On end-extensions of models of $\neg exp$

Fernando Ferreira

Universidade de Lisboa, Portugal

Abstract

Every model of $I\Delta_0$ is the tally part of a model of the stringlanguage theory Th-FO (a main feature of which consists in having induction on notation restricted to certain AC^0 sets). We show how to "smoothly" introduce in Th-FO the binary length function, whereby it is possible to make exponential assumptions in models of Th-FO. These considerations entail that every model of $I\Delta_0 + \neg exp$ is a proper initial segment of a model of Th-FO and that a *modicum* of bounded collection is true in these models.

Mathematics Subject Classification: 03F30, 03C62, 68Q15.

Keywords: bounded arithmetic; $I\Delta_0$; computational complexity; AC^0; bounded collection.

1 Introduction

Consider a model of Samuel Buss' bounded arithmetic theory S_2^1 (see [1]). The elements of this model can be seen as finite (standard and non-standard) sequences of zeroes and ones (strings). Its tally elements (i.e., its elements that are strings of ones) make up, in a natural way, a model of $I\Delta_0$ (where, for instance, addition is given by the concatenation of two strings). In fact, the tally part of this model is even a model of Buss' stronger theory V_1^1. Furthermore, any model of V_1^1 is the tally part of a model of S_2^1. A perfect matching, we may say. This correspondence is much more general than this particular case. For instance, the tally parts of models of S_{k+1}^i are, exactly, the models of V_k^i. These results are essentially due to Jan Krajíček [2]. They also appeared in the first version of this paper [3], and syntactic formulations of them were obtained by Gaisi Takeuti and Alexander Razborov (in [4] and [5], respectively). A question pops out: what is exactly the theory of which $I\Delta_0$ is the tally part? That is, we want to solve the "equation":

$$\frac{S_2^1}{V_1^1} = \frac{x}{I\Delta_0}$$

Contrary to the case of the theories S_2^1 and V_1^1, there is a (seemingly) unavoidable change of language between the language of arithmetic of $I\Delta_0$ and the stringlanguage of the theory *Th-FO* that is the solution to the above "equation" (formulations of the this theory were also independently given by Domenico Zambella [6] and Peter Clote & Gaisi Takeuti [7]). The problem concerns the multiplication function. More specifically, the theory Th-FO has induction on notation for predicates in Neil Immerman's class *FO* of *first-order expressible* properties (these are defined in terms of first-order definability in suitable finite structures with domain $\{0, 1, \ldots, n\}$; Immerman's original paper is [8]). This 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). Well, it stems from deep work of M. Ajtai [9] and, independently, of M. Furst, J. Saxe and M. Sipser (see [10] for an exposition of this latter work) that the multiplication function is not an AC^0 notion (however, it is an open question whether the *graph* of multiplication is in AC^0).

The language which we use for formulating Th-FO was introduced in [11], and an interesting feature of it is that although multiplication is conspicuous by its absence, it is nevertheless possible to formulate exponential assumptions in Th-FO. More precisely, the binary length function $\ell h(x)$, which gives (in binary notation) the length of a string, is an FO-function and provably satisfies in Th-FO some basic properties. This has some nice implications, namely that every model of $I\Delta_0 + \neg exp$ sits, as a *proper* initial segment, in a model of Th-FO. This, in turn, implies that a *modicum* of bounded collection is provable in $I\Delta_0 + \neg exp$. Moreover, this *modicum* is almost the best that we can, at present, hope for (some more of bounded collection entails a positive answering to the $P \neq NP$ question). These results give insight into a question of Alex Wilkie and Jeff Paris, on whether the theory $I\Delta_0 + \neg exp$ proves the scheme of collection for bounded formulae.

This paper is organized in the following way. In the next section we establish and give a precise meaning to the correspondence between Th-FO and $I\Delta_0$. While at this, we define FO-relations and functions in arbitrary models of Th-FO. In the third section we expand the original language of Th-FO in order to have available a function symbol for each (description of a) FO-function. This expansion is technically useful in the final section and, incidentally, permits the characterization of the provably total functions (with appropriate graphs) of Th-FO. In the fourth section we show how to make exponential assumptions in models of Th-FO and prove that a *modicum* of bounded collection holds in models of $I\Delta_0 + \neg exp$. The last result of the paper separates the theories Th-FO and $I\Delta_0$ by a Π^0_1-sentence.

2 The correspondence between $\mathbf{I\Delta_0}$ and Th-FO

The first-order stringlanguage of the binary tree of the finite sequences of zeroes and ones 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:

$$\begin{array}{rl}
x \frown \epsilon = x & x \times \epsilon = \epsilon \\
x \frown (y \frown 0) = (x \frown y) \frown 0 & x \times (y \frown 0) = (x \times y) \frown x \\
x \frown (y \frown 1) = (x \frown y) \frown 1 & x \times (y \frown 1) = (x \times y) \frown x \\
x \frown 0 = y \frown 0 \rightarrow x = y & x \frown 1 = y \frown 1 \rightarrow x = y
\end{array}$$

$$\begin{array}{rcl}
x \subseteq \epsilon & \leftrightarrow & x = \epsilon \\
x \subseteq y \frown 0 & \leftrightarrow & x \subseteq y \vee x = y \frown 0 \\
x \subseteq y \frown 1 & \leftrightarrow & x \subseteq y \vee x = y \frown 1 \\
x \frown 0 & \neq & y \frown 1 \\
x \frown 0 & \neq & \epsilon \\
x \frown 1 & \neq & \epsilon
\end{array}$$

The interpretations of the symbols of the stringlanguage in the standard model are immediately clear, except (perhaps) for $\times$. The language is simple and natural, but unfamiliarity takes a toll. For ease and convenience of reference, we present a small table:

symbol	*formal definition*	*standard interpretation*
ϵ	primitive	empty word
0	primitive	one bit word 0
1	primitive	one bit word 1
$x \frown y$	primitive	concatenation of x with y
$x \times y$	primitive	$x \frown x \frown \ldots \frown x$, length($y$) times
$x \subseteq y$	primitive	x is an initial subword of y
$x \subset y$	$x \subseteq y \wedge x \neq y$	x is a proper initial subword of y
$x \subseteq^* y$	$\exists z \subseteq y(z \frown x \subseteq y)$	x is a subword of y
$tally(x)$	$x = 1 \times x$	x is a string of 1's
$x \leq y$	$1 \times x \subseteq 1 \times y$	length(x)$\leq$length(y)
$x \equiv y$	$x \leq y \wedge y \leq x$	x and y have the same length
$bit(x,u) = 1$	$\exists w \subseteq x(w \equiv u \wedge w1 \subseteq x)$	the (length(u) + 1)-bit of x is 1
$bit(x,u) = 0$	$\exists w \subseteq x(w \equiv u \wedge w0 \subseteq x)$	the (length(u) + 1)-bit of x is 0

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 $\forall x \subseteq^* t(\ldots)$ or $\exists x \subseteq^* t(\ldots)$, where t is a term in which the variable x does not occur. Let Ψ be a class of formulae of the stringlanguage. The theory Ψ-NIA (for *Notation Induction Axioms*) consists of the fourteen basic open axioms plus the induction scheme:

$$F(\epsilon) \wedge \forall x(F(x) \to F(x0) \wedge F(x1)) \to \forall x F(x) \tag{1}$$

where $F \in \Psi$, possibly with parameters. In the sequel, we will use at ease plenty of simple facts that can be deduced in the theory sw.q.-NIA. Here is a sample of them: $0 \neq 1$; $(xy)z = x(yz)$; $x \subseteq xz$; $xy \subseteq xw \to y \subseteq w$; $x \equiv y \wedge x \subseteq y \to x = y$; $x \subseteq z \wedge y \subseteq z \to x \subseteq y \vee y \subseteq x$; $x \subset y \to x0 \subseteq y \dot{\vee} x1 \subseteq y$; and $x \subseteq y \wedge y \subseteq x \to x = y$. A longer list of simple facts like these, together with deductions of them in sw.q.-NIA, can be found in [11]. Two properties of sw.q.-NIA are directly relevant for this paper. Firstly, the tally part of a model of sw.q.-NIA is a model of $I\Delta_0$ in a natural way: just interpret the constant 0 by ϵ, the successor function S by "concatenation with 1", "+" by "$\frown$", "$\cdot$" by "$\times$" and "$\leq$" by "$\subseteq$". Secondly, the following holds:

Proposition. $sw.q.-NIA \vdash \forall x \forall y(x \equiv y \wedge \forall u \subset 1 \times x(bit(x,u) = 1 \leftrightarrow bit(y,u) = 1) \to x = y)$.

Proof : We reason inside an arbitrary model of sw.q.-NIA. Suppose that the antecedent of the implication holds. We show, by induction on notation on the variable z, that $\forall z(z \subseteq x \wedge \forall u \subset 1 \times z(bit(z,u) = 1 \leftrightarrow bit(y,u) = 1) \to z \subseteq y))$. Note that the case $z = x$ yields $x \subseteq y$. Similarly, we can show that $y \subseteq x$ and, hence, conclude that $x = y$.

The base case of the induction is clear. Assume that $z0 \subseteq x$ and that $\forall u \subset 1 \times z0(bit(z0,u) = 1 \leftrightarrow bit(y,u) = 1)$ (the case for $z1$ is handled similarly). By induction hypothesis, we can conclude that $z \subseteq y$. Moreover, it is easy to argue that $z \neq y$. (Just this once we present the full argument: $z = y \Rightarrow z \equiv y \Rightarrow z \equiv x \Rightarrow 1 \times z = 1 \times x \Rightarrow (1 \times z)1 \not\subseteq 1 \times x \Rightarrow 1 \times z0 \not\subseteq 1 \times x \Rightarrow z0 \not\subseteq x$.) Hence, either $z0 \subseteq y$ or $z1 \subseteq y$. The second case leads to a contradiction. In effect, if $z1 \subseteq y$ then $bit(y, 1 \times z) = 1$ and, by assumption, $bit(z0, 1 \times z) = 1$, which is a contradiction. □

We caution the reader not to be misled by the apparent strength and elegance of the theory sw.q.-NIA. In our opinion, this theory is uninteresting and artificial (see [12] for a discussion of this). The same cannot be said of the following theory,

Definition. *The theory* Th-FO *is the theory sw.q.-NIA plus the following string-building principle:*

$$\forall u(tally(u) \to \exists x \equiv u \forall v \subset u(bit(x, v) = 1 \leftrightarrow F(v))) \tag{2}$$

where F is a sw.q.-formulae, possibly with parameters.

In order to "grow" a model of Th-FO out of an arbitrary "$I\Delta_0$-tally", it is convenient to work with a second-order (or relativized) version of $I\Delta_0$. This theory, called $\Delta_0 - CA_0$ ("CA" for comprehension axiom), is formulated in a two-sorted language with number variables, $w, y, z, \ldots$ and set variables $W, Y, Z, \ldots$. A *first-order* formula is a formula that does not contain any quantifications over set variables; following [1], we say that a formula is *bounded* if it does not contain any unbounded quantifications over number variables (it may contain quantifications over set variables or bounded quantifications over number variables). Equality between set variables "$Y = Z$" is not a primitive notion, but rather defined by "$\forall w(w \in Y \leftrightarrow w \in Z)$" and, hence, it is not a bounded formula. The axioms of $\Delta_0 - CA_0$ are the basic axioms of $I\Delta_0$ (see, for instance, the fifteen axioms of PA^- in chapter 2 of [13]), plus the induction axiom $\forall W(0 \in W \wedge \forall w(w \in W \to w+1 \in W) \to \forall w(w \in W))$ and the comprehension scheme $\exists W \forall w(w \in W \leftrightarrow A(w))$, where A is a bounded first-order formula, possibly with number or set parameters. Remark that the combination of the axiom of induction with the comprehension scheme gives rise to the scheme of induction for bounded first-order formulae (i.e., $I\Delta_0$ is a subtheory of $\Delta_0 - CA_0$). A *structure* for the language of $\Delta_0 - CA_0$ is a pair $\mathcal{M} = (M, S)$, where M is a structure for the language of first-order arithmetic, and S is a set of subsets of M (occasionally, we will use the notation $S^{\mathcal{M}}$ to make visible the fact that S comes from the model $\mathcal{M}$). The main thing to observe in the clauses for the truth definition is that the set variables range over S. This means that the logic of the theory $\Delta_0 - CA_0$ is first-order logic.

Proposition. *For any model M of $I\Delta_0$, there is S a set of subsets of M such that (M, S) is a model of $\Delta_0 - CA_0$.*

Proof : Just let S be the set of all Δ_0-definable subsets of M. □

Corollary. *The theory $\Delta_0 - CA_0$ is conservative over $I\Delta_0$.*

Proof : This is a consequence of the above proposition and the completeness theorems. □

A bounded formula of the theory $\Delta_0 - CA_0$ is called *strictly bounded*, if all its atomic subformulae of the form $t \in W$ occur in the context $t \in W \wedge t < w$ (abbreviated, $t \in W^w$), with w not occuring in the term t. Given a model $\mathcal{M} = (M, S)$ of $\Delta_0 - CA_0$, and given $\alpha \in M$ and $\Omega \in S$, we denote by Ω^α the pair $(\{\beta \in M : \mathcal{M} \models \beta \in \Omega \wedge \beta < \alpha\}, \alpha)$. The element α is called the $\mathcal{M}$-length of the pair. (Note that the first entry of Ω^α is in S.) Call S_b the set of all these pairs.

Definition. *A description of a k-ary* FO-relation *is a first-order strictly bounded formula*

$$A(w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$$

where all the free variables are as shown.

Let A be as in the previous definition. Given $\mathcal{M} = (M, S)$ a model of $\Delta_0 - CA_0$, there is a natural way of defining a k-ary relation $[A]_{\mathcal{M}}$ in S_b: we say that $(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) \in [A]_{\mathcal{M}}$ if, and only if, $\mathcal{M} \models A(\alpha_1, \ldots, \alpha_k, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$. Let us give some examples/definitions:

1. *equal*(W^w, Y^y): $w = y \wedge \forall z < w(z \in W^w \leftrightarrow z \in Y^y)$.
2. *initial*(W^w, Y^y): $w \leq y \wedge \forall z < w(z \in W^w \leftrightarrow z \in Y^y)$.

3. $part(W^w, Y^y)$: $\exists x \leq y(x + w \leq y \wedge \forall z < w(z \in W^w \leftrightarrow x + z \in Y^y))$.

4. Given A and B descriptions of k-ary FO-relations, define $neg(A)$ and $and(A, B)$ by $\neg A$ and $A \wedge B$, respectively.

5. Given $A(w, w_1, \ldots, w_k, W^w, W_1^{w_1}, \ldots, W_k^{w_k})$ a description of a $(k+1)$-ary FO-relation, define the $(k+1)$-ary FO-relation $all(A)$ by

$$\forall x \leq w \forall v \leq w(x \leq v \rightarrow A(v - x, w_1, \ldots, w_k, W^w||_{[x,v]}, W_1^{w_1}, \ldots, W_k^{w_k}))$$

with x and v new variables. In the above, $\ldots, W^w||_{[x,v]}, \ldots$ modifies the formula at hand by replacing its subformulae of the form $t \in W^w$ by $x + t \in W^v$. This definition is contrived so that, given any model $\mathcal{M} = (M, S)$ of $\Delta_0 - CA_0$ and given $\Omega^\alpha, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ in S_b then, $(\Omega^\alpha, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) \in [all(A)]_{\mathcal{M}}$ if, and only if, for all Σ^β such that $\mathcal{M} \models part(\Sigma^\beta, \Omega^\alpha)$, $(\Sigma^\beta, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) \in [A]_{\mathcal{M}}$.

Definition. *A description of a k-ary* FO-function *is a pair consisting of a first-order strictly bounded formula*

$$A(u, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$$

and a term $t(w_1, \ldots, w_k)$, where all the free variables are as shown. The variable u is called the special *variable of the description.*

Let (A, t) be as in the previous definition. Given $\mathcal{M} = (M, S)$ a model of $\Delta_0 - CA_0$, we want to define a k-ary total function $[A, t]_{\mathcal{M}}$ in S_b. Take $\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ elements of S_b. By (something equivalent to) the least number principle in $\Delta_0 - CA_0$, there is a unique $\alpha \in M$ such that $\mathcal{M} \models L_{[A,t]}(\alpha, \alpha_1, \ldots, \alpha_k, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$, where $L_{[A,t]}(u, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$ is the following first-order strictly bounded formulae:

$$[\forall w \leq t(w_1, \ldots, w_k) A(w, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k}) \wedge u = 0] \vee$$
$$\vee [u \leq t(w_1, \ldots, w_k) \wedge \neg A(u, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k}) \wedge$$
$$\wedge \forall w \leq t(w_1, \ldots, w_k)(u < w \rightarrow A(w, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k}))]$$

Now, define $[A, t]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) = \{\beta \in M : \mathcal{M} \models A(\beta, \alpha_1, \ldots, \alpha_k, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})\}^\alpha$. The idea is that α, which is the greatest element not exceeding t for which A is false (otherwise, α is 0), operates as a mark for the $\mathcal{M}$-length of $[A, t]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$.

The following are some examples/definitions:

6. $conc(W^w, Y^y)$: $(u \in W^w \vee (w \leq u \wedge u - w \in Y^y), w + y)$.

7. $prod(W^w, Y^y)$: $(\exists q < y \exists r < w(u = qw + r \wedge r \in W^w), wy)$.

8. $tail(W^w, Y^y)$: $(y + u \in W^w \vee y + u > w, w)$.

9. Constants (0-ary functions) are not ruled out in the above definition. The next three 0-ary description will be of use later: $(u = u, 0)$, $(u \neq u, 1)$, and $(u = 0, 1)$.

10. Let (A, t) be a description of a k-ary FO-function such that, for any model $\mathcal{M}$ of $\Delta_0 - CA_0$, the $\mathcal{M}$-length of any value in the range of $[A, t]_{\mathcal{M}}$ is 1. We may consider this description the characteristic function of the k-ary FO-relation given by the description,

$$A(0, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$$

A suitable formulation of the converse statement also holds.

11. Given a description $D = (B(u, y_1, \ldots, y_k, Y_1^{y_1}, \ldots, Y_k^{y_k}), t(y_1, \ldots, y_k))$ of a k-ary FO-function, and given k descriptions $D_i = (A_i(u, w_1, \ldots, w_r, W_1^{w_1}, \ldots, W_r^{w_r}), t_i(w_1, \ldots, w_r))$, $1 \leq i \leq k$, of r-ary FO-functions, we define (the composition of these functions by) the r-ary function description $comp(D; D_1, \ldots, D_k)$ whose first component is

$$\exists y_1 \leq t_1(\vec{w}) \ldots \exists y_k \leq t_k(\vec{w}) \, (\bigwedge_{1 \leq i \leq k} L_{[D_i]}(y_i, \vec{w}, W_1^{w_1}, \ldots, W_r^{w_r})$$

$$\wedge \, (B(u, \vec{y}, Y_1^{y_1}|_{A_1}, \ldots, Y_k^{y_k}|_{A_k}) \vee u > t(y_1, \ldots, y_k)))$$

and whose second component is $t(t_1(\vec{w}), \ldots, t_k(\vec{w}))$. In the above, $\ldots, Y^y|_A, \ldots$ modifies the formulae at hand by replacing its subformulae of the form $t \in Y^y$ by $A(t, \ldots) \wedge t < y$. This definition is contrived to make the following true: if $\mathcal{M} = (M, S)$ is a model of $\Delta_0 - CA_0$ then, for all $\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ in S_b, $[comp(D; D_1, \ldots, D_k)]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) = [D]_{\mathcal{M}}([D_1]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}), \ldots, [D_k]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}))$.

12. Given $D(w, w_1, \ldots, w_k, W^w, W_1^{w_1}, \ldots, W_k^{w_k})$ a description of a $(k+1)$-ary FO-relation, let $witness(D)$ be the $(k+1)$-ary function description whose first component is

$$\forall v \leq w [D(v, w_1, \ldots, w_k, W^v, W_1^{w_1}, \ldots, W_k^{w_k}) \wedge$$

$$\wedge \, \forall x < v \neg D(x, w_1, \ldots, w_k, W^x, W_1^{w_1}, \ldots, W_k^{w_k}) \rightarrow u \in W^v \vee u > v]$$

and whose second component is w. Consider $\mathcal{M} = (M, S)$ a model of $\Delta_0 - CA_0$, and take $\Omega^\alpha, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ elements of S_b for which there is $\beta \leq \alpha$ such that $(\Omega^\beta, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) \in [D]_{\mathcal{M}}$. Then $[witness(D)]_{\mathcal{M}}(\Omega^\alpha, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) = \Omega^\beta$, for the least such β.

13. Given $D(w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$ a description of a n-ary FO-relation and given two descriptions $D_i = (A_i(u, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k}), t_i(w_1, \ldots, w_k))$, $i \in \{0, 1\}$, of k-ary functions, let $case(D; D_1, D_2)$ be the k-ary function description whose first component is

$$[D(w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$$
$$\wedge (A_1(u, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k}) \vee u > t_1(w_1, \ldots, w_k))]$$
$$\vee \, [\neg D(w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$$
$$\wedge (A_2(u, w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})) \vee u > t_2(w_1, \ldots, w_k))]$$

and whose second component is $t_1(w_1, \ldots, w_k) + t_2(w_1, \ldots, w_k)$. Consider $\mathcal{M} = (M, S)$ a model of $\Delta_0 - CA_0$ and take $\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ elements of S_b. Then,

$$[case(D; D_1, D_2)]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) =$$

$$= \begin{cases} [D_1]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) & \text{if } (\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) \in [D_1]_{\mathcal{M}} \\ [D_2]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) & \text{otherwise} \end{cases}$$

Theorem. *Every model of $I\Delta_0$ is the tally part of a model of Th-FO.*

Proof : Let M be a model of $I\Delta_0$ and take S such that $\mathcal{M} = (M, S)$ is a model of $\Delta_0 - CA_0$. The model $\mathcal{M}$ is the basis for the construction of a model $\mathcal{M}^\diamond$ of Th-FO whose tally part is M. The universe of $\mathcal{M}^\diamond$ is S_b; the interpretations of the constant symbols ϵ, 0 and 1 are M^0, $\emptyset^1$ and $\{0\}^1$, respectively; the interpretation of $\subseteq$ is $[initial]_{\mathcal{M}}$; and the interpretations of $\frown$ and $\times$ are, respectively, $[conc]_{\mathcal{M}}$ and $[prod]_{\mathcal{M}}$. It is straightforward to show that N satisfies the fourteen basic axioms and that the map $i(\alpha) := \{\beta \in M : \beta < \alpha\}^\alpha$ is an isomorphism between M and the tally part of $\mathcal{M}^\diamond$. The following are also easy to check:

i) for all Ω in S, $\mathcal{M}^\diamond \models \Omega^0 = \epsilon$;

ii) for all α, β in M and $\Omega \in S$, $\beta \leq \alpha$ iff $\mathcal{M}^\diamond \models \Omega^\beta \subseteq \Omega^\alpha$;

iii) for all α, β in M and Ω, Σ in S, $\mathcal{M} \models part(\Omega^\alpha, \Sigma^\beta)$ iff $\mathcal{M}^\diamond \models \Omega^\alpha \subseteq^* \Sigma^\beta$;

iv) for all α in M and Ω in S, $\alpha \in \Omega$ (resp., $\alpha \notin \Omega$) iff $\mathcal{M}^\diamond \models \Omega^{\alpha+1} = \Omega^\alpha \frown 1$ (resp., $\Omega^\alpha \frown 0$);

v) for all α, β in M and Ω in S such that $\beta < \alpha$, $\beta \in \Omega$ (resp., $\beta \notin \Omega$) iff $\mathcal{M}^\diamond \models bit(\Omega^\alpha, i(\beta)) = 1$ (resp., $= 0$).

vi) for all α in M and Ω in S, $\mathcal{M}^\diamond \models tally(\Omega^\alpha)$ iff $\Omega^\alpha = i(\alpha)$.

The following fact is crucial to showing that the schemes (1) and (2) hold in $\mathcal{M}^\diamond$ for sw.q.-formulae:

(F1) For every sw.q.-formula $F(x_1, \ldots, x_k)$ of the language of Th-FO, there is a first-order strictly bounded formula $F^\diamond(w_1, \ldots, w_k, W_1^{w_1}, \ldots, W_k^{w_k})$ of the language of $\Delta_0 - CA_0$ such that, for all elements $\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ in S_b,

$$\mathcal{M}^\diamond \models F(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) \Leftrightarrow \mathcal{M} \models F^\diamond(\alpha_1, \ldots, \alpha_k, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$$

The map $^\diamond$ is defined in two steps. Firstly, to each r-ary term t of the language of Th-FO we associate a description $t^\diamond$ for a r-ary FO-function such that, for all $\Omega^\alpha, \Omega_1^{\alpha_1}, \ldots, \Omega_r^{\alpha_r}$ in S_b, $\mathcal{M}^\diamond \models t(\Omega_1^{\alpha_1}, \ldots, \Omega_r^{\alpha_r}) = \Omega^\alpha \Leftrightarrow [t^\diamond]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_r^{\alpha_r}) = \Omega^\alpha$. This term-to-term map is easily defined by induction on the complexity of t with the aid of the examples 6, 7, 9, and 11. Secondly, the map $^\diamond$ is expanded to the sw.q.-formula with the aid of examples 1, 2,4, 5, 10, and 11.

In order to show that (1) holds in $\mathcal{M}^\diamond$, take $F(x, \ldots)$ an arbitrary sw.q.-formula and suppose that $\mathcal{M}^\diamond \not\models F(\Omega^\alpha, \ldots)$, for some Ω^α in S_b and for some parameters. By (F1), $\mathcal{M} \not\models F^\diamond(\alpha, \ldots, \Omega^\alpha, \ldots)$. Due to the fact that $\mathcal{M}$ is a model of $\Delta_0 - CA_0$, either $\mathcal{M}^\diamond \not\models F^\diamond(0, \ldots, \Omega^0, \ldots)$ or $\mathcal{M}^\diamond \models F^\diamond(\beta, \ldots, \Omega^\beta, \ldots) \wedge \neg F^\diamond(\beta+1, \ldots, \Omega^{\beta+1}, \ldots)$, where β is an element of M preceding α. In the first alternative, $\mathcal{M}^\diamond \not\models F(\epsilon, \ldots)$; in the second alternative, $\mathcal{M}^\diamond \models F(\Omega^\beta, \ldots) \wedge \neg F(\Omega^{\beta+1}, \ldots)$ and by the above property iv, we get the right conclusion. To show that (2) holds in $\mathcal{M}^\diamond$, take again a sw.q.-formula $F(x, \ldots)$, and let $\alpha \in M$. We need to prove that there is Ω in S such that, for all $\beta < \alpha$, $\beta \in \Omega$ iff $\mathcal{M} \models F^\diamond(\beta, \ldots, i(\beta), \ldots)$. The existence of such an Ω is a consequence of the comprehension scheme of $\Delta_0 - CA_0$. $\square$

Conversely, to a model N of Th-FO we can associate a model $N^\star$ of $\Delta_0 - CA_0$. The first-order part of $N^\star$ is $tally(N) := \{a \in N : N \models tally(a)\}$ which, as we have already mentioned, is naturally a model of $I\Delta_0$. Given $a \in N$, let $s(a) := \{v \in tally(N) : N \models v \subset 1 \times a \wedge bit(a, v) = 1\}$. Take S^N the set of all subsets Ω of $tally(N)$ satisfying the following condition: for all $u \in tally(N)$, there is $a \in N$, $a \equiv u$, such that $s(a) = \{v \in tally(N) : v \subset u \wedge v \in \Omega\}$. The structure $N^\star$ is, by definition, $(tally(N), S^N)$.

Theorem. *Let N be a model of Th-FO. Then $N^\star$ is a model of $\Delta_0 - CA_0$.*

Proof : We have to check that the induction axiom and the Δ_0-comprehension scheme hold in $N^\star$. To argue for the truth of the induction axiom, take $\Omega \in S^N$, $u \in tally(N)$, and assume that $0 \in \Omega \wedge u \notin \Omega$. By definition of S^N, there is $a \in N$ such that $s(a) = \{v \in tally(N) : v \subset u \frown 1 \wedge v \in \Omega\}$. Hence, $N \models bit(a, \epsilon) = 1 \wedge \neg bit(a, u) = 1$. Now, the scheme of induction on notation for sw.q.-formulae guarantees the existence of $v \subset u$ such that $N \models bit(a, v) = 1 \wedge \neg bit(a, v \frown 1) = 1$, i.e., $v \in \Omega$ and $v +^{N^\star} 1^{N^\star} \notin \Omega$.

In order to so show that the Δ_0-comprehension scheme holds in $N^\star$ we need a lemma and the following fact:

(B1) For every first-order strictly bounded formula $A(w_1,\ldots,w_k,W_1^{w_1},\ldots,W_k^{w_k})$ of the language of $\Delta_0 - CA_0$, there is a sw.q.-formula $A^\star(x_1,\ldots,x_k)$ of the language of Th-FO such that, for all elements $a_1,\ldots,a_k$ in N,

$$N^\star \models A(1\times a_1,\ldots,1\times a_k, s(a_1)^{1\times a_1},\ldots,s(a_k)^{1\times a_k}) \Leftrightarrow N \models A^\star(a_1,\ldots,a_k)$$

The map * is specified in three steps. Firstly, to each term $t(y_1,\ldots,y_r,w_1,\ldots,w_k)$ of the language of $\Delta_0 - CA_0$ we associate a term $t^\star(y_1,\ldots,y_r,x_1,\ldots,x_k)$ of the language of Th-FO, obtained from t by replacing each occurence of 0 by ϵ, of $+$ by $\frown$, of $\cdot$ by $\times$, and each occurence of w_i by $1\times x_i$. Secondly, we define $(t=q)^\star$ as $t^\star = q^\star$, $(t \le q)^\star$ as $t^\star \subseteq q^\star$, and $(t \in W_i^{w_i})^\star$ as $bit(x_i, t^\star)=1$. Finally, let $(\neg A)^\star$ be $\neg A^\star$, $(A\wedge B)^\star$ be $A^\star \wedge B^\star$, and let $(\forall y \le t A(y,\ldots))^\star$ be $\forall y \subseteq t^\star A^\star(y,\ldots)$.

Lemma. *Let $A(y_1,\ldots,y_k,W_1,\ldots,W_r)$ be a bounded formula of the language of $\Delta_0 - CA_0$, where all the free variables are as shown. Then the theory $I\Delta_0$, enlarged with the logical axioms for the second order language, proves the following sentence:*

$$\forall y \exists z \forall x \ge z \forall W_1 \ldots \forall W_r \forall y_1 \le y \ldots \forall y_k \le y (A(y_1,\ldots,y_k,W_1,g,W_r) \leftrightarrow A(y_1,\ldots,y_k,W_1^x,\ldots,W_r^x))$$

Proof of the lemma : The proof is by induction on the complexity of A. There are only three cases we need worrying about. When A is $t(y_1,\ldots,y_k)\in W$, put $z = t(y,\ldots,y)$. This z does the job because all terms of the language of $I\Delta_0$ are provably monotonous. Consider now the case when A is $\exists W B(y_1,\ldots,y_k,W,W_1,\ldots,W_r)$: given y there is, by induction hypothesis, an element z that works for the formula B. The very same z works for A. Lastly, suppose A is $\forall x \le t(y_1,\ldots,y_k) B(x,y_1,\ldots,y_k,W_1,\ldots,W_r)$. Given y, let $y' = max\{y, t(y,\ldots,y)\}$. By induction hypothesis, take z that works for B and y'. Then z does the job for A and the original y. $\square$ (of the lemma)

We are now in position to show that the Δ_0-comprehension scheme holds in $N^\star$. Given a first-order bounded formula $A(y,y_1,\ldots,y_k,W_1,\ldots,W_r)$ and given elements $u_1,\ldots,u_k$ in $tally(N)$ and $\Omega_1,\ldots,\Omega_r$ in S^N, we need to show that the set $\{v \in tally(N) : N^\star \models A(v,u_1,\ldots,u_k,\Omega_1,\ldots,\Omega_r)\}$ is in S^N. According to the definition of S^N, this is equivalent to showing that for all $u \in tally(N)$ there is $a \in N$ such that $s(a)$ is equal to the set $\Sigma = \{v \in tally(N) : v \subset u$ and $N^\star \models A(v,u_1,\ldots,u_k,\Omega_1,\ldots,\Omega_r)\}$. By the previous lemma, Σ is $\{v \in tally(N) : v \subset u$ and $N^\star \models A(v,u_1,\ldots,u_k,\Omega_1^\alpha,\ldots,\Omega_r^\alpha)\}$, for some $\alpha \in tally(N)$. Take $a_1,\ldots,a_r$ in N such that $\Sigma = \{v \in tally(N) : v < u$ and $N^\star \models A(v,u_1,\ldots,u_k,s(a_1)^\alpha,\ldots,s(a_r)^\alpha)\}$. According to property (B1), there is a sw.q.-formula F such that $N \models F(v,u_1,\ldots,u_k,a_1,\ldots,a_r,\alpha)$ if, and only if, $N^\star \models A(v,u_1,\ldots,u_k,s(a_1)^\alpha,\ldots,s(a_r)^\alpha)$. By the string-building principle (2), pick a satisfying the following property: for all $v \in tally(N)$ with $v \subset u$, $N \models bit(a,v) \leftrightarrow F(v,u_1,\ldots,u_k,a_1,\ldots,a_r,\alpha)$. This a does the job. $\square$ (of the theorem)

Let N be a model of Th-FO. It is straightforward to argue that $N^{\star\diamond}$ is isomorphic to N in a natural way (and we write, $N^{\star\diamond} \approx N$). Conversely, consider $\mathcal{M} = (M,S)$ a model of $\Delta_0 - CA_0$. It is easy to argue that $\mathcal{M}^{\diamond\star}$ is (up to a natural isomorphism) of the form (M,S'), with $S_b = S'_b$ (we write, $\mathcal{M}^{\diamond\star} \approx_b \mathcal{M}$). Hence, although $\mathcal{M}^{\diamond\star}$ and $\mathcal{M}$ are not necessarily isomorphic, the above condition is sufficient to insure that bounded formulae are absolute between $\mathcal{M}^{\diamond\star}$ and $\mathcal{M}$ (the lemma inserted in the proof of the previous theorem is used to proving this). These considerations allow us to speak of *natural pairs* $(\mathcal{M},N)$, where $\mathcal{M}$ is a model of $\Delta_0 - CA_0$, N is a model of Th-FO, $N \approx \mathcal{M}^\diamond$, and $N^\star \approx_b \mathcal{M}$.

Consider $(\mathcal{M},N)$ a natural pair and let $\Omega^\alpha \in S_b^{\mathcal{M}}$ and $a \in N$. We say that Ω^α and a are in *natural correspondence* if $\alpha = 1\times a$ and $\{v \in M : v < \alpha \;\&\; v \in \Omega\} = \{v \in tally(N) : v \subset \alpha \;\&\; N \models bit(a,v)=1\}$. With this terminology, if $\Omega_1^{\alpha_1},\ldots,\Omega_k^{\alpha_k}$ and $a_1,\ldots,a_k$ are parwise corresponding elements, then the properties (F1) and (B1) can be rephrased as follows:

(F2) Given $F(x_1, \dots, x_k)$ a sw.q.-formula of the language of Th-FO, $F^\diamond$ is a first-order strictly bounded formula of the language of $\Delta_0 - CA_0$ such that,

$$N \models F(a_1, \dots, a_k) \Leftrightarrow \mathcal{M} \models F^\diamond(\alpha_1, \dots, \alpha_k, \Omega_1^{\alpha_1}, \dots, \Omega_k^{\alpha_k})$$

(B2) Given $A(w_1, \dots, w_k, W_1^{w_1}, \dots, W_k^{w_k})$ a first-order strictly bounded formula of the language of $\Delta_0 - CA_0$, $A^\star(x_1, \dots, x_k)$ is a sw.q.-formula of the language of Th-FO such that,

$$\mathcal{M} \models A(\alpha_1, \dots, \alpha_k, \Omega_1^{\alpha_1}, \dots, \Omega_k^{\alpha_k}) \Leftrightarrow N \models A^\star(a_1, \dots, a_k)$$

A consequence of the above discussion and of the completeness theorems is that the formulae F and $F^{\diamond\star}$ (resp., A and $A^{\star\diamond}$) are equivalent in Th-FO (resp., in $\Delta_0 - CA_0$).

3 The theory Th-FO expanded

In this section we define an expansion Th-FO$^+$ of the theory Th-FO. The language of this new theory consists of the original language of Th-FO plus a k-ary function symbol f_D for each description D of a k-ary FO-function. The axioms of Th-FO$^+$ are those of Th-FO plus two *function axioms* for each such description $D = (A, t)$:

$$\forall x \forall x_1 \dots \forall x_k (L^\star_{[D]}(x, x_1, \dots, x_k) \leftrightarrow f_D(x_1, \dots, x_k) \equiv x) \tag{3}$$

$$\forall u \forall x_1 \dots \forall x_k (u \subset 1 \times f_D(x_1, \dots, x_k) \rightarrow (bit(f_D(x_1, \dots, x_k), u) = 1 \leftrightarrow A^\star(u, x_1, \dots, x_k))) \tag{4}$$

Lemma.

a) Let D be a k-ary FO-description, N a model of Th-FO$^+$, and take $\mathcal{M}$ a model of $\Delta_0 - CA_0$ such that $(\mathcal{M}, N)$ is a natural pair. If $a, a_1, \dots, a_k$ and $\Omega^\alpha, \Omega_1^{\alpha_1}, \dots, \Omega_k^{\alpha_k}$ are pairwise corresponding elements then,

$$N \models f_D(a_1, \dots, a_k) = a \Leftrightarrow [D]_\mathcal{M}(\Omega_1^{\alpha_1}, \dots, \Omega_k^{\alpha_k}) = \Omega^\alpha$$

b) The map $^\diamond$ can be extended to the open formulae of the language of Th-FO$^+$, with the equivalence (F2) still holding.

c) Let D be a description of a k-ary function. Then there is a term q of the language of Th-FO such that,

$$Th - FO^+ \vdash \forall x_1 \dots \forall x_k \, f_D(x_1, \dots, x_k) \leq q(x_1, \dots, x_k)$$

d) For each term $t(x_1, \dots, x_k)$ of the language of Th-FO$^+$, there is a description D of a k-ary FO-function such that,

$$Th - FO^+ \vdash \forall x_1 \dots \forall x_k \, t(x_1, \dots, x_k) = f_D(x_1, \dots, x_k)$$

e) If $F_1(x_1, \dots, x_k), \dots, F_r(x_1, \dots, x_k)$ are open formulae of the language of Th-FO$^+$ and if $D_1, \dots, D_r, D_{r+1}$ are descriptions of k-ary FO-function symbols, then there is a description D' of a k-ary FO-function such that,

$$Th - FO^+ \vdash (F_1 \wedge f_{D'} = f_{D_1}) \vee (\neg F_1 \wedge F_2 \wedge f_{D'} = f_{D_2}) \vee \dots \vee (\neg F_1 \wedge \dots \wedge \neg F_r \wedge f_{D'} = f_{D_{r+1}})$$

f) *For any open formulae $F(x, x_1, \ldots, x_k)$ of the language of Th-FO$^+$, there is a $(k+1)$-ary description D of a FO-function such that,*

$$Th - FO^+ \vdash (\exists y \subseteq xF(y, x_1, ..., x_k)) \rightarrow f_D(x, x_1, ..., x_k) \subseteq x \wedge F(f_D(x, x_1, ..., x_k), x_1, ..., x_k)$$

The same is true (with a different D) if "initial subwordness" is replaced by "subwordness".

Proof : Let $D = (A, t)$ and suppose that $N \models f_D(a_1, \ldots, a_k) = a$. The axiom (3) entails that $N \models L^{\star}_{[D]}(\alpha, a_1, \ldots, a_k)$. By (F2), $\mathcal{M} \models L^{\star\diamond}_{[D]}(\alpha, \alpha_1, \ldots, \alpha_k, i(\alpha), \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$ and, hence, $calM \models L_{[D]}(\alpha, \alpha_1, \ldots, \alpha_k, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$. This shows that the second component of $[D]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$ is, indeed, α. On the other hand, the axiom (4) implies that $\mathcal{M} \models \forall w < \alpha(w \in \Omega^\alpha \leftrightarrow A^{\star\diamond}(w, \alpha_1, \ldots, \alpha_k, i(w), \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}))$. Hence,

$$\mathcal{M} \models \forall w < \alpha(w \in \Omega^\alpha \leftrightarrow A(w, \alpha_1, \ldots, \alpha_k, \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}))$$

From the above, we conclude that the $[D]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}) = \Omega^\alpha$. The converse statement now follows from the bitwise characterization of the elements of N (see the opening proposition of this paper). Part b) is a consequence of part a) and of the examples given in the previous section. The proof of part c) stems easily from the proof of part a). The statements d) and e) and the first part of f) follow from a), the examples 6, 7, 9, 11 (for d), 13 (for e), 12 (for f) of the previous section, and the completeness theorems. The second part of f) reduces to two applications of the first part. In effect, by the example 8 of the previous section, there is a description *tail* of a binary FO-function such that $Th - FO^+ \vdash \forall x \forall y(y \subseteq x \rightarrow y \frown f_{tail}(y, x) = x)$. Now, observe that Th-FO$^+$ proves the equivalence $\exists y \subseteq^* xF(y, \ldots) \leftrightarrow \exists z \subseteq x \exists y \subseteq f_{tail}(z, x)\, F(y, \ldots)$. □

Proposition. *If N is a model of Th-FO$^+$ and R is a substructure of N (with respect to the language of Th-FO$^+$), then R is also a model of Th-FO$^+$.*

Proof : The truth of the fourteen basic axioms is obviously inherited by R, since these axioms are universal. The scheme of induction on notation for sw.q.-formulae can be reformulated by

$$F(\epsilon) \wedge \neg F(y) \rightarrow \exists x \subset y(F(x) \wedge ((x0 \subseteq y \wedge \neg F(x0)) \vee (x1 \subseteq y \wedge \neg F(x1))))$$

where F is a sw.q.-formulae. Hence, the inheritance by R of the truth of this scheme follows from the fact that sw.q.-formulae are absolute between N and R. More specifically: if $F(x_1, \ldots, x_k)$ is a sw.q.-formula and $a_1, \ldots, a_k$ are elements of R, then $R \models F(a_1, \ldots, a_k)$ if, and only if, $N \models F(a_1, \ldots, a_k)$. This fact is proved by induction on the complexity of F, using property f) of the above lemma.

There remains to show that the string-building principle (2) is true in R. To see this, take $F(x, x_1, \ldots, x_k)$ a sw.q.-formula, $a_1, \ldots, a_k$ elements of R and $\alpha \in tally(N)$. Consider the following description D of a $(k+1)$-ary FO-function:

$$(u < w_{k+1} \wedge F^\diamond(u, w_1, \ldots, w_k, i(u), W_1^{w_1}, \ldots, W_k^{w_k}), w_{k+1})$$

where u is the special variable. Pick $\mathcal{M}$ a model of $\Delta_0 - CA_0$ such that $(\mathcal{M}, N)$ is a natural pair, and let $\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ be the parwise corresponding elements to $a_1, \ldots, a_k$. Then, for $\alpha \in M$,

$$[D]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}, i(\alpha)) = \{v \in M : v < \alpha \wedge F^\diamond(v, \alpha_1, \ldots, \alpha_k, i(v), \Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})\}^\alpha$$

According to (B2), the first component of this pair, which we designate by Σ, is $\{v \in tally(N) : N \models v \subset \alpha \wedge F^{\diamond\star}(v, a_1, \ldots, a_k)\}$. Hence, $\Sigma = \{v \in tally(N) : N \models v \subset \alpha \wedge F(v, a_1, \ldots, a_k)\}$. By hypothesis, the element $f_D(\alpha, a_1, \ldots a_k)$ is in R. By a) of the above lemma, this element is the corresponding element to Σ^α. It follows from the definition of "corresponding element" that $f_D(\alpha, a_1, \ldots, a_k)$ is the value a such that $N \models a \equiv \alpha \wedge \forall v \subset \alpha(bit(a, v) = 1 \leftrightarrow F(v, a_1, \ldots, a_k))$. Due to the absoluteness of the sw.q.-formulae, this equivalence holds in R. □

Theorem. *Suppose that* $Th - FO^+ \vdash \forall x_1 \ldots \forall x_k \exists y F(x_1, \ldots, x_k, y)$, *where* F *is an open formula of the language of* $Th - FO^+$. *Then there is a description* D *of a* k*-ary FO-function such that,*

$$Th - FO^+ \vdash \forall x_1 \ldots \forall x_k F(x_1, \ldots, x_k, f_D(x_1, \ldots, x_k))$$

Proof : By the previous proposition, Th-FO$^+$ is a universal theory. Due to d) and e) of the above lemma, the result follows from Herbrand's theorem for universal theories. □

Theorem. *Every model of Th-FO is the reduct of a model of Th-FO*$^+$.

Proof : Take N an arbitrary model of Th-FO and let D be a description of a k-ary FO-function. We define the interpretation of f_D in N in the obvious way: given $a_1, \ldots, a_k$ elements of N, consider $\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k}$ their parwise corresponding elements in a model $\mathcal{M}$ - with $(\mathcal{M}, N)$ a natural pair - and define $f_D(x_1, \ldots, x_k)$ as the corresponding element to $[D]_{\mathcal{M}}(\Omega_1^{\alpha_1}, \ldots, \Omega_k^{\alpha_k})$. It is now a straightforward consequence of the properties (F2) and (B2) that the axioms (3) and (4) hold. □

Corollary. *The theory Th-FO*$^+$ *is conservative over Th-FO.* □

Define a $sw.q.^+ - formulae$ exactly like a sw.q.-formula, except for permitting the new function symbols f_D in the language to start the recursive definition. By b) and f) of the above lemma and by (B2), every such formula is equivalent (modulo ThFO$^+$) to a sw.q.-formula (we will say that this latter formula is obtained by "unwinding" the former formula). Hence, instantiations of the schemes (1) and (2) by sw.q.$^+$-formulae are still valid in Th-FO$^+$. This is a very convenient fact. In effect, it enables the work with function symbols that witness the truth of $\forall\exists sw.q.$-sentences which are provable in Th-FO in order to prove in Th-FO$^+$ a sentence F of the original language, and - finally - to conclude (by the above corollary) that $Th - FO \vdash F$. We describe this process as "working with smoothly introduced function symbols".

4 Exponential assumptions and bounded collection

The formula "$(x \leq y \wedge x \not\equiv y) \vee (x \equiv y \wedge \exists w \subseteq x(w0 \subseteq x \wedge w1 \subseteq y))$", abbreviated "$x <_\ell y$", defines a total ordering in the standard model, first according to length and then, within the same length, lexicographically. With the help of some easy checkings, we can smoothly introduce a unary function symbol $S(x)$ for "the immediate successor of x with respect to $<_\ell$". That is, $Th - FO^+ \vdash S(\epsilon) = 0 \wedge \forall x(S(x0) = x1 \wedge S(x1) = S(x)0)$.

Lemma. *There is a binary sw.q.-formula* $L(x, y)$ *such that,*

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

b) $Th - FO \vdash L(\epsilon, \epsilon)$

c) $Th - FO^+ \vdash \forall x \forall y(L(x, y) \to L(x0, S(y)) \wedge L(x1, S(y)))$

Proof : By results of James Bennett and Jeff Paris, we know that there is a Δ_0-formula $\theta(w, y, z)$ which expresses the relation $w^y = z$ in the standard model of arithmetic and such that the usual defining recurrence relations of exponentiation are provable in $I\Delta_0$. Hence, it is possible to "speak in $I\Delta_0$" of binary expansions of numbers (see [14] for the details). We may also (smoothly) introduce in the language of $I\Delta_0$ function symbols $|w|$ and $(w)_u$ so that "if $w = \sum_{u=0}^{s}(1+\delta_u)\cdot 2^{s-u}$, where $\delta_u \in \{0, 1\}$, then $|w| = s + 1$ and $(w)_u = \delta_u$". As we know, the tally part of a model of Th-FO is a model of $I\Delta_0$. So, by the above discussion and the previous section, we can smoothly introduce in the language of Th-FO two function symbols $|x|$ and $(x)_u$ so that, if $tally(x)$ then

"$x = \sum_{u=0}^{|x|-1}(1+(x)_u)\cdot 2^{|x|-u-1}$, with all the arithmetic operations done in the tally part (and the understanding that $|0| = 0$ and that the empty sum is 0)". Let $L(x, y)$ be the (unwinding of the) following formula,

$$y \equiv |1 \times x| \wedge \forall u \subset |1 \times x| \, (bit(y, u) = 1 \leftrightarrow (1 \times x)_u = 1)$$

Part a) is a consequence of (2) and the bitwise characterization of the elements in models of Th-FO. Part b) is trivial, and part c) holds because the theory $I\Delta_0$ proves that both the indexes and the length of the binary expansion of a number modify in the right way when a unit is added to it. $\Box$

According to the previous section, we can smoothly introduce in Th-FO a unary function symbol ℓh such that: $Th - FO^+ \vdash \ell h(\epsilon) = \epsilon$ and $Th - FO^+ \vdash \ell h(x0) = \ell h(x1) = S(\ell h(x))$. The existence of this function symbol permits the formulation of exponential assumptions in models of Th-FO without having to go through the definition of multiplication.

Lemma.

a) $Th - FO^+ \vdash x \leq y \wedge x \not\equiv y \rightarrow \ell h(x) <_\ell \ell h(y)$

b) $Th - FO^+ \vdash y <_\ell \ell h(x) \rightarrow \exists z \subseteq x \, \ell h(z) = y$

Proof : To show a), fix x and prove by induction on notation on z that $\forall z(z \neq \epsilon \rightarrow \ell h(x) <_\ell \ell h(x \frown z))$. To argue for b), pick y and x with $y <_\ell \ell h(x)$ and, to obtain a contradiction, assume that $\forall z \subseteq x \, \ell h(z) \neq y$. Argue by induction on notation on z that $\forall z(z \subseteq x \rightarrow \ell h(z) <_\ell y)$. The case $z = x$ originates a contradiction. $\Box$

If we view each element x of an arbitrary model of $I\Delta_0$ as the string of zeroes and ones $(x)_0(x)_1 \ldots (x)_{|x|-1}$, it is clear that all the primitive symbols of the stringlanguage have a Δ_0-rendering in the language of arithmetic, except for the binary function symbol $\times$ (a model of $I\Delta_0$ is closed under $\times$ if, and only if, it satisfies the so-called axiom Ω_1). A $sw.q.^m - formula$ of the stringlanguage is defined exactly as a sw.q.-formula except for the $\times$-function symbol, which is replaced by a ternary relational graph counterpart. Clearly, the sw.q.$^{\mathrm{m}}$-formulae have natural Δ_0-renderings. In the sequel, when we speak of sw.q.$^{\mathrm{m}}$-formulae in the language of arithmetic, we mean their natural Δ_0-renderings.

With the above observations in mind, consider M an arbitrary model of $I\Delta_0$. As we have seen, M is the tally part of a model N of Th-FO. Let $\ell h(N)$ be the set $\{x \in N : \exists y \in tally(N) \, \ell h(y) = x\}$. By b) of the previous lemma, $\ell h(N)$ is an initial segment of N, i.e., if $x, y \in N$, $x <_\ell y$ and $y \in \ell h(N)$ then $x \in \ell h(N)$. On the other hand, $\ell h(N)$ can be seen as a copy of M by viewing it as inheriting the Δ_0-structure of M *via* the binary length function (which is injective in the tally part of N). Due to the way the things are set up, the relations of $\ell h(N)$ that come from sw.q.$^{\mathrm{m}}$-relations in M *via* the function ℓh coincide with the sw.q.$^{\mathrm{m}}$-relations that come from the fact that $\ell h(N)$ is a substructure of N. Furthermore, it is clear that the order $<$ of M translates (*via* ℓh) into the order $<_\ell$, and that the successor operation in M translates into the S operation.

The discussion in the previous paragraph is summarized by the first part of the following result:

Main Theorem. *Every model M of $I\Delta_0$ is the initial segment of a model N of Th-FO such that $\ell h(N) = M$. Moreover, if M is not a model of exp, then M is a* proper *initial segment of N.*

Proof : In order to prove the second part of this result, we need to make a preliminary observation. In the observation, as well as in the remaining of the proof, we identify M with $tally(N)$ (this is not so in the statement of the theorem). Suppose that $y \in tally(N)$ is an element such that $x = \ell h(y) \in tally(N)$. Since x is a string of ones in N we conclude, by the definition of ℓh, that $M \models$ "$y = \sum_{u=0}^{x-1} 2^{x-u}$", i.e., $M \models$ "$y = 2^{x+1} - 2$". (The converse also holds, i.e., if $x, y \in M$ and $M \models$ "$y = 2^{x+1} - 2$" then $N \models \ell h(y) = x$.)

Now, assume that $\ell h(N) = N$ and take an arbitrary element $x \in tally(N)$. By assumption, there is $y \in tally(N)$ such that $\ell h(y) = x$. Hence, $M \models$ "$y = 2^{x+1} - 2$". This entails that $M \models \exists y$"$y = 2^x$". $\Box$

We have the folowing interesting situation. Every model M of $I\Delta_0 + \neg exp$ is a proper initial segment of a model of Th-FO but, in the meantime, while going from the original model to its end-extension, the language changes from the language of arithmetic to the stringlanguage of the binary tree. Moreover, this is a genuine change, since it does not seem possible to "smoothly" define the multiplication function in the end-extension.

There is a *canonical way* of associating a model N_M of Th-FO to a model M of $I\Delta_0$ satisfying the specifications of the previous theorem. Just let N_M be $(M,S)^\diamond$, where S is the set of all Δ_0-definable subsets of M. This permits to give a meaning to the concept of FO-relation in an arbitrary model of $I\Delta_0$. More precisely, we say that $X \subseteq M^r$ defines a r-ary *FO-relation in* M if there is a sw.q.-formula $F(\vec{x}, \vec{y})$ and parameters $\vec{p}$ in M such that $X = \{\vec{x} \in M^r : N_M \models F(\vec{x}, \vec{p})\}$. Obviously, there is a direct way to define FO-relations in models of $I\Delta_0 + \Omega_1$. The reader should convince himself that, in this case, the two notions coincide.

The next three theorems are variations on a single theme, that of "a *modicum* of bounded collection holds in models of $I\Delta_0 + \neg exp$".

Theorem (variation I). *Let M be a model of $I\Delta_0 + \neg exp$ and suppose that $X \subseteq M \times M$ is a binary FO-relation in M. Then, for all $a \in M$,*

$$M \models \forall x \leq a \exists y (T(y) \wedge (x,y) \in X) \rightarrow \exists z \forall x \leq a \exists y \leq z \, (x,y) \in X \tag{5}$$

where $T(y)$ stands for $\exists u$"$2^{u+1} - 2 = y$".

Proof : First of all note that for any $a \in M$, $M \models T(a) \Leftrightarrow N_M \models tally(a)$. (This was argued for in the proof of the main theorem.) By definition of FO-relation in M, there is a sw.q.-formula $F(x,y,\vec{w})$ and elements $\vec{p}$ in M such that $X = \{(x,y) \in M^2 : N_M \models F(x,y,\vec{p})\}$. Assume, by hypothesis, that $M \models \forall x \leq a \exists y (T(y) \wedge (x,y) \in X)$. We may rephrase this by $N_M \models \forall x \leq_\ell a \exists y \in M(tally(y) \wedge F(x,y,\vec{p}))$. Hence, for every element $y_0 \in tally(N_M) \setminus M$, we have $N_M \models \forall x \leq_\ell a \exists y \subseteq y_0 F(x,y,\vec{p})$.

Let $b \in tally(N_M)$ such that $N_M \models \ell h(b) = a$. Using the fact that $\{x \in M : x \leq_\ell a\} = \{\ell h(u) : u \subseteq b\}$, we get

$$N_M \models \forall u \subseteq b \exists y \subseteq y_0 \, F(\ell h(u), y, \vec{p}) \tag{6}$$

for every $y_0 \in tally(N_M) \setminus M$. The formula to the right of the symbol "$\models$" is a sw.q.$^+$-formula. By an underspill argument, we may conclude that there is $y_0 \in tally(N_M) \cap M$ for which (6) holds. This entails that $M \models \forall x \leq a \exists y \leq y_0 (x,y) \in X$. $\Box$

The next variation is a weaker, purely syntactical corollary of the previous variation.

Theorem (variation II). *For any sw.q.$^{\mathrm{m}}$-formulae $A(x,y)$, possibly with parameters, of the language of arithmetic,*

$$I\Delta_0 + \neg exp \vdash \forall x \leq a \exists y (T(y) \wedge A(x,y)) \rightarrow \exists z \forall x \leq a \exists y \leq z A(x,y) \tag{7}$$

where $T(y)$ stands for $\exists u$"$2^{u+1} - 2 = y$". $\Box$

Ever since the seminal work of Jeff Paris and Laurence Kirby in [15], it is well known that the theory $I\Delta_0$ does not prove the scheme of collection for bounded arithmetic formulae, i.e., does not prove every instance of

$$\forall x \leq a \exists y A(x,y) \rightarrow \exists z \forall x \leq a \exists y \leq z A(x,y) \tag{8}$$

where A is a bounded formulae of the language of arithmetic (possibly with parameters). More recently, at the end of [16], Alex Wilkie and Jeff Paris asked the "intriguing" (*sic*) question of whether the above scheme (8) is provable in $I\Delta_0 + \neg exp$. The previous two variations say that a *modicum* of bounded collection is, indeed, a consequence of this theory. Remark that this *modicum* is non-trivial since, in the presence of *exp*, it implies the full scheme of bounded collection (note that when exponentiation holds, bounded quantifications can be replaced by subword quantifications).

There are two natural ways to attempt to generalize variation I. One way is to remove, or to weaken, condition $T(y)$. The other way is to allow more general relations X in statement (5). As a matter of fact, there is a balance between these two possibilities: simply removing condition $T(y)$ is (easily seen to be) equivalent to permitting, instead, Σ_1^p-relations X. And this latter is beyond our present reach because of work in [17] showing that that entails $P \neq NP$. So, either we try to weaken (without removing) condition $T(y)$ or, else, we try to consider binary relations X with complexity falling between FO and NP. We explore the first possibility.

Definition. *A sw.q.-predicate $P(x)$ is* provably sparse *in Th-FO if,*

$$Th - FO \vdash \forall u \exists y \forall z (z \leq u \wedge P(z) \to z \subseteq^* y) \tag{9}$$

The computer scientist says that a set $S \subseteq \{0,1\}^*$ is *sparse* if there is an integer polynomial $p(n)$ such that, for every $n \in \omega$, $card\{x \in S : length(x) \leq n\} \leq p(n)$. We want to remark that a provably sparse (in Th-FO) sw.q.-predicate $P(x)$ does, indeed, define a sparse set in the standard model. This is a consequence of a Parikh type result (see, for instance, chapter V.1 of [18]), to the effect that the statement (9) implies the existence of a term $t(u)$ of the language of Th-FO such that $\forall u \exists y \leq t(u) \forall z (z \leq u \wedge P(z) \to z \subseteq^* y)$.

Let M be a model of $I\Delta_0$. We say that a set $S \subseteq M$ is *FO-sparse* if there is a provably sparse sw.q.-predicate $P(x)$ such that $S = \{x \in M : N_M \models P(x)\}$.

Theorem (variation III). *Let M be a model of $I\Delta_0 + \neg exp$ and suppose that $S \subseteq M$ is a FO-sparse set in M and that $X \subseteq M \times M$ is a binary FO-relation in M. Then, for all $a \in M$,*

$$M \models \forall x \leq a \exists y (y \in S \wedge (x,y) \in X) \to \exists z \forall x \leq a \exists y \leq z \, (x,y) \in X$$

Proof : Let $P(x)$ be the provably sparse sw.q.-predicate defining S and fix an element $\tilde{u} \in tally(N_M) \setminus M$. According to condition (9), there is $y_0 \in N_M$ such that

$$N_M \models \forall z \leq \tilde{u} (P(z) \to z \subseteq^* y_0)$$

Assume, by hypothesis, that $M \models \forall x \leq a \exists y (y \in S \wedge (x,y) \in X)$ and take an arbitrary element $u \in N_M \setminus M$ such that $u \subseteq \tilde{u}$. By the first condition on u, $N_M \models \forall x \leq_\ell a \, \exists y \leq u (P(y) \wedge F(x,y,\vec{p}))$, where F and $\vec{p}$ are, respectively, the sw.q.-formula and the parameters that define the FO-relation X. Now, the second condition on u plus the considerations on the previous paragraph yield

$$N_M \models \forall x \leq_\ell a \, \exists y \subseteq^* y_0 \, (y \leq u \wedge P(y) \wedge F(x,y,\vec{p})) \tag{10}$$

Let $b \in tally(N_M)$ such that $N_M \models \ell h(b) = a$. We can rephrase (10) by

$$N_M \models \forall v \subseteq b \, \exists y \subseteq^* y_0 \, (y \leq u \wedge P(y) \wedge F(\ell h(v), y, \vec{p})) \tag{11}$$

By an underspill argument, we may conclude that there is $u \in tally(N_M) \cap M$ for which (11), and hence (10), holds. We conclude that $M \models \forall x \leq a \exists y \leq u \, (x,y) \in X$. $\square$

We finish with the following separation result,

Theorem. *There is a sw.q.$^{\text{m}}$-formula $A(x)$ such that $I\Delta_0 \vdash \forall x A(x)$ but $Th - FO \not\vdash \forall x A(x)$.*

Proof : In order to obtain a contradition, assume that no such sw.q.$^{\mathrm{m}}$-formula exists. Take M_0 a model of $I\Delta_0+\Omega_1$ in which there is a semantic tableaux proof d of $0=1$ from $I\Delta_0+\Omega_1$. This means that $M_0 \models \exists x F(x,d)$, for a certain sw.q.-formula F. (This rests on the fact that NP-relations can be defined by formulae of the form "$\exists x \leq t(\ldots)\, A(x,\ldots)$", with A a sw.q.-formula - see [11].) Clearly, there exists a sw.q.$^{\mathrm{m}}$-formula G so that the theory Th-FO (and, *a fortiori*, $I\Delta_0+\Omega_1$) proves $\forall y(\exists x F(x,y) \leftrightarrow \exists z G(z,y))$. This is done by absorbing existential commitments into the quantifier "$\exists z$". By assumption and easy model theory, the model N_{M_0} of the theory Th-FO can be embedded into a model M_1 of $I\Delta_0$ such that sw.q.$^{\mathrm{m}}$-formulae are absolute between N_{M_0} and M_1. Moreover, we may assume that M_1 also satisfies the axiom Ω_1 (if the original model does not satisfy this axiom, consider its initial segment cofinal in N_{M_0}). Iterate this process ω-times to obtain a chain $M_0 \subseteq N_{M_0} \subseteq M_1 \subseteq N_{M_1} \subseteq \ldots$, where the $\subseteq$-signs mean that each left entry is a substructure of the right entry with respect to the modified language of Th-FO (obtained by replacing the binary $\times$-function symbol by a ternary relational graph counterpart), and that the truth of sw.q.$^{\mathrm{m}}$-formulae is preserved between the entries. Clearly $\bigcup_{n\in\omega} N_{M_n}$ is a model of Th-FO+$\{\forall x \exists y\, \ell h(y)=x\}$, i.e., it is a model of $I\Delta_0+exp$. By results of Alex Wilkie and Jeff Paris in [19], $\bigcup_{n\in\omega} N_{M_n} \models \forall x \forall y \neg F(x,y)$. Hence, by absoluteness (*via* the formula G) $M_0 \models \forall x \neg F(x,d)$. This is a contradiction. □

References

[1] Buss S.R.: *Bounded Arithmetic*, Ph.D. Dissertation, Princeton University, 1985. A revision of this thesis was published by Bibliopolis in 1986.

[2] Krajíček J.: "Exponentiation and Second Order Bounded Arithmetic", *Annals of Pure and Applied Logic* 48, pp. 261-276 (1990).

[3] Ferreira F.: "On End Extensions of Models of $\neg exp$", pre-print, CMAF 22/91, Lisboa (1991).

[4] Takeuti G.: "RSUV Isomorphisms", in Clote, P., & Krajíček, J. (eds.), *Arithmetic, Proof Theory, and Computational Complexity*, Oxford Logic Guides 23, Oxford University Press, pp. 364-386 (1993).

[5] Razborov A.: "An Equivalence between Second Order Bounded Domain Bounded Arithmetic and First Order Bounded Arithmetic", *ibidem*, pp. 247-277.

[6] Zambella, D.: *Chapters in Bounded Arithmetic & Provability Logic*, Ph.D. Dissertation, Universiteit van Amsterdam, 1994.

[7] Clote P. & Takeuti G.: "First Order Bounded Arithmetic and Small Boolean Circuit Complexity Classes", in Clote, P. & Remmel, J. (eds.), *Feasible Mathematics II*, Birkhäuser, pp. 154-218 (1995).

[8] Immerman N.: "Descriptive and Computational Complexity", in Hartmanis, J. (ed.), *Computational Complexity Theory*, AMS Short Course Lecture Notes 38, American Mathematical Society, pp. 75-91 (1989).

[9] Ajtai, M.: "Σ^1_1-formulae on Finite Structures", *Annals of Pure and Applied Logic* 24, pp. 1-24 (1983).

[10] Håstad J.: *Computational Limitations for Small Depth Circuits*, Ph.D. Dissertation, Massachussetts Institute of Technology, 1986.

[11] Ferreira F.: *Polynomial Time Computable Arithmetic and Conservative Extensions*, Ph. D. Dissertation, Pennsylvania State University, 1988.

[12] Ferreira F.: “Some Notes on Subword Quantification and Induction thereof”, to appear in *Logic and Algebra in Memory of Roberto Megari.*

[13] Kaye R.: *Models of Peano Arithmetic*, Oxford Logic Guides 15, Claredon Press, 1991.

[14] Wilkie A.J.: “Modèles nonstandard de l’arithmétique et complexité algorithmique”, in Ressayre, J. & Wilkie, A. (eds.), *Modèles non standard en arithmétique et théorie des ensembles*, Publications Mathématiques de l’Université Paris VII, vol. 22, pp. 5-45 (1987).

[15] Paris J.B. & Kirby L.A.S.: “Σ_n-collection Schema in Arithmetic”, in Macintyre, A. et al. (eds.), *Logic Coloquium 1977*, Studies in Logic and the Foundations of Mathematics, North-Holland, pp. 199-209 (1978).

[16] Wilkie A.J. & Paris J.B.: “On the Existence of End Extensions of Models of Bounded Induction”, in Fenstad, J. E. et al. (eds.), *Logic, Methodology and Philosophy of Science VIII*, Elsevier Science Publishers, pp. 143-161 (1989).

[17] Ferreira F.: “Binary Models Generated by their Tally Part”, *Archive for Mathematical Logic* 33, pp. 283-289 (1994).

[18] Hájek P. & Pudlák P.: *Metamathematics of First-Order Arithmetic*, Perspectives in Mathematical Logic, Springer-Verlag, 1993.

[19] Wilkie A.J. & Paris J.B.: “On the Scheme of Induction for Bounded Arithmetic Formulas”, *Annals of Pure and Applied Logic* 35, pp. 261-302 (1987).

Universidade de Lisboa
Departamento de Matemática
Rua Ernesto de Vasconcelos, Bloco C1, 3
1700 Lisboa
PORTUGAL
(ferferr@ptmat.lmc.fc.ul.pt)