow P^c(\beta, \overline{x})$
6. $D(\alpha, \overline{x}) \rightarrow D(\alpha, f^c(\alpha, \overline{x}))$
7. $\alpha \leq \beta \rightarrow f^c(\alpha, \overline{x}) = f^c(\beta, \overline{x})$

where $D(\alpha, \overline{x})$ abbreviates $\wedge_{1 \leq i \leq n} D(\alpha, x_i)$, on the supposition that $\overline{x}$ stands for the n-tuple $x_1, x_2, \ldots, x_n$. Note that Θ is such that every model of Θ corresponds uniquely to a Kripke structure.

It is straightforward to translate the forcing clauses into the extended language. Firstly we must define t^c_α, for t a term of $\mathcal{L}$ and α a variable of the node-sort. If t is a variable x, x^c_α is x. If t is $f(t_1, \ldots, t_n)$, then t^c_α is $f^c(\alpha, (t_1)^c_\alpha, \ldots, (t_n)^c_\alpha)$. We are now ready to give the clauses for translating the forcing relation:

1. $(\Vdash_\alpha P(t_1, \ldots, t_n))^c$ is $P^c(\alpha, (t_1)^c_\alpha, \ldots, (t_n)^c_\alpha)$
2. $(\Vdash_\alpha A \wedge B)^c$ is $(\Vdash_\alpha A)^c \wedge (\Vdash_\alpha B)^c$
3. $(\Vdash_\alpha A \vee B)^c$ is $(\Vdash_\alpha A)^c \vee (\Vdash_\alpha B)^c$
4. $(\Vdash_\alpha A \rightarrow B)^c$ is $\forall \beta \geq \alpha((\Vdash_\beta A)^c \rightarrow (\Vdash_\beta B)^c)$
5. $(\Vdash_\alpha \exists x A(x))^c$ is $\exists x(D(\alpha, x) \wedge (\Vdash_\alpha A(x))^c)$
6. $(\Vdash_\alpha \forall x A(x))^c$ is $\forall \beta \geq \alpha \forall x(D(\beta, x) \rightarrow (\Vdash_\beta A(x))^c)$

The following is straightforward:

$$\mathcal{M} \Vdash_\alpha A \text{ if, and only if, } \mathcal{M}^c \models (\Vdash_\alpha A)^c$$

Lemma. *For any countable Kripke model $\mathcal{M}$ of $PTCA^+$ there is a countable Kripke model $\mathcal{M}^\infty$ of $PTCA^+_\infty$ which forces exactly the same first-order sentences.*

Proof : Let $\mathcal{M}$ be a countable Kripke model of $PTCA^+$, and consider $\mathcal{M}^c$ its associated classical structure, as described above. Take $\mathcal{N}$ a (countable) recursively saturated structure elementarily equivalent to $\mathcal{M}^c$, and read-off from $\mathcal{N}$ the unique Kripke structure $\mathcal{M}^\infty$ associated with it. We must check that for any recursive enumeration $F_0(x), F_1(x), \ldots$ of first-order formulas of L_p with only a finite number of parameters,

$$\mathcal{M}^\infty \Vdash \forall x \bigvee_n F_n(x) \rightarrow \bigvee_n \forall x \bigvee_{k \leq n} F_k(x)$$

In order to show this, let α be an arbitrary node of $\mathcal{M}^\infty$ such that,

$$\mathcal{M}^\infty \Vdash_\alpha \forall x \bigvee_n F_n(x)$$

This means that,

$$\mathcal{N} \models \forall \beta \geq \alpha \forall x (D(\beta, x) \rightarrow \bigvee_n (\Vdash_\beta F_n(x))^c)$$

It is clear that the sequence of formulas $(\Vdash_\beta F_0(x))^c, (\Vdash_\beta F_1(x))^c, \ldots$ is still a recursive enumeration. Hence, due to the recursive saturation of $\mathcal{N}$, we may conclude that,

$$\mathcal{N} \models \bigvee_n \forall \beta \geq \alpha \forall x (D(\beta, x) \rightarrow \bigvee_{k \leq n} (\Vdash_\beta F_k(x))^c)$$

This shows that,

$$\mathcal{M}^\infty \Vdash_\alpha \bigvee_n \forall x \bigvee_{k \leq n} F_k(x)$$

□

The next ingredient that we need is the operation ( ) → $(\Sigma)'$ described by Smorynski in [12]. We briefly sketch this (two-stage) operation. The first stage consists in defining the disjoint sum $\sum_{i \in I} \mathcal{M}_i$ of a family $(\mathcal{M}_i)_{i \in I}$ of Kripke structures. This disjoint sum is the natural Kripke structure obtained from the family $(\mathcal{M}_i)_{i \in I}$ whose underlying partial ordering is the disjoint sum of the partial orderings of the members of the family (note that if the family has more than one member, its disjoint union does not have a least element). It is a simple fact that if $(\mathcal{M}_i)_{i \in I}$ is a family of models of $PTCA^+$, then so is its disjoint sum. The second stage of the operation is a *slash* construction. Given $\mathcal{M}$ a Kripke model (not necessarily with a least element) of $PTCA^+$, $\mathcal{M}'$ is obtained from $\mathcal{M}$ by adding a new node below all the nodes of $\mathcal{M}$, and by putting there the standard model $\{0, 1\}^*$. This construction is well defined, since atomic formulas are decidable in $PTCA^+$ (see the last result of the appendix). The following lemma can be proved like theorem 5.2.4 of [12]:

Lemma. *Let $(\mathcal{M}_i)_{i \in I}$ be a family of Kripke models of $PTCA^+$. Then $(\sum_{i \in I} \mathcal{M}_i)'$ is a model of $PTCA^+$.*

We are now ready to prove the conservativity result of the previous section.

Proof (of conservativity result): Let $A_0, A_1, \ldots$ be a sequence of (first-order) sentences of L_P, and suppose that $PTCA^+_\infty \Vdash \vee_n A_n$. In order to get a contradiction, assume that there is no $m \in \omega$ such that $PTCA^+ \vdash_i A_m$. By the completeness theorem of intuitionistic logic, for each $m \in \omega$, there is a Kripke model $\mathcal{M}_m$ of $PTCA^+$ which does not force A_m. Let $\mathcal{M}$ be $(\sum_n \mathcal{M}_n)'$. According to the previous lemma, this is a model of $PTCA^+$ and it is a simple exercise to show that, for any $m \in \omega$, $\mathcal{M} \nVdash A_m$. Now, by the first lemma above, let $\mathcal{M}^\infty$ be a Kripke model of $PTCA^+_\infty$ which forces the same first-order sentences as $\mathcal{M}$. Thus, in particular, for every $m \in \omega$, $\mathcal{M}^\infty \nVdash A_m$. This contradicts the fact that $\mathcal{M}^\infty$ forces $\vee_n A_n$. □

4 Two more applications

The method of section 2 generalizes naturally to the other levels of Buss's hierarchy of theories, thus providing alternative proofs of the results of Victor Harnik in [9]. Let us describe these results in our stringlanguage notation. Given $j \geq 2$, Σ^b_j-NIA is the stringlanguage analogue of the theory

S^j_2 of Buss, and $\exists^{\leq}\Delta^b_j$-NIA is the analogue of (what may be called) $S^j_2(PV_j)$ (see [10]). The theory $\exists^{\leq}\Delta^b_j$-NIA and its language are fully described in [7]. We briefly discuss them here. In order to introduce the language L_j ($j \geq 2$), it is better to start with L_1. This is just the language L_P of section 2. The language L_j is obtained from L_{j-1} by adding a new function symbol $K_{\exists^{\leq}A}(\overline{x}, y)$ for each open formula $A(\overline{x}, z)$ of L_{j-1} – with the intended meaning of being the characteristic function of the set defined by the predicate $\exists z \leq y\, A(\overline{x}, z)$ – and, then, by permitting the construction of new function symbols by means of composition and bounded iteration on notation (thus obtaining a function symbol for each function in $\square^p_j$). The theory $\exists^{\leq}\Delta^b_1$-NIA is just $PTCA^+$. The theory $\exists^{\leq}\Delta^b_j$-NIA is obtained from $\exists^{\leq}\Delta^b_{j-1}$-NIA by adding the following three classes of axioms:

(1) If $A(\overline{x}, z)$ is an open formula of L_{j-1}, then

$$K_{\exists^{\leq}A}(\overline{x}, y) = 0 \vee K_{\exists^{\leq}A}(\overline{x}, y) = 1$$
$$K_{\exists^{\leq}A}(\overline{x}, y) = 1 \rightarrow \exists z \leq y\, A(\overline{x}, z)$$
$$K_{\exists^{\leq}A}(\overline{x}, y) = 0 \rightarrow \forall z \leq y\, \neg A(\overline{x}, z)$$

are axioms. (Note that the above slightly departs from the definition in [7], although both definitions are classically equivalent.)

(2) Open axioms describing simple definitional properties of the other new function symbols (other than the K's).

(3) The scheme of induction on notation for formulas of the form $\exists x \leq t\, A$, where t is a term in which the variable x does not occur and A is an open formula of the language L_j (note that these formulas define exactly the Σ^p_j-sets in the standard model).

In classical logic it is well-known that the theory $\exists^{\leq}\Delta^b_j$-NIA is a conservative extension of the theory Σ^b_j-NIA (see, for instance, [10]). However, as Harnik remarked, this requires application of excluded middle for Σ^b_{j-1}-formulas and for Π^b_{j-1}-formulas (this is on a par with the case $j = 1$, notwithstanding the fact that in the base case the required instances of excluded middle come automatically). Let Ω_j be the set of all formulas of the form $\phi \vee \neg\phi$, where $\phi \in \Sigma^b_{j-1} \cup \Pi^b_{j-1}$. By the previous discussion, the intuitionistic theory $\exists^{\leq}\Delta^b_j$-NIA is conservative over intuitionistic Σ^b_j-NIA. Harnik's result can be reformulated thus:

Theorem (Harnik [9]). *Let $j \geq 2$. Suppose that the theory $\Sigma^b_j - NIA + \Omega_j \vdash_i \forall\overline{x}\exists y A(\overline{x}, y)$, where A is an arbitrary formula of the language of L whose free variables are among $\overline{x}$ and y. Then there is a $\square^p_j$-function f such that,*

$$\exists^{\leq}\Delta^b_j - NIA \vdash_i \forall\overline{x}\, A(\overline{x}, f(\overline{x}))$$

Proof (sketch): Given $A(w)$ a Σ^b_{j-1}-formula, we introduce the notions $\{z\}^A_n(\overline{x}) \downarrow$ and $\{z\}^A_n(\overline{x})$, which can be "smoothly" formalized within intuitionistic $\exists^{\leq}\Delta^b_j$-NIA by an open formula of L_j, respectively, a function symbol of L_j. These are familiar notions: $\{z\}^A_n(\overline{x})$ is the output of the Turing calculation with Gödel number z and oracle $A(w)$ for the input $\overline{x}$, *provided* that this calculation is done in less than $(\ell_1 + \ell_2 + 2)^n$ steps, where ℓ_1 and ℓ_2 are, respectively, the lengths of z and $\overline{x}$ (when the calculation exceeds this number of steps, i.e., when $\{z\}^A_n(\overline{x}) \downarrow$ does not hold, the default value ϵ is given). Let $K_{j-1}(w)$ be a natural Σ^b_{j-1} complete set. We shall use the following result:

Result. *Given f a $\Box_j^p$-function, there is a term $e \in \{0,1\}^*$ and an element $m \in \omega$ such that the theory $\exists^{\leq}\Delta_j^b$-NIA proves the following intuitionistically,*

$$\forall \overline{x} \, (\{e\}_m^{K_{j-1}}(\overline{x}) \downarrow \wedge f(\overline{x}) = \{e\}_m^{K_{j-1}}(\overline{x}))$$

A proof of a reformulation of the above result appears in Pudlak's monograph [8] for the classical case. However, it is easy to see that Pudlak's arguments also go through in the intuitionistic case since they only use excluded middle for open formulas of L_j (and these are, of course, decidable).

Given $j \geq 2$, we will work with the concept of q-realizability obtained from that of section 2 by modifying the first clause to,

$z\mathbf{q}A$ is A, if A is an open formula of L_j

and by changing, throughout, $\{z\}_n(x) \downarrow$ and $\{z\}_n(x)$ for $\{z\}_n^{K_{j-1}}(x) \downarrow$ and $\{z\}_n^{K_{j-1}}(x)$, respectively. A straightforward reformulation of the soundness theorem holds (the proof uses suitable modifications of the six results mentioned in section 2; for instance, the above result is the modified version of result 1 that is now needed). The only novelty in the proof of the soundness theorem is the q-realizability of the axioms in (1) above. The first and last groups of these axioms pose no trouble (note that the q-realizability of $\forall z \leq y \, \neg A(\overline{x}, z)$ reduces to $\forall z \leq y \, \neg A(\overline{x}, z)$ itself). We only need to be concerned with the q-realizability of the statements,

$$K_{\exists^{\leq} A}(\overline{x}, y) = 1 \rightarrow \exists z \leq y \, A(\overline{x}, z)$$

where $A(\overline{x}, z)$ is an open formula of L_{j-1}. This easily follows from the fact that there is a function symbol w_A of L_j such that the theory $\exists^{\leq}\Delta_j^b$-NIA proves intuitionistically,

$$\forall \overline{x} \forall y \, (\exists z \leq y \, A(\overline{x}, z) \; \rightarrow \; w_A(\overline{x}, y) \leq y \wedge A(\overline{x}, w_A(\overline{x}, y)))$$

This result was proved in [7] for the classical case, but the same proof also holds intuitionistically.

The result of Harnik now follows from the soundness theorem and a suitable conservativity result. There are no problems in proving such a conservativity result by the methods of section 3. □

Finally, we briefly describe the case of the theory $I\Sigma_1$, the fragment of PA whose induction scheme is restricted to (strict) Σ_1-formulas. It is well-known that the primitive recursive functions can be smoothly introduced in $I\Sigma_1$, even intuitionistically. If we extend the language of arithmetic L in order to contain function symbols for each (description of a) primitive recursive function, we thus obtain the theory PRA^+. In short, this theory is formulated in the extended language L_P of primitive recursive arithmetic and its non-logical axioms are the defining equations for all primitive recursive functions plus the axiom scheme of induction restricted to Σ_1-formulas. Recently, Kai Wehmeier proved the following theorem:

Theorem (Wehmeier [15]). *Suppose that $I\Sigma_1 \vdash_i \forall \overline{x} \exists y A(\overline{x}, y)$, where A is an arbitrary formula of the language of L whose free variables are among $\overline{x}$ and y. Then there is a primitive recursive function f such that,*

$$PRA^+ \vdash_i \forall \overline{x} \, A(\overline{x}, f(\overline{x}))$$

The method of proof of section 2 yields this result if we suitably modify the notions of $\{x\}_n(\overline{y})$ and $\{x\}_n(\overline{y}) \downarrow$. For each n, let E_n be the n^{th} Grzegorczyk function (we are following the notation of [11]). We define $\{x\}_n(\overline{y})$ as the output of the Turing machine calculation with Gödel number x for the input $\overline{y}$, *provided* that this calculation is done in less than $E_n(max(x, \overline{y}))$ steps (when the calculation exceeds this number of steps, i.e., when $\{x\}_n(\overline{y}) \downarrow$ does not hold, the default value 0 is given). These two notions can be formalized within intuitionistic PRA^+ *via* an open formula, respectively, a function symbol of the extended language L_P. With these definitions, we have available suitable modifications of results 1 and 5 of section 2 (the other results are immediate). These modified results are, respectively,

Result. *Given f a primitive recursive function, there is a term $e \in \omega$ and an element $m \in \omega$ such that the theory PRA^+ proves the following intuitionistically,*

$$\forall \overline{x} \left(\{e\}_m(\overline{x}) \downarrow \wedge f(\overline{x}) = \{e\}_m(\overline{x}) \right)$$

Result. *Given $m \in \omega$, there is a binary primitive recursive function $R = R_m$ with the following property: for every $n, s \in \omega$ there is $p \in \omega$ such that the theory PRA^+ proves the following intuitionistically,*

$$\{v\}_n(\overline{z}) \downarrow \rightarrow \{R(v,w)\}_p(\overline{z},0) \downarrow \wedge \{R(v,w)\}_p(\overline{z},0) = \{v\}_n(\overline{z})$$

and

$$\{R(v,w)\}_p(\overline{z},x) \downarrow \wedge \{w\}_s(\overline{z},x,\{R(v,w)\}_p(\overline{z},x)) \downarrow \rightarrow$$
$$\rightarrow \{R(v,w)\}_p(\overline{z},x+1) \downarrow \wedge \{R(v,w)\}_p(\overline{z},x+1) = \{w\}_s(\overline{z},x,\{R(v,w)\}_p(\overline{z},x))$$

where $\overline{z}$ is a m-tuple of variables.

With the above, the proof proceeds like in section 2.

5 Acknowledgements

The first author would like to thank José Luís Fiadeiro for a pertinent remark and Dick de Jongh for the encouragement.

References

[1] Samuel Buss. *Bounded Arithmetic.* PhD thesis, Princeton University, June 1985. A revision of this thesis was published by Bibliopolis in 1986.

[2] Samuel Buss. The polynomial hierarchy and intuitionistic bounded arithmetic. In Alan L. Selman, editor, *Structure in Complexity Theory*, pages 77–103. Springer-Verlag Lecture Notes in Computer Science No. 223, 1986.

[3] Stephen Cook and Alasdair Urquhart. Functional interpretations of feasibly constructive arithmetic. *Annals of Pure and Applied Logic*, 63:103–200, 1993.

[4] Michael Dummett. *Elements of Intuitionism*, volume 2 of *Oxford Logic Guides.* Oxford University Press, 1977.

[5] Fernando Ferreira. *Polynomial Time Computable Arithmetic and Conservative Extensions.* PhD thesis, Pennsylvania State University, December 1988.

[6] Fernando Ferreira. Polynomial time computable arithmetic. In Wilfried Sieg, editor, *Logic and Computation*, pages 161–180. American Mathematical Society, 1990.

[7] Fernando Ferreira. Stockmeyer induction. In Samuel Buss and Philip Scott, editors, *Feasible Mathematics*, pages 161–180. Birkhäuser, 1990.

[8] Petr Hájek and Pavel Pudlák. *Metamathematics of First-Order Arithmetic*, chapter V, Bounded Arithmetic. Springer-Verlag, 1993.

[9] Victor Harnik. Provably total functions of intuitionistic bounded arithmetic. *The Journal of Symbolic Logic*, 57(2):466–477, 1992.

[10] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, 1995.

[11] H. E. Rose. *Subrecursion. Functions and hierarchies*, volume 9 of *Oxford Logic Guides.* Oxford University Press, 1984.

[12] Craig Smoryński. Applications of Kripke models. In A. S. Troelstra, editor, *Metamathematical Investigations of Intuitionistic Arithmetic and Analysis*, chapter V, pages 324–391. Springer-Verlag, 1973.

[13] D. van Dalen. Intuitionistic logic. In D. Gabbay et F. Guenthner, editor, *Handbook of Philosophical Logic*, chapter III.4, pages 225–339. D. Reidel Publishing Company, 1986.

[14] D. van Dalen and A. S. Troelstra. *Constructive Mathematics. An Introduction*, volume 1. North-Holland, 1988.

[15] Kai Wehmeier. Fragments of HA based on Σ_1-induction. Preprint, Institut für mathematische Logick und Grundlagenforschung, Westfälische Wilhelms-Universität Münster, 1996.

Appendix

A formula ϕ is *decidable* in the theory Γ if the formula $\phi \vee \neg\phi$ is intuitionistically derivable from Γ. The aim of this appendix is to show that the swq-formulas are decidable in the theory $\Sigma_1^b - NIA$. The following proof actually shows that the swq-formulas are decidable in the theory consisting of the fourteen basic open axioms together with the notation induction scheme for swq-formulas.

Proposition 1. *The formula $x = \epsilon$ is decidable.*

Proof : By notation induction on x applied to the formula $x = \epsilon \vee x \neq \epsilon$, using axioms 13 and 14. □

Lemma 2. *The following are intuitionistically derivable in $\Sigma_1^b - NIA$:*

(2.1) $(xy)z = x(yz)$

(2.2) $\epsilon x = x$

(2.3) $\epsilon \neq 0 \wedge \epsilon \neq 1$

(2.4) $x \subseteq x$

(2.5) $x \subseteq x0 \wedge x \subseteq x1$

(2.6) $x \subseteq xz$

(2.7) $x \neq \epsilon \rightarrow 0 \subseteq x \vee 1 \subseteq x$

(2.8) $x \subseteq y \rightarrow x = y \vee x0 \subseteq y \vee x1 \subseteq y$

(2.9) $x \subseteq y \wedge y \subseteq z \rightarrow x \subseteq z$

(2.10) $x \subseteq z \wedge y \subseteq z \rightarrow x \subseteq y \vee y \subseteq x$

(2.11) $x \neq \epsilon \rightarrow \exists z(z0 = x \vee z1 = x)$

(2.12) $xy = \epsilon \rightarrow x = \epsilon \wedge y = \epsilon$

(2.13) $x \subseteq y \rightarrow \exists z(xz = y)$

Proof : (2.1) is proved by notation induction on z using axioms 1, 2 and 3. (2.2) is proved by notation induction on x using axiom 1 and (2.1). (2.3) is a consequnce of axioms 13 and 14 and of (2.2). (2.4) is proved by induction on x using axioms 9, 10 and 11. (2.5) is an immediate consequence of (2.4) and axioms 10 and 11. Similarly, (2.7), (2.8), (2.9) and (2.10) are proven by notation induction on x, y, z and z, respectively. (2.11) is proven by notation induction on x applied to the swq-formula $x \neq \epsilon \rightarrow \exists z \subseteq x(z0 = x \vee z1 = x)$. To show (2.12) we firstly note that the implication $y \neq \epsilon \to xy \neq \epsilon$ is an immediate consequence of (2.11) plus axioms 13 and 14. Since "being equal to ϵ" is decidable, the assertion $xy = \epsilon$ entails $y = \epsilon$ and, henceforth, $x = \epsilon$ as well. Finallly, (2.13) is proven by notation induction on y applied to the swq-formula $x \subseteq y \to \exists z \subseteq^* y\,(xz = y)$. □

Lemma 3. *The following are intuitionistically derivable in $\Sigma_1^b - NIA$:*

(3.1) $1 \times zx = (1 \times z)(1 \times x)$
(3.2) $(1 \times x)1 = 1(1 \times x)$
(3.3) $(1 \times x)(1 \times y) = (1 \times x)(1 \times z) \to 1 \times y = 1 \times z$
(3.4) $1 \times x = \epsilon \to x = \epsilon$
(3.5) $x \subseteq y \wedge 1 \times x = 1 \times y \to x = y$
(3.6) $xy = x \to y = \epsilon$
(3.7) $x \subseteq y \wedge y \subseteq x \to x = y$

Proof : (3.1) and (3.2) are straightforward by notation induction. (3.3) is also proved by notation induction on x. The base case $x = \epsilon$ is immediate by (2.2), since $1 \times \epsilon = \epsilon$ by axiom 5. Assume that $(1 \times x0)(1 \times y) = (1 \times x0)(1 \times z)$. Then, by axiom 6, $(1 \times x)1(1 \times y) = (1 \times x)1(1 \times z)$. Hence, by (3.2), $(1 \times x)(1 \times y)1 = (1 \times x)(1 \times z)1$. Thus, by axiom 8, we may conclude that $(1 \times x)(1 \times y) = (1 \times x)(1 \times z)$. By induction hypothesis we get $1 \times y = 1 \times z$. The case $x1$ is similar.

Since "being equal to ϵ" is decidable, (3.4) is equivalent to $x \neq \epsilon \to 1 \times x \neq \epsilon$. Suppose $x \neq \epsilon$. By (2.11) there is z such that $x = z0$ (the case $x = z1$ is similar). Hence, $1 \times x = 1 \times z0 = (1 \times z)1$, and this last term is not equal to ϵ by axiom 14. In order to show (3.5), assume that $x \subseteq y$ and $1 \times x = 1 \times y$. By (2.13), take z such that $y = xz$. By (3.1) we get $1 \times y = (1 \times x)(1 \times z)$. By (3.3) this entails $1 \times z = \epsilon$. We may conclude that $z = \epsilon$ by (3.4). (3.5) is also easy: if $xy = x$ then $1 \times xy = 1 \times x$ and so, by (3.1), we get $(1 \times x)(1 \times y) = 1 \times x$. This entails $1 \times y = \epsilon$, and so – by (3.4) – $y = \epsilon$.

Finally, assume that $x \subseteq y$ and $y \subseteq x$. By (2.13) take z and w such that $y = xz$ and $x = yw$. We get $y = ywz$ and so, by (3.6), $wz = \epsilon$. Hence, by (2.12), $w = z = \epsilon$, i.e., $x = y$.

□

Definition. *$x \perp y$ abbreviates the following formula:*

$$\exists z((z0 \subseteq x \wedge z1 \subseteq y) \vee (z1 \subseteq x \wedge z0 \subseteq y))$$

Lemma 4. *The following are intuitionistically derivable in $\Sigma_1^b - NIA$:*

(4.1) $x \perp y \vee x \subseteq y \vee y \subseteq x$
(4.2) $x \perp y \to x \nsubseteq y$

Proof : The proof of (4.1) is by notation induction on y (this is permissible since the formula $x \perp y$ is readily equivalent to a swq-formula). The base case $x = \epsilon$ makes the second disjunct true. Assume, by induction hypothesis, that $x \perp y$ or $x \subseteq y$ or $y \subseteq x$ (in order to conclude a similar disjunct for $y0$ – the case for $y1$ is similar). If either the first or the second of theses disjuncts is true, the same applies to the disjunct $x \perp y0 \vee x \subseteq y0$. Otherwise, $y \subseteq x$. In this case, by (2.8), either $y0 \subseteq x$ or $y1 \subseteq x$ or $y = x$. We respectively conclude either $y0 \subseteq x$ or $x \perp y0$ or $x \subseteq y0$.

To show (4.2), assume that $x \perp y$ and $x \subseteq y$. Take, without loss of generality, an element z such that $z0 \subseteq x$ (thus, $z0 \subseteq y$) and $z1 \subseteq y$. By (2.10) either $z0 \subseteq z1$ or $z1 \subseteq z0$. In either case we get a contradiction by (3.5) and axiom 12. □

Proposition 5. *The formulas $x \subseteq y$ and $x = y$ are decidable.*

Proof : Take x and y. By (4.1), either $x \perp y$ or $x \subseteq y$ or $y \subseteq x$. We saw in the last lemma that the first disjunct implies $x \nsubseteq y$. Hence, we need only consider the case $y \subseteq x$. By (2.8), either $y0 \subseteq x$ or $y1 \subseteq x$ or $y = x$. The last case poses no trouble. Anyone one of the first two cases in conjunction with $x \subseteq y$ gives rise to a contradiction (i.e., in these cases $x \nsubseteq y$ holds intuitionistically). Let us see, for instance, that $y0 \subseteq x$ and $x \subseteq y$ gives rise to a contradiction. By (2.9) these two statements imply $y0 \subseteq y$. Hence, $y = y0z$, for some z. By (3.6) this implies that $0z = \epsilon$, which in turn implies $0 = \epsilon$, a contradiction with (2.3).

By (2.4) and (3.7), $x = y$ is equivalent to $x \subseteq y \wedge y \subseteq x$. Hence, $x = y$ is equivalent to a Boolean combination of decidable formulas, and hence it is decidable. □

Proposition 6. *Let $A(x)$ be a decidable swq-formula in which the variable y does not occur. Then the formulas $\exists x \subseteq y\, A(x)$ and $\forall x \subseteq y\, A(x)$ are decidable. As a consequence, the statement $x \subseteq^* y$ is decidable.*

Proof : We show by notation induction on y that the swq-formula

$$(\star) \qquad \exists x \subseteq y\, A(x) \vee \neg \exists x \subseteq y\, A(x)$$

is intuitionistically derivable from the theory $\Sigma_1^b - NIA$. The base case $y = \epsilon$ reduces to the decidability of $A(\epsilon)$. Now, assume by induction hypothesis that $(\star)$ holds. Well, the formula $\exists x \subseteq y0\, A(x)$ is equivalent to $A(y0) \vee \exists x \subseteq y\, A(x)$. This last statement is a Boolean combination of decidable statements and, hence, is decidable. Similarly for $y1$ instead of $y0$. The universal case is analogous.

By the above, the formula $F(x, y, z) := \exists w \subseteq y\, (wx \subseteq z)$ is decidable. In particular, $x \subseteq^* y$ – which is $F(x, y, y)$ – is decidable.

□

Lemma 7. *The following are intuitionistically derivable in $\Sigma_1^b - NIA$:*

(7.1) $x0 \subseteq xy \rightarrow 0 \subseteq y$
(7.2) $x1 \subseteq xy \rightarrow 1 \subseteq y$
(7.3) $xy \subseteq xw \rightarrow y \subseteq w$
(7.4) $xy = xw \rightarrow y = w$

Proof : In order to prove (7.1), assume that $x0 \subseteq xy$. Then there is z such that $x0z = xy$ and, henceforth, $1 \times x0z = 1 \times xy$. Since $1 \times 0z = (1 \times 0)(1 \times z) = 1(1 \times z)$, we may conclude by (3.19, (3,3) and (2.6) that $1 \subseteq 1 \times y$ and, *fortiori*, that $y \neq \epsilon$. By (2.7) either $0 \subseteq y$ or $1 \subseteq y$. We show that the latter alternative does not hold. In fact, if this alternative were the case, $y = 1w$ for some w. Hence $x0 \subseteq x1w$. This implies, by (2.10) and (3.5) that $x0 = x1$, which contradicts axiom 12. The proof of (7.2) is similar. (7.3) is proved by notation induction on y. The base case $y = \epsilon$ is trivial. Suppose that $xy0 \subseteq xw$. Then $xy \subseteq xw$ and, by induction hypothesis, $y \subseteq w$. So, $w = yu$, for a certain u. We get $xy0 \subseteq xyu$ and, according to (7.1), $0 \subseteq u$, i.e., $u = 0v$ for some v. Hence $w = y0v$, getting $y0 \subseteq w$. Tha case for $y1$ is similar. Finally, (7.4) is a consequence of (7.3) and (3.7). □

Proposition 9. *Let $A(x)$ be a decidable swq-formula in which the variable y does not occur. Then the formulas $\exists x \subseteq^* y\, A(x)$ and $\forall x \subseteq^* y\, A(x)$ are decidable.*

Proof : Notice that the formula $\exists x \subseteq^* y\, A(x)$ is equivalent to:

$$\exists z \subseteq y \exists w \subseteq^* y\, (zw = y \wedge \exists x \subseteq w\, A(x))$$

Hence, by proposition 6 it is enough to show that the formula,

$$\exists w \subseteq^* y\, (zw = y \wedge \exists x \subseteq w\, A(x))$$

is decidable. This is a consequence of propositions 5 and 6 and lemma (7.4).

The case of the universal quantifier is similar. □

The latter proposition together with proposition 5 and the fact that Boolean combinations of decidable formulas are decidable yield,

Theorem. *Every swq-formula is decidable in $\Sigma_1^b - NIA$.*

From proposition 5, it is also clear that,

Theorem. *Every open formula of L_P is decidable in $PTCA^+$.*