Some notes on subword quantification and induction thereof

Fernando Ferreira*

Departamento de Matemática, Universidade de Lisboa, Rua Ernesto de Vasconcelos, bloco C1, P-1700 Lisboa, Portugal (ferferr@lmc.fc.ul.pt)

Abstract

The first section of this paper consists of a defense of the binary string notation for the formulation of weak theories of arithmetic which have computational significance. We defend that a stringlanguage is the most natural framework and that the usual arithmetic setting suffers from some troubles when dealing with very low complexity classes. Having introduced in the first section the theory $Th - FO$ - associated with a rather robust uniform version of the class of problems that can be decided by constant depth, polynomial size circuit families (the so-called AC^0-class) - we prove in the second section that the deletion of a crucial axiom from $Th - FO$ results in a theory which is unsuitable from the computational point of view.

Keywords: bounded arithmetic; computational complexity; AC^0; provably total functions.

1 The apology of a notation

In his Ph.D. Dissertation [1], Samuel Buss studies systems of arithmetic related to conspicuos classes of computational complexity. The main results of Buss show that the provability of certain sentences of the type "$\forall x \exists y A(x, y)$" in suitable sub-theories of Peano Arithmetic imply the existence of a function f such that $A(n, f(n))$, for all $n \in \omega$, and such that f has a certain computational complexity. Buss is interested in computational complexity classes consisting only of *feasible computable* functions and this requirement excludes, *a fortiori*, the exponential function. On the proof-theoretic side, this requirement compels the theories of arithmetic to be *weak theories*, i.e., theories that do not prove the totality of the exponential function.

A good first example is the theory $I\Delta_0 + \Omega_1$. This theory consists of $I\Delta_0$, the main feature of which is the restriction of the induction scheme to bounded formula of the language of $I\Delta_0$, plus a Π^0_2-axiom (the Ω_1-principle) saying that the function $\lambda x.x^{\lfloor log x \rfloor}$ is total ($\lfloor w \rfloor$ represents the greatest integer less than or equal to w). The language of the theory $I\Delta_0 + \Omega_1$ is the usual language of arithmetic: a constant 0, a unary function symbol S, two binary function symbols $+$ and $\cdot$ and a binary relation symbol $\leq$. This language presents some technical difficulties for the study of the provable total functions of $I\Delta_0 + \Omega_1$. A first reason is that $I\Delta_0 + \Omega_1$ does not have a Π^0_1-axiomatization. Hence it is not suitable for the formulation of a Parikh type theorem (we recommend chapter V of [2] as a reference for this section).

Buss gave a reformulation of the theory $I\Delta_0 + \Omega_1$. His reformulation adds to the usual language of arithmetic two unary function symbols $\lfloor \frac{1}{2}x \rfloor$, $|x|$ (for $\lceil log_2(x + 1) \rceil$, the length of the binary representation of x) and a binary function symbol $x\#y$ (for $2^{|x| \cdot |y|}$, the "smash" function)[1]. In this language Buss presents a Π^0_1-axiomatization consisting of thirty two basic open axioms, plus the usual scheme of induction for bounded formulae, resulting in the so-called theory T_2 (the

*This work was partially supported by project 6E91 of CMAF (Portugal)

induction scheme, whose instances are "$A(0) \wedge \forall x(A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)$", where A is a bounded formula, does not consist of Π_1^0-sentences but can be easily reformulated as such by "$\forall x(A(0) \wedge \neg A(x) \rightarrow \exists y \leq x(A(y) \wedge \neg A(y+1)))$"). Parikh's theorem applies:

Theorem. *If $T_2 \vdash \forall x \exists y A(x,y)$, where A is a bounded formula, then there is a term $t(x)$ of the language of T_2 such that $T_2 \vdash \forall x \exists y \leq t(x) A(x,y)$.*

From the truth of "$\forall x \exists y \leq t(x) A(x,y)$" alone, one easily concludes that the witness function $f(n) = \mu m A(n,m)$ is computable in polynomial space - indeed, even computable in polynomial time with an oracle in PH (the polynomial time hierarchy). More specifically, if the relation $A(x,y)$ is in Σ_n^p (and this is always the case for a certain n) then f is in $\Box_{n+1}^p$. This analysis takes little advantage of the provability of "$\forall x \exists y A(x,y)$" in T_2, relying solely upon the very general fact of Parikh. As we will see, Buss is able to provide a deeper analysis.

The class of *sharply bounded formulae* is the smallest class of formulae of the language of T_2 that contains the atomic formulae and that is closed under Boolean operations and *sharply bounded* quantifications (these are quantifications of the form $\forall x \leq |t|(...)$ or $\exists x \leq |t|(...)$, where t is a term in which the variable x does not occur). The Σ_n^b*-formulae*, $n \geq 1$, are the bounded formulae of the language of T_2 with the following form:

$$(BD) \qquad \exists x_1 \leq t_1 \forall x_2 \leq t_2 \exists x_3 \leq t_3 \ldots Q x_n \leq t_n \, A$$

where A is a sharply bounded formula, $t_1, \ldots, t_n$ are terms of the language and the quantifier Q is a $\forall$ or a $\exists$ depending on whether n is even or odd (respectively). The Σ_n^b-formulae define, in the standard model, the Σ_n^p-relations of PH. Hence, there is a matching between bounded formulae of the language of T_2 and the levels of the polynomial time hierarchy. Moreover, this is a *faithful* matching in the sense that the complexity of formula-construction goes hand-in-hand with the complexity levels of the polynomial hierarchy. In other words, a sub-formula of a Σ_n^b-formula can only define Σ_n^p-relations.[2]

Let Ψ be a set of formulae. The $\Psi - PIND$ axioms are:

$$(PIND) \qquad A(0) \wedge \forall x(A(\lfloor \frac{1}{2} x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x)$$

where $A \in \Psi$, possibly with parameters. The theory S_2^n $(n \geq 1)$ consists of the thirty two basic open axioms plus the $\Sigma_n^b - PIND$ axioms (it is well known that $T_2 = \cup_{n \in \omega} S_2^n$). Buss' main result of his thesis is the following:

Theorem. *If $S_2^n \vdash \forall x \exists y A(x,y)$, where A is a Σ_n^b-formula, then there is $f \in \Box_n^p$ such that $A(k, f(k))$, for all $k \in \omega$.*[3]

In the above, $f(k)$ is not necessarily the least m such that $A(k,m)$. The function f is constructed by means of a careful analysis of the proof of "$\forall x \exists y A(x,y)$" in S_2^n, and the importance of the faithfulness of the matching between Σ_n^b-formulae and Σ_n^p-relations cannot be over-emphasized in this respect. It is this faithfulness that permits a successful application of Gentzen's Hauptsatz (*vulgo* cut-elimination) to proving the above theorem. In short, Buss' notation for $I\Delta_0 + \Omega_1$ is not only superior to the usual notation on the account of providing Π_1^0-axiomatizations but, more important, on the account of giving faithful representations of the polynomial hierarchy.

Nonetheless, a critique can be made of Buss' notation. The most important is that it is not faithful with respect to certain complexity classes below the class P of polynomial time decidable predicates (we will discuss this later). It also parts from the notation of choice of most computer scientists working on feasibility.

In our Ph.D. Dissertation [3] (see, also, [4]) we work with a language based on the operation of concatenation, following Quine [5] and Smullyan [6]. Our intended (standard) model is the tree $\{0,1\}^*$ of binary strings. The first-order stringlanguage of the binary tree consists 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:

$$\begin{array}{rcl@{\qquad}rcl}
x \frown \epsilon = x & & & x \times \epsilon = \epsilon & & \\
x \frown (y \frown 0) = (x \frown y) \frown 0 & & & x \times (y \frown 0) = (x \times y) \frown x & & \\
x \frown (y \frown 1) = (x \frown y) \frown 1 & & & x \times (y \frown 1) = (x \times y) \frown x & & \\
x \frown 0 = y \frown 0 \rightarrow x = y & & & x \frown 1 = y \frown 1 \rightarrow x = y & & \\
x \subseteq \epsilon & \leftrightarrow & & x = \epsilon & & \\
x \subseteq y \frown 0 & \leftrightarrow & & x \subseteq y \vee x = y \frown 0 & & \\
x \subseteq y \frown 1 & \leftrightarrow & & x \subseteq y \vee x = y \frown 1 & & \\
x \frown 0 & \neq & & y \frown 1 & & \\
x \frown 0 & \neq & & \epsilon & & \\
x \frown 1 & \neq & & \epsilon & &
\end{array}$$

In the standard model, $x \times y$ is the word x concatenated with itself length of y times (the growth rate of $\times$ corresponds exactly to the growth rate of Buss' smash function $\#$). *Subwordness* of x with respect to y, denoted by $x \subseteq^* y$, is defined by $\exists z \subseteq y\, (z \frown x \subseteq y)$. The class of *sw.q.-formulae* ("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 $\forall x \subseteq^* t(...)$ or $\exists x \subseteq^* t(...)$, where t is a term in which the variable x does not occur. These formulae define in the standard model the so-called class FO of *first-order expressible* properties: this notion was introduced by Neil Immerman in [7] and was originally defined in terms of first-order definability in suitable finite structures with domain $\{0, 1, \cdots, n-1\}$. The FO-class is included in AC^0, the class of sets that can be decided by constant depth, polynomial size circuit families (one should view the class of FO-relations as a rather robust uniform version of AC^0). In the same paper, Immerman also discusses what we call FO-functions. In parallel with the set case, these functions can also be computed by constant depth, polynomial size circuit families (the so-called AC^0-functions). A more detailed rendering of these notions can be found in [8].

The relation of x being of length less than or equal to the length of y, denoted by $x \leq y$, is defined by $1 \times x \subseteq 1 \times y$;[4] $x \equiv y$ abbreviates $x \leq y \wedge y \leq x$. The class of *bounded formulae*, also named the class of Σ^b_∞-formulae, is the smallest class of formulae containing the sw.q.-formulae and closed under Boolean operations and bounded quantification, i.e., quantification of the form $\forall x \leq t(...)$ or $\exists x \leq t(...)$, where t is a term in which the variable x does not occur. In the standard model these formulae define exactly the sets of the polynomial hierarchy. Mimicking Buss' terminology, we define the Σ^b_n-formulae ($n \geq 1$) as the bounded formulae with the form (BD) above, where A is sw.q.-formula and $t_1, \ldots, t_n$ are terms of the new language. Not surprisingly, these Σ^b_n-formulae define exactly the Σ^p_n-relations.

The theory $\Sigma^b_n - NIA$ (for *Notation Induction Axioms*) consists of the basic axioms plus the induction scheme,

$$(NIA) \qquad A(\varepsilon) \wedge \forall x\, (A(x) \rightarrow A(x0) \wedge A(x1)) \rightarrow \forall x\, A(x)$$

where A is a Σ^b_n-formula, possibly with parameters. This theory is equivalent, in a sense that could be made precise, to Buss' theory S^n_2, and it is partly a matter of taste and habitude the preference for working within the string setting.

In the sequel, we will be interested in the theory $Th - FO$. The axioms of this theory consist of the fourteen basic open axioms, the scheme of induction on notation (NIA) for sw.q.-formulae, and a string-building principle:

$$(SB) \qquad \forall u(tally(u) \rightarrow \exists x \equiv u \forall v \subset u(bit(x,v) = 1 \leftrightarrow A(v)))$$

where "$v \subset u$" abbreviates "$v \subseteq u \wedge v \neq u$", "$bit(x,v) = 1$" abbreviates "$\exists w \subseteq x(w \equiv v \wedge w1 \subseteq x)$", and A is a sw.q.-formula (possibly with parameters). This is a rather weak theory, but still an interesting one[5]. The theory $Th - FO$ is not an arithmetical theory in the usual sense. However, it is possible to do some arithmetic in $Th - FO$. More specifically, it is possible to "smoothly" introduce the successor and the addition functions in $Th - FO$. We are using the term "smoothly" in the following sense: it is possible to expand the language of $Th - FO$ with new function symbols S and $+$ such that the usual recursive defining relations are provable and such that these new symbols count as primitive when making an analysis of whether a particular formula of the extended language falls within a pertinent class of formulae (e.g., whether a particular formulae is a sw.q.-formula). Let us briefly see how arithmetic notions can be introduced in the theory $Th - FO$.

The models of $Th - FO$ have a canonical linear ordering $<_\ell$, which is formally defined by a sw.q.-formula:

$$x <_\ell y := (x \leq y \wedge x \not\equiv y) \vee (x \equiv y \wedge \exists z \subseteq x(z0 \subseteq x \wedge z1 \subseteq y))$$

In the standard model this yields a ω-like ordering:

0	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
ϵ	0	1	00	01	10	11	000	001	010	011	100	$\cdots$

Having this correspondence in mind, we introduce arithmetic notions in models of $Th - FO$. The graph of the successor function is easily defined by the following sw.q.-formula θ_1:

$$\theta_1(x,y) := (x = 1 \times x \wedge y = 0 \times x1) \vee \exists w \subseteq x \exists z \subseteq x(x = w0 \frown (1 \times z) \wedge y = w1 \frown (0 \times z))$$

Moreover,

$$(I\theta_1) \qquad Th - FO \vdash \forall x \exists^1 y\, \theta_1(x,y)$$

$$(II\theta_1) \qquad Th - FO \vdash \theta_1(\epsilon, 0)$$

$$(III\theta_1) \qquad Th - FO \vdash \forall x \forall y(\theta_1(x0, x1) \wedge (\theta_1(x,y) \rightarrow \theta(x1, y0)))$$

The proofs of these three facts are elementary and can be obtained by means of judicious uses of the axioms. Some basic properties recur in these proofs (and in proofs of similar nature), e.g.: $\epsilon \subseteq x$; $x \subseteq x$; $x \subseteq y \rightarrow x \subseteq^* y$; $x \subseteq^* y \wedge y \subseteq^* z \rightarrow x \subseteq^* z$; $x \subseteq^* y \frown z \rightarrow \exists x_1 \subseteq^* y \exists x_2 \subseteq z\,(x = x_1 \frown x_2)$; and $x \subseteq^* y \times z \rightarrow \exists x_1 \subseteq^* y \exists x_2 \subseteq z \exists x_3 \subseteq y\,(x = x_1 \frown (y \times x_2) \frown x_3)$. Actually, all these properties are provable without the use of the string-building principle. (Proofs of the previous statements were worked out in detail in [3].) The properties $(I\theta_1)$, $(II\theta_1)$ and $(III\theta_1)$ permit to "smoothly" introduce in the theory $Th - FO$ a new unary function symbol S (for the *successor* function) satisfying the following recursive specifications: $S(\epsilon) = 0$; $S(x0) = x1$; and $S(x1) = S(x) \frown 0$. Almost dually, it is also possible to introduce the corresponding predecessor function: $pred(\epsilon) = pred(0) = \epsilon$; $pred(x0) = pred(x) \frown 1$, for $x \neq \epsilon$; and $pred(x1) = x0$.

The introduction of "addition" is not so straightforward. Perhaps the easiest way to introduce it consists in reducing this operation of addition to the usual addition in binary number notation. The configuration of a number in binary notation is a non-empty string of zeroes and ones which does not begin by a zero, with the sole exception of the string 0 itself. The relation β that is the graph of the order-preserving, no-gap, bijection between $\{0,1\}^*$ and the set of binary number configurations is sw.q.-definable. In fact:

$$\beta(x,y) \leftrightarrow (x = \epsilon \wedge y = 0) \vee (x \neq \epsilon \wedge y = 1 \frown pred(x))$$

Here is a picture:

$$\begin{array}{ccccccccccccc} \epsilon & 0 & 1 & 00 & 01 & 10 & 11 & 000 & 001 & 010 & 011 & 100 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 1 & 10 & 11 & 100 & 101 & 110 & 111 & 1000 & 1001 & 1010 & 1011 & \cdots \end{array}$$

It is not difficult to see that,

$$Th - FO \vdash \forall x \exists^1 y \, \beta(x,y)$$

$$Th - FO \vdash \forall y (bin(y) \rightarrow \exists^1 x \, \beta(x,y))$$

where $bin(y)$ abbreviates $y = 0 \vee \exists z \subseteq^* y(y = 1z)$. This permitts to "smoothly" introduce two unary function symbols β_f and β_b in the theory $Th - FO$ such that the sentences $\forall x(\beta(x, \beta_f(x))$, $\forall y(bin(y) \rightarrow \beta(\beta_b(y), y))$, $\forall x(x = \beta_b(\beta_f(x)))$, and $\forall y(bin(y) \rightarrow y = \beta_f(\beta_b(y)))$ are provable in $Th - FO$. The definition of binary addition can be obtained by a sw.q.-formula with the help of the ternary *carry* predicate (the following is a standard construction; see [9]):

$$carry(x,y,u) := tally(u) \wedge \exists v \subset u(bit(x,v) = 1 \wedge bit(y,v) = 1 \wedge$$

$$\wedge \forall w \subset u(v \subseteq w \rightarrow bit(x,w) = 1 \vee bit(y,w) = 1))$$

Now, if we let $sum(x,y,z)$ be

$$bin(x) \wedge bin(y) \wedge bin(z) \wedge (\forall u \subset 1 \times z(bit(z,u) = 1 \leftrightarrow (bit(x,u) = 1 \dot{\vee} bit(y,u) = 1 \dot{\vee} carry(x,y,u))))$$

where $\dot{\vee}$ stands for the exclusive *or*, we get the graph of binary addition. Define $\theta_2(x,y,z)$ by $\beta_b(sum(\beta_f(x), \beta_f(y), \beta_f(z)))$. It is a matter of careful attention to detail and habitude with the axioms to show that,

$(I\theta_2)$ $$Th - FO \vdash \forall x \forall y \exists^1 z \, \theta_2(x,y,z)$$

$(II\theta_2)$ $$Th - FO \vdash \forall x \theta_2(x, \epsilon, x)$$

$(III\theta_2)$ $$Th - FO \vdash \forall x \forall y \forall z(\theta_2(x,y,z) \rightarrow \theta_2(x, S(y), S(z)))$$

(The string-building principle is used to proving the existence part of $(I\theta_2)$.) The previous three properties permit to "smoothly" introduce in the theory $Th - FO$ a new binary function symbol $+$ such that $x + \epsilon = x$ and $x + S(y) = S(x + y)$.

The next natural step towards defining arithmetic notions in $Th - FO$ consists in introducing the multiplication function. Well, at this point we are faced with a stumbling block, since there is no Σ_1^b-formula θ_3 such that,

$(I\theta_3)$ $$Th - FO \vdash \forall x \forall y \exists^1 z \, \theta_3(x,y,z)$$

$(II\theta_3)$ $$Th - FO \vdash \forall x \theta_3(x, \epsilon, \epsilon)$$

$(III\theta_3)$ $$Th - FO \vdash \forall x \forall y \forall z(\theta_3(x, y, z) \rightarrow \theta_3(x, S(y), z + x))$$

The reason for the inexistence of such a formula rests on deep work in circuit complexity theory. If such a formula existed, then the unique binary function f such that $\theta_3(\sigma, \tau, f(\sigma, \tau))$, for all σ,τ in $\{0,1\}^*$, would be a FO-function (this is a consequence of a theorem in [8] which characterizes the provably total functions, with Σ_1^b-graphs, of the theory $Th - FO$). Hence, *a fortiori*, f is an AC^0-function, and this easily entails that the usual multiplication function on the setting of binary number configurations is also an AC^0-function. Well, this latter fact contradicts work of M. Furst, J. Saxe and M. Sipser and, independently, of M. Ajtai.[6]

The previous discussion explains why Buss' arithmetic language is inadequate for the formulation of the theory $Th - FO$, since the representation of sw.q.-relations in Buss' language uses the multiplication function pervasively. In short, Buss' notation is not faithful with respect to sw.q.-relations.[7] This is the main point of the present section.

Annotations

[1] The growth rate of the smash function entails that lengths of numbers are closed under multiplication. This enables the formulation of many standard constructions, in particular of polynomial time computations.

[2] The definiton of Σ_n^b-formula presented here is what Buss calls a *strict* Σ_n^b-formula. Buss defines Σ_n^b-formulae in a more general way. For this latter definition we have to modify slightly the concept of faithfulness: it means that every positive (*resp.*, negative) occurrence of a sub-formula of a Σ_n^b-formula is a Σ_n^p-relation (*resp.*, a Π_n^p-relation).

[3] Buss also remarked that the conclusion of the theorem is provable in S_2^n (pace a suitable formalization).

[4] This appropriation of the traditional symbol for the usual order of the natural numbers has, sometimes, been criticized. We maintain that it has virtualities from the point of view of computational complexity because the number of natural numbers less than or equal to n has the same order of growth as the number of elements of $\{0,1\}^*$ with length less than or equal to the length of a word σ of length $|n|$.

[5] A reason for its interest, apart from being closely related to the FO-class, is its bearing on $I\Delta_0$ (see [8] for an explanation of this). The theory $Th - FO$ was also independently defined by Zambella [10]. In his setting, it is called $\Sigma_0^p - comp$.

[6] In groundbreaking papers [11] and [12], these authors proved that "parity" is not an AC^0-predicate. ("Parity" is the set of elements of $\{0,1\}^*$ with an even number of 1's.) The fact that "parity" is AC^0-reducible to "multiplication" is explained in [13].

[7] Buss' class of sharply bounded formulae is, in certain aspects, a bizarre class: in effect, all the initial functions and relations of this class, as well as all its closure operations, are of AC^0-character, with the sole exception of the multiplication function. (For an in-depth study of sharply bounded predicates, consult [14].) A similar remark applies to the class SR of *strictly rudimentary* formulae, as introduced by Wilkie and Paris in [15].

2 The unsuitability of a theory

The theory S_2^0 consists of the thirty two basic open axioms of Buss plus the $PIND$ axioms for sharply bounded formulae. Gaisi Takeuti proved in [16] that the sentence "$\forall x \exists y(x = 0 \vee x = y+1)$" cannot be deduced in S_2^0. In our opinion, this result shows that the theory S_2^0 is uninteresting and artificial. Namely, it shows that S_2^0 is too sensible to the basic open axioms and to the exact language chosen. Let $sw.q. - NIA$ be the theory in the stringlanguage formed by the fourteen open axioms listed in the previous section and the scheme of induction on notation (NIA) for sw.q.-formulae (the reader should compare this theory with $Th - FO$). Is $sw.q. - NIA$ an interesting theory? Similarly, the answer is no. We show that the function $\lambda\sigma.\bar{\sigma}$, where the string $\bar{\sigma}$ is

obtained from σ by changing zeroes into ones and ones into zeroes, is not provably total in the theory $sw.q. - NIA$. More specifically, let "$y = \bar{x}$" abbreviate the sw.q.-formula,

$$y \equiv x \wedge \forall x' \subseteq x \exists y' \subseteq y \, (y' \equiv x' \wedge (x'0 \subseteq x \rightarrow y'1 \subseteq y) \wedge (x'1 \subseteq x \rightarrow y'0 \subseteq y))$$

We prove the following result:

Theorem. *The theory $sw.q. - NIA$ does not prove $\forall x \exists y$"$y = \bar{x}$".*

We need to prepare the ground for the proof of this theorem. In what follows we will use at ease the provability of some simple facts in the theory $sw.q. - NIA$, e.g., those listed in the previous section during the discussion of the properties $(I\theta_1)$, $(II\theta_1)$ and $(III\theta_1)$.

Proposition 1. *Let $A(x)$ be a sw.q.-formula, possibly with parameters. Then the theory $sw.q. - NIA$ proves the following sentence,*

$$A(\epsilon) \wedge \neg A(y) \rightarrow \exists x \subseteq y \, (A(x) \wedge ((x0 \subseteq y \wedge \neg A(x0)) \vee (x1 \subseteq y \wedge \neg A(x1)))).$$

Proof : Consider the formula $B(x) := x \subseteq y \rightarrow A(x)$ and assume that $A(\epsilon)$ and $\neg A(y)$. Then $B(\epsilon)$ and $\neg B(y)$. By the scheme (NIA) for sw.q.-formulae we may conclude that there is x such that either $B(x) \wedge \neg B(x0)$ or $B(x) \wedge \neg B(x1)$. Such an x does the job. □

Given two structures M and N for the stringlanguage, we say that N is a *weak end-extension* of M, and write $M \subseteq_w N$, if M is a substructure of N and the following implication holds: $a \in M$, $b \in N$, $b \subseteq^* a \Rightarrow b \in M$.

Proposition 2. *Let $M \subseteq_w N$. Then the sw.q.-formulae are absolute between M and N, i.e., given any sw.q.-formula $A(\vec{x})$, with the free variables as shown, and given $\vec{a}$ in M, we have the equivalence $M \models A(\vec{a}) \Leftrightarrow N \models A(\vec{a})$.*

Proof : The proof is by a straightforward induction on the complexity of the formulae A. □

Corollary. *Let $M \subseteq_w N$, with N a model of $sw.q. - NIA$. Then M is also a model of $sw.q. - NIA$.*

Proof : It is clear that M satisfies the basic axioms, since these are open axioms. The validity of the induction scheme (NIA) for sw.q.-formulae is a consequence of the reformulation of this scheme given in proposition 1, and of the absoluteness of sw.q.-formulae. □

Let k be a positive integer. We define by induction on n ($n \in \omega$) the following $(k+1)$-predicates:

$$cl_0(y, x_1, \ldots, x_k) := y = 0 \vee y = 1 \vee y \subseteq^* x_1 \vee \ldots \vee y \subseteq^* x_k$$

$$cl_{n+1}(y, x_1, \ldots, x_k) := \exists z \exists w (cl_n(z, x_1, \ldots, x_k) \wedge cl_n(w, x_1, \ldots, x_k) \wedge (y = z \frown w \vee y = z \times w)).$$

Lemma.

1. *For all $n \in \omega$, $sw.q. - NIA \vdash \forall \vec{x} \, cl_n(\epsilon, \vec{x})$.*
2. *If $n, m \in \omega$ and $n \leq m$ then $sw.q. - NIA \vdash \forall \vec{x} \forall y (cl_n(y, \vec{x}) \rightarrow cl_m(y, \vec{x}))$.*
3. *For all $n \in \omega$, $sw.q. - NIA \vdash \forall \vec{x} \forall y \forall z (cl_n(z, \vec{x}) \wedge y \subseteq^* z \rightarrow cl_{3n}(y, \vec{x}))$.*

Proof : The first part is clear. For the second part, it is enough to show that $sw.q. - NIA \vdash \forall\vec{x}\forall y(cl_n(y,\vec{x}) \to cl_{n+1}(y,\vec{x}))$. This follows immediately from part 1.

The third part is proved by induction on n. The base case is clear. Assume the conclusion for n. We reason inside $sw.q. - NIA$. Fix $\vec{x}$, y and z and suppose that $cl_{n+1}(z,\vec{x})$ and $y \subseteq^* z$. Then there are elements z_1 and z_2 such that $cl_n(z_1,\vec{x})$, $cl_n(z_2,\vec{x})$ and either $z = z_1 \frown z_2$ or $z = z_1 \times z_2$. Firstly, let us consider the case when $z = z_1 \frown z_2$. Take y_1 and y_2 with $y_1 \subseteq^* z_1$, $y_2 \subseteq z_2$, and $y = y_1 \frown y_2$. By induction hypotheses, we have $cl_{3n}(y_1,\vec{x})$ and $cl_{3n}(y_2,\vec{x})$. Hence $cl_{3n+1}(y_1 \frown y_2,\vec{x})$. With more reason (see part 2), we have $cl_{3n+3}(y,\vec{x})$. Lastly, consider the case when $z = z_1 \times z_2$. Take y_1, y_2 and y_3 such that $y_1 \subseteq^* z_1$, $y_2 \subseteq z_2$, $y_3 \subseteq z_1$, and $y = y_1 \frown (z_1 \times y_2) \frown y_3$. By induction hypothesis, we have $cl_{3n}(y_1,\vec{x})$, $cl_{3n}(y_2,\vec{x})$, and $cl_{3n}(y_3,\vec{x})$. Hence, we successively get $cl_{3n+1}(z_1 \times y_2,\vec{x})$, $cl_{3n+2}(y_1 \frown (z_1 \times y_2),\vec{x})$ and, finally, $cl_{3n+3}(y_1 \frown (z_1 \times y_2) \frown y_3),\vec{x})$. □

Given a model M of $sw.q. - NIA$ and $\vec{a}$ a sequence of elements of M, we define $cl_n^M(\vec{a}) := \{b \in M : M \models cl_n(b,\vec{a})\}$ and $cl_\infty^M(\vec{a}) := \cup_{n\in\omega} cl_n^M(\vec{a})$. By the previous lemma, it is clear that $cl_\infty^M(\vec{a})$ is a weak substructure of M and, hence, a model of $sw.q. - NIA$.

Proposition 3. *Suppose that $sw.q. - NIA \vdash \forall\vec{x}\exists y A(\vec{x},y)$, where A is a sw.q.-formula. Then there is $n \in \omega$ such that $sw.q. - NIA \vdash \forall\vec{x}\exists y(cl_n(y,\vec{x}) \wedge A(\vec{x},y))$.*

Proof : Assume, to obtain a contradiction, that for all $n \in \omega$, $sw.q. - NIA \nvdash \forall\vec{x}\exists y(cl_n(y,\vec{x}) \wedge A(\vec{x},y))$. Add to the stringlanguage a new sequence of constant symbols $\vec{c}$ (one for each corresponding variable of $\vec{x}$). It is easy to see that the theory $sw.q. - NIA \bigcup \{\forall y(cl_n(y,\vec{c}) \to \neg A(\vec{c},y)) : n \in \omega\}$ is finitely consistent. Hence, by compactness, this theory has a model M. Let us use the very same $\vec{c}$ for the interpretation of the constant symbols $\vec{c}$ in M. As we have remarked, $cl_\infty^M(\vec{c})$ is a model of $sw.q. - NIA$. So, by hypothesis, $cl_\infty^M(\vec{c}) \models \forall\vec{x}\exists y A(\vec{x},y)$. Take $b \in cl_\infty^M(\vec{c})$ such that $cl_\infty^M(\vec{c}) \models A(\vec{c},b)$. By absoluteness, $M \models A(\vec{c},b)$. On the other hand, $b \in cl_n^M(\vec{c})$ for some $n \in \omega$, i.e., $M \models cl_n(b,\vec{c})$. This contradicts the definition of M. □

Let us introduce some easy combinatorial notions. For a positive integer i, denote by b_i the word $00\ldots01$ consisting of $(i+1)$ initial zeroes followed by 1. We say that a word σ has a *k-block*, $k \geq 1$, if there is j, $j \geq 1$, such that $b_j \frown b_{j+1} \frown \ldots \frown b_{j+k-1} \subseteq^* \sigma$.

Lemma. *If the word $\sigma_1 \frown \sigma_2$ has a $2k$-block, then either σ_1 or σ_2 has a k-block.*

Proof : Let β, with $\beta \subseteq^* \sigma_1\sigma_2$, be a $2k$-block. If $\beta \subseteq^* \sigma_1$ or $\beta \subseteq^* \sigma_2$, there is nothing to prove. Otherwise, $\beta = \rho_1\rho_2$ with $\sigma_1 = \sigma_1'\rho_1$ and $\sigma_2 = \rho_2\sigma_2'$, for some σ_1', σ_2'. Consider β_1' the largest initial sub-block of β such that $\rho_1 = \beta_1'\alpha_1$, for some α_1, and consider β_2' the largest final sub-block of β such that $\rho_2 = \alpha_2\beta_2'$, for some α_2. Clearly, $\alpha_1\alpha_2$ is either ϵ or a 1-block. Hence, if β_1' is a i-block and β_2' is a j-block, we have $i + j \geq 2k - 1$. This implies that either $i \geq k$ or $j \geq k$. □

Lemma. *If the word $\sigma_1 \times \sigma_2$ has a $4k$-block, then σ_1 has a k-block.*

Proof : Let β, with $\beta \subseteq^* \sigma_1 \times \sigma_2$, be a $4k$-block. We claim that $\beta \subseteq^* \sigma_1\sigma_1\sigma_1$. Note that if this is the case, then the result follows from the previous lemma.

In order for $\sigma_1 \times \sigma_2$ to have a $4k$-block, σ_1 must have at least two 1's. So, consider a fixed subword τ of σ_1 of the form $100\ldots01$. If $\beta \subseteq^* \overbrace{\sigma_1\sigma_1\ldots\sigma_1}^{j\text{-times}}$, with $j > 3$, and $\beta \not\subseteq^* \sigma_1\sigma_1\sigma_1$, then $\sigma_1\sigma_1 \subseteq^* \beta$. This implies that τ occurs twice in β, contradicting the form of β. □

We are now ready to prove the theorem.

Proof of the theorem: In order to obtain a contradiction, assume that $sw.q.-NIA \vdash \forall x \exists y \text{“}y = \bar{x}\text{”}$. Then, by proposition 3, there is $n \in \omega$ such that $sw.q.-NIA \vdash \forall x \exists y (cl_n(y,x) \wedge \text{“}y = \bar{x}\text{”})$. In particular, this is true in the standard model $\{0,1\}^*$. For this n consider the word $\rho = \bar{b}_1 \frown \bar{b}_2 \frown \ldots \frown \bar{b}_{4^n}$. We claim that the 4^n-block $b_1 \frown b_2 \frown \ldots \frown b_{4^n}$ is not in $cl_n^{\{0,1\}^*}(\rho)$. This is, of course, a contradiction.

We actually prove that for any $k \in \omega$, if $\sigma \in cl_k^{\{0,1\}^*}(\rho)$ then σ does not contain 4^k-blocks. The claim follows from the case $k = n$. We show this by induction on k. If $k = 0$ then either $\sigma = 0$ or $\sigma = 1$ or $\sigma \subseteq^* \rho$: in all these cases $001 \not\subseteq^* \sigma$ and, hence, σ does not have 4^0-blocks. Assume the result for k and suppose that $\sigma \in cl_{k+1}^{\{0,1\}^*}(\rho)$. Then there are $\sigma_1, \sigma_2 \in cl_k^{\{0,1\}^*}(\rho)$ such that either $\sigma = \sigma_1 \frown \sigma_2$ or $\sigma = \sigma_1 \times \sigma_2$. Now, if σ has 4^{k+1}-blocks then, by the previous two lemmas, we can conclude that either σ_1 or σ_2 has 4^k-blocks, which contradicts the induction hypothesis. □

The results of this second section appeared in our Ph.D. Dissertation [3]. An abstract reporting them was published in The Journal of Symbolic Logic (see [17]). A preliminary result towards proving the main result of this section was first obtained by Mantzivis. Mantzivis' result is concerned with a theory even weaker than $sw.q.-NIA$, namely the theory of the stringlanguage consisting of the fourteen basic open axioms together with the scheme of induction on notation (NIA) for the smallest class of formulae that contains the atomic formulae and it is closed under Boolean operations and *initial* subword quantification. Mantzivis showed that the function that associates to a non-empty word the one obtained by deleting its first bit, is not provably total in this theory.

References

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

[2] Petr Hájek and Pavel Pudlák. *Metamathematics of First-Order Arithmetic*. Perspectives in Mathematical Logic. Springer-Verlag, 1993.

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

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

[5] W. V. Quine. Concatenation as a basis for arithmetic. *The Journal of Symbolic Logic*, 11:105–114, 1946.

[6] Raymond Smullyan. *Theory of Formal Systems*. Princeton University Press, 1961.

[7] Neil Immerman. Descriptive and computational complexity. In Juris Hartmanis, editor, *Computational Complexity Theory*. American Mathematical Society, 1989. Volume 38 of the Proceedings of Symposia in Applied Mathematics.

[8] Fernando Ferreira. On end-extensions of models of $\neg exp$. Technical Report 5, CMAF: Universidade de Lisboa, 1994.

[9] Larry Stockmeyer and Uzi Vishkin. Simulation of parallel random access machines by circuits. *SIAM Journal of Computing*, 13:409–422, 1984.

[10] Domenico Zambella. *Chapters on Bounded Arithmetic & Provability Logic*. PhD thesis, Universiteit van Amsterdam, September 1994. The relevant chapter is the first.

[11] J. Saxe M. Furst and M. Sipser. Parity, circuits and the polynomial time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.

[12] Miklos Ajtai. Σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–24, 1983.

[13] Ingo Wegener. *The Complexity of Boolean Functions*. Wiley-Teubner, 1987.

[14] Spyro-Giorgio Mantzivis. Circuits in bounded arithmetic (part I). *Annals of Mathematics and Artificial Intelligence*, 6:127–156, 1992.

[15] Alex Wilkie and Jeff Paris. On the scheme of induction for bounded arithmetic formulas. *Annals of Pure and Applied Logic*, 35:261–302, 1987.

[16] Gaisi Takeuti. Sharply bounded arithmetic and the function $a\dot{-}1$. In Wilfried Sieg, editor, *Logic and Computation*, pages 281–288. American Mathematical Society, 1990.

[17] Fernando Ferreira. Subword quantification and the complement function (abstract). *The Journal of Symbolic Logic*, 57:295, 1992.