What are the $\forall\Sigma_1^b$-consequences of T_2^1 and T_2^2?

Fernando Ferreira

Universidade de Lisboa, Portugal

Abstract

We formulate schemes (M_1) and (M_2) of the "typical" $\forall\Sigma_1^b$-sentences that are provable in T_2^1, respectively T_2^2. As an application, we reprove a recente result of Buss and Krajíček which describes witnesses for the $\forall\Sigma_1^b$-sentences provable in T_1^1 in terms of solutions to PLS-problems.

1 Introduction

In his 1985 Princeton University Doctoral Thesis, Samuel Buss introduced a series of bounded theories of arithmetic which are closely related to the Meyer-Stockmeyer complexity hierarchy. A notable example of this closeness is the following particular case of Buss' main theorem of his dissertation: if $S_2^1 \vdash \forall x \exists y A(x,y)$, with $A \in \Sigma_1^b$, then there is a $\Box_1^p$-function f, i.e., a polynomial time computable function, such that, for all $n \in \omega$, $A(n, f(n))$. This suggests the investigation of the $\forall\Sigma_1^b$-consequences of bounded theories stronger than S_2^1. For instance, what are the $\forall\Sigma_1^b$-consequences of T_2^k $(k \geq 1)$? What are, indeed, the provably total functions (with Σ_1^b-graphs) of T_2^k? Something rather trivial can be said at once. According to the so-called Parikh's theorem, if $T_2^k \vdash \forall x \exists y A(x,y)$, with $A \in \Sigma_1^b$, then there is a term $t(x)$ such that T_2^k proves $\forall x \exists y \leq t(x) A(x,y)$. In particular this sentence is true and - from this fact alone - it follows that there exists a $\Box_2^p$-function f such that, for all $n \in \omega$, $A(n, f(n))$. However, this information comes solely from the truth of the sentence $\forall x \exists y \leq t(x) A(x,y)$, and totally neglects its provability in T_2^k.

We do not adress directly the question of characterizing the provably total functions (with Σ_1^b-graphs) of T_2^k. This we were not able to do. We rather adress the related issue of describing the "typical" $\forall\Sigma_1^b$-consequences of T_2^k. More precisely, we would like to formulate a *distinct* scheme (M_k) of $\forall\Sigma_1^b$-sentences such that,

I. each instance of (M_k) is provable in T_2^k, and

II. every $\forall\Sigma_1^b$-consequence of T_2^k is provable in S_2^1 plus the scheme (M_k).

We believe that this constitutes a sensible first answer to the question posed in the title of the paper. For instance, it is very clear from the form of the sentences in (M_2) that they embody stronger minimization assumptions than the sentences in (M_1). Perhaps the study of these principles (M_k) will be helpful in answering whether the relativized theories $T_2^k(\alpha)$ and $S_2^k(\alpha)$ can be separated by a $\forall\Sigma_1^b(\alpha)$-sentence (this is known to be true for $k = 1$; *vide* Buss' dissertation).

We describe a method for obtaining these schemes (M_k), and we do actually calculate the schemes (M_1) and (M_2). In the final section of the paper we show that our study of the case $k = 1$ yields a recent characterization (due to Buss and Krajíček) of the $\forall\Sigma_1^b$-consequences of T_1^1 in terms of solutions to certain complexity theoretic problems introduced by Johnson, Papadimitriou and Yannakakis.

2 Notation and main lemma

We mainly follow Buss' notation in [1], except for the few departures discussed ahead. A first departure consists in using Buss' acronym PV_1 for the first-order version of the quantifier-free theory PV_1. This first-order counterpart is a universal theory stated in a language that has function symbol for each (canonical description of a) polynomial time computable function. (Our paper [2] describes in detail a theory of this sort. However, this theory is formulated in a stringlanguage, not in the arithmetic language of Buss.) In trying to present a uniform and perspicuous treatment, we introduce the classes of $\check{\Pi}^b_k$-formulae (for $k \geq 0$). These are the bounded formulae of the form

$$\forall x_1 \leq t_1 \exists x_2 \leq t_2 \dots Q x_k \leq t_k A$$

where Q is $\forall$ if n is odd and $\exists$ if n is even, $t_1, \dots, t_k$ are terms, and A is a quantifier-free formula of the language of PV_1. The classes of $\check{\Sigma}^b_k$-formulae are defined in a dual manner. Hence, we are embedding the language of PV_1 in Buss' original language. The main fact to keep in mind is that the class $\check{\Pi}^b_0$ defines all polynomial time decidable relations, not just the sharply bounded ones. In tune with the above definition, we assume that the theories S^k_2 and T^k_2 ($k \geq 1$) are stated in the enlarged language. This is a harmless move, since all polynomial time computable functions can be "smoothly" introduced in S^1_2. In other words, these new theories are conservative extensions of the original theories S^k_2 and T^k_2. More generally, every $\square^p_k$-function can be "smoothly" introduced in S^k_2. In view of this fact (due to Buss), we will occasionally assume that the language of S^k_2 contains function symbols for the $\square^p_k$-functions, without explicitly telling so. In a nutshell, sometimes it is convenient to suppose that $PV_k \subseteq S^k_2$, where the PV_k's are the theories introduced by Krajíčeck et al. in [3] (although we really use their first-order versions). Lastly, we abbreviate a sequence of variables (or terms) $x_0, x_1, \dots, x_r$ by $\bar{x}$ and modify (abbreviate) related notation accordingly.

Lemma. *Let $k \geq 1$ and $A(x,y) \in \check{\Sigma}^b_k$. The following three statements are equivalent:*

(1) $T^k_2 \vdash \forall x \exists w A(x,w)$

(2) There are $B \in \check{\Pi}^b_{k-1}$ and $g, f, h \in \square^p_k$ such that

$$S^k_2 \vdash \forall x B(x, g(x))$$

$$S^k_2 \vdash \forall x \forall w (B(x,w) \rightarrow A(x, f(x,w)) \vee (h(x,w) < w \wedge B(x, h(x,w))))$$

(3) There is $B \in \check{\Pi}^b_{k-1}$ such that

$$PV_1 \vdash \forall x \exists w B(x,w)$$

$$PV_1 \vdash \forall x \forall w (B(x,w) \rightarrow \exists y A(x,y) \vee \exists w' < w B(x,w'))$$

Proof : Without loss of generality, we may suppose $A \in \check{\Pi}^b_{k-1}$. This supposition is admissible since two existential quantifiers can be merged into a single one by means of a pairing function *pair* which is polynomial time computable, whose decoding projections pr_0, pr_1 are also polynomial time computable and such that the code/decode relations are provable in PV_1. For later convenience, we further assume that *pair* is (provably) bijective and that $x_0 \leq w_0 \wedge x_1 \leq w_1 \rightarrow pair(x_0,x_1) \leq pair(w_0,w_1)$. Under this simplifying assumption, we show that (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1). The implication (3) $\Rightarrow$ (2) is immediate by Herbrand's theorem, since B is equivalent to an open formula of the language of PV_k and since this theory is universal (and a subtheory of S^k_2). To argue for the implication (2) $\Rightarrow$ (1) we will use the well-known characterization of the theory T^k_2 (essencially due to Buss in [1]) which states that T^k_2 is equivalent to the theory PV_1 plus the scheme of minimization for $\check{\Pi}^b_{k-1}$-formulae. We remind that this scheme consists of all (universal closures of) formulae of the type

$$\exists x A(x) \rightarrow \exists x (A(x) \wedge \forall y < x \neg A(y))$$

where A is a formula in $\check{\Pi}^b_{k-1}$, possibly with parameters. Now, suppose that (2) holds. We reason inside T^k_2. Let x be an arbitrary element. By hypothesis, $B(x, g(x))$. Using the minimization scheme, pick w such that $B(x, w) \wedge \forall w' < w \neg B(x, w')$ holds. This implies $A(x, f(x, w))$ and, therefore, that $\exists y A(x, y)$ is true.

The proof of (1) ⇒ (3) is more substantial. Following Buss [1], we reformulate the theory T^k_2 in Gentzen's sequent calculus. Occasionally, our notation for the sequent calculus differs from Buss': for instance, we use the colon - instead of the arrow - to separate the cedents in a sequent, and we reserve the arrow for the implication sign (instead of Buss' horseshoe). Moreover, to simplify the reading process, we systematically use the standard abbreviation $<$. The sequent calculus for T^k_2 treats bounded quantification as a syntactic operation in its own right (as opposed to an abbreviation), and Buss listed in his thesis twenty two structural and logical inferences for this "bounded" logic. The sequent calculus reformulation of T^k_2 has, also, the cut inferences

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

and the so-called MIN-inferences

$$\frac{\Gamma, A(x) \ : \ \Delta, \exists x' < x A(x')}{\Gamma, A(t) \ : \ \Delta}$$

where $A \in \check{\Pi}^b_{k-1}$, t is any term and x is an eigenvariable that does not appear in the lower sequent.

The initial sequents are the logical ones, of the form $A : A$, with A atomic, plus some mathematical sequents corresponding to the axioms of the universal theory PV_1. The main observation to make is that the initial sequents contain only quantifier-free formulae.

This sequent calculus is equivalent to the theory T^k_2 in the usual sense, i.e, $T^k_2 \vdash A$ if, and only if, the sequent $:A$ is derivable in the calculus. The only significant thing to show in this respect is that the minimization scheme is derivable in the sequent calculus. In fact,

$$\begin{array}{rcl}
\dfrac{\cdots}{A(z) \ : \ A(z)} & & \dfrac{\cdots}{\exists y < z A(y) \ : \ \exists y < z A(y)} \\
\hline
A(z) \to \exists y < z A(y), A(z) & : & \exists y < z A(y) \\
\hline
\forall x (A(x) \to \exists y < x A(y)), A(z) & : & \exists y < z A(y) \\
\hline
\forall x (A(x) \to \exists y < x A(y)), A(z) & : & \\
\hline
A(z) & : & \neg \forall x (A(x) \to \exists y < x A(y)) \\
\hline
\cdots & & \cdots \\
\hline
A(z) & : & \exists x (A(x) \wedge \forall y < x \neg A(y)) \\
\hline
\exists x A(x) & : & \exists x (A(x) \wedge \forall y < x \neg A(y)) \\
\hline
 & : & \exists x A(x) \to \exists x (A(x) \wedge \forall y < x \neg A(y))
\end{array}$$

Now, suppose that $T^k_2 \vdash \forall x \exists y A(x, y)$, where $A \in \check{\Pi}^b_{k-1}$. Then, the sequent $: \exists y A(x, y)$ is derivable in the above sequent calculus. By Gentzens cut elimination theorem, adapted to our setting, there is a so-called free-cut free derivation (see Buss [1]) of this sequent. Hence, there is a (tree) derivation of $: \exists y A(x, y)$ such that all sequents (nodes) $\Gamma : \Delta$ that occur in the (tree) derivation consist only of formulae of the type $\exists \check{\Pi}^b_{k-1}$. By logic alone, write the conjunction of Γ as $\exists \bar{u} T(\bar{p}, \bar{u})$, with T a conjunction of $\check{\Pi}^b_{k-1}$-formulae, and write the disjunction of Δ as $\exists \bar{v} D(\bar{p}, \bar{v})$, with D a disjunction of $\check{\Pi}^b_{k-1}$-formulae. We claim that there is $B(\bar{p}, \bar{u}, w) \in \check{\Pi}^b_{k-1}$ satisfying the following two conditions:

$$PV_1 \vdash \forall \bar{p} \forall \bar{u} (T(\bar{p}, \bar{u}) \to \exists w B(\bar{p}, \bar{u}, w))$$

$$PV_1 \vdash \forall \bar{p} \forall \bar{u} \forall w (B(\bar{p}, \bar{u}, w) \wedge T(\bar{p}, \bar{u}) \to \exists \bar{y} D(\bar{p}, \bar{y}) \vee \exists w' < w B(\bar{p}, \bar{u}, w'))$$

The case when $\Gamma : \Delta$ is the root of the tree derivation gives the desired conclusion. We prove the claim by induction on the length of the largest branch in the tree derivation above the node $\Gamma : \Delta$. When this length is zero we are at a top node, i.e., at an axiom, and hence there is really nothing to prove since these nodes consist only of quantifier-free formulae. The structural inferences pose no trouble. The propositional inferences may solely apply to quantifier-free formulae and thus are easy to deal with. Concerning the quantifier inferences, we illustrate the most complex case, namely the inference $\forall \leq: right$ (or, dually, $\exists \leq: left$):

$$\frac{x \leq t, \Gamma \quad : \quad \Delta, A(x)}{\Gamma \quad : \quad \Delta, \forall z \leq t A(z)}$$

where x is a variable that does not appear in the lower sequent. Recall that every formulae of the tree derivation is of the form $\exists \check{\Pi}^b_{k-1}$. In particular, $\forall z \leq t A(z)$ must be in $\check{\Pi}^b_{k-1}$. Thus, $A \in \check{\Sigma}^b_{k-2}$. By induction hypothesis, there is $B' \in \check{\Pi}^b_{k-1}$ such that the theory PV_1 proves both

$$\forall \bar{p} \forall x \forall \bar{u} (x \leq t(\bar{p}) \wedge T(\bar{p}, \bar{u}) \rightarrow \exists w B'(\bar{p}, x, \bar{u}, w))$$

$$\forall \bar{p} \forall x \forall \bar{u} \forall w (B'(\bar{p}, x, \bar{u}, w) \wedge x \leq t(\bar{p}) \wedge T(\bar{p}, \bar{u}) \rightarrow \exists \bar{y} D(\bar{p}, y) \vee A(x, \bar{p}) \vee \exists w' < w B'(\bar{p}, x, \bar{u}, w'))$$

Let $B(\bar{p}, \bar{u}, w)$ be the following $\check{\Pi}^b_{k-1}$-formula:

$$(B'(\bar{p}, 0, \bar{u}, w) \wedge \forall z \leq t(\bar{p}) A(z, \bar{p})) \vee (B'(\bar{p}, pr_0(w), \bar{u}, pr_1(w)) \wedge pr_0(w) \leq t(\bar{p}) \wedge \neg A(pr_0(w), \bar{p}))$$

Strictly speaking this is not a $\check{\Pi}^b_{k-1}$-formula, although it is clearly equivalent to such one in the theory PV_1. (In the sequel, we often abuse the language in this way.) It is straightforward to see that the formula B satisfies the two required conditions associated with the lower sequent of the inference $\forall \leq: right$.

There remains to check the cut-inferences and the MIN-inferences. Let us first consider the cut case. Suppose $A(\bar{p})$ is $\exists s Q(\bar{p}, s)$, with $Q \in \check{\Pi}^b_{k-1}$. By induction hypothesis there is $B_0 \in \check{\Pi}^b_{k-1}$ such that

$$PV_1 \vdash \forall \bar{p} \forall \bar{u} \forall s (T(\bar{p}, \bar{u}) \wedge Q(\bar{p}, s) \rightarrow \exists w B_0(\bar{p}, \bar{u}, s, w))$$

$$PV_1 \vdash \forall \bar{p} \forall \bar{u} \forall s \forall w (B_0(\bar{p}, \bar{u}, s, w) \wedge T(\bar{p}, \bar{u}) \wedge Q(\bar{p}, s) \rightarrow \exists \bar{y} D(\bar{p}, \bar{y}) \vee \exists w' < w B_0(\bar{p}, \bar{u}, s, w'))$$

and there is $B_1 \in \check{\Pi}^b_{k-1}$ such that

$$PV_1 \vdash \forall \bar{p} \forall \bar{u} (T(\bar{p}, \bar{u}) \rightarrow \exists w B_1(\bar{p}, \bar{u}, w))$$

$$PV_1 \vdash \forall \bar{p} \forall \bar{u} \forall w (B_1(\bar{p}, \bar{u}, w) \wedge T(\bar{p}, \bar{u}) \rightarrow \exists \bar{y} D(\bar{p}, \bar{y}) \vee \exists s Q(\bar{p}, s) \vee \exists w' < w B_1(\bar{p}, \bar{u}, w'))$$

Using thrice a well-known result of Parikh (see, for instance, [1]), there are terms $t(\bar{p}, \bar{u})$, $q(\bar{p}, \bar{u})$ and $r(\bar{p}, \bar{u})$ of the language of PV_1 such that the theory PV_1 proves

$$\forall \bar{p} \forall \bar{u} (T(\bar{p}, \bar{u}) \rightarrow \exists w \leq t(\bar{p}, \bar{u}) B_1(\bar{p}, \bar{u}, w))$$

$$\forall \bar{p} \forall \bar{u} \forall w \leq t(\bar{p}, \bar{u}) (B_1(\bar{p}, \bar{u}, w) \wedge T(\bar{p}, \bar{u}) \rightarrow \exists \bar{y} D(\bar{p}, \bar{y}) \vee \exists s \leq q(\bar{p}, \bar{u}) Q(\bar{p}, s) \vee \exists w' < w B_1(\bar{p}, \bar{u}, w'))$$

$$\forall \bar{p} \forall \bar{u} \forall s \leq q(\bar{p}, \bar{u}) (T(\bar{p}, \bar{u}) \wedge Q(\bar{p}, s) \rightarrow \exists w \leq r(\bar{p}, \bar{u}) B_0(\bar{p}, \bar{u}, s, w))$$

Define $B(\bar{p}, \bar{u}, w)$ as the disjunction

$$(pr_0(w) \geq r(\bar{p}, \bar{u}) \wedge B_1(\bar{p}, \bar{u}, pr_0(w) - r(\bar{p}, \bar{u})) \wedge pr_1(w) = 1 + q(\bar{p}, \bar{u})) \vee$$

$$\vee (pr_0(w) \leq r(\bar{p}, \bar{u}) \wedge pr_1(w) \leq q(\bar{p}, \bar{u}) \wedge B_0(\bar{p}, \bar{u}, pr_1(w), pr_0(w)) \wedge Q(\bar{p}, pr_1(w)))$$

Firstly, we show that B, as defined above, satisfies the first condition. We reason inside PV_1. Assume $T(\bar{p}, \bar{u})$, and take $a \leq t(\bar{p}, \bar{u})$ such that $B_1(\bar{p}, \bar{u}, a)$ is true. Let w_0 be $a + r(\bar{p}, \bar{u})$ and let w_1 be $1 + q(\bar{p}, \bar{u})$. It is clear that $B(\bar{p}, \bar{u}, c)$ holds, where $c = pair(w_0, w_1)$, since the first disjunct of B becomes true. In order to verify the second condition, assume $B(\bar{p}, \bar{u}, w) \wedge T(\bar{p}, \bar{u})$. If the second disjunct of $B(\bar{p}, \bar{u}, w)$ holds, the matter is easy. Alternatively, the first disjunct is valid. We may assume, without loss of generality, that $pr_0(w) - r(\bar{p}, \bar{u}) \leq t(\bar{p}, \bar{u})$ is true. (In fact, if $pr(w_0) - r(\bar{p}, \bar{u}) > a$, then $B(\bar{p}, \bar{u}, c)$ and $c < w$.) There are two cases to consider. The case when $\forall s \leq q(\bar{p}, \bar{u}) \neg Q(\bar{p}, \bar{s})$ is straightforward. Otherwise, take $w_1 \leq q(\bar{p}, \bar{u})$ such that $Q(\bar{p}, w_1)$ holds, and pick $w_0 \leq r(\bar{p}, \bar{u})$ such that $B_0(\bar{p}, \bar{u}, w_1, w_0)$ is true. Note that $pair(w_0, w_1) < w$, since $w_0 \leq r(\bar{p}, \bar{u}) \leq pr_0(w)$ and $w_1 \leq q(\bar{p}, \bar{u}) < pr_1(w)$. By construction, the second disjunct of $B(\bar{p}, \bar{u}, pair(w_0, w_1))$ is true.

Let us finally consider the MIN-inferences. By induction hypothesis, there is $B' \in \check{\Pi}^b_{k-1}$ such that the theory PV_1 proves both

$$\forall \bar{p} \forall x \forall \bar{u} (T(\bar{p}, \bar{u}) \wedge A(\bar{p}, x) \rightarrow \exists w B'(\bar{p}, x, \bar{u}, w))$$

$$\forall \bar{p} \forall x \forall \bar{u} \forall w (B'(\bar{p}, x, \bar{u}, w) \wedge T(\bar{p}, \bar{u}) \wedge A(\bar{p}, x) \rightarrow \exists \bar{y} D(\bar{p}, \bar{y}) \vee \exists x' < x A(\bar{p}, x') \vee \exists w' < w B'(\bar{p}, x, \bar{u}, w'))$$

By a previous remark, the result of Parikh guarantees that there is a term d such that

$$PV_1 \vdash \forall \bar{p} \forall x \leq t(\bar{p}) \forall \bar{u} (T(\bar{p}, \bar{u}) \wedge A(\bar{p}, x) \rightarrow \exists w < d(\bar{p}, \bar{u}) B'(\bar{p}, x, \bar{u}, w))$$

Let $B(\bar{p}, \bar{u}, w)$ be the following $\check{\Pi}^b_{k-1}$-formula:

$$B'(\bar{p}, qt(w; d(\bar{p}, \bar{u})), \bar{u}, rm(w; d(\bar{p}, \bar{u}))) \wedge qt(w; d(\bar{p}, \bar{u})) \leq t(\bar{p}) \wedge A(\bar{p}, qt(w; d(\bar{p}, \bar{u})))$$

where $qt(w; d(\bar{p}, \bar{u}))$ and $rm(w; d(\bar{p}, \bar{u}))$ are, respectively, the quotient and the remainder of the dividion of w by $d(\bar{p}, \bar{u})$. In other words: $w = qt(w; d(\bar{p}, \bar{u}))d(\bar{p}, \bar{u}) + rm(w; d(\bar{p}, \bar{u}))$, where $rm(w; d(\bar{p}, \bar{u})) < d(\bar{p}, \bar{u})$. We show that B, as defined above, satisfies the two required conditions to keep the induction going. In order to check the first condition, assume $T(\bar{p}, \bar{u}) \wedge A(\bar{p}, t(\bar{p}))$. Then, there exists $a < d(\bar{p}, \bar{u})$ such that $B'(\bar{p}, t(\bar{p}), \bar{u}, a)$ holds. Clearly, $B(\bar{p}, \bar{u}, c)$, where $c = t(\bar{p})d(\bar{p}, \bar{u}) + a$. Let us now argue for the validity of the second condition. Assume $B(\bar{p}, \bar{u}, w) \wedge T(\bar{p}, \bar{u}) \wedge A(\bar{p}, t(\bar{p}))$. In particular, $B'(\bar{p}, qt(w; d(\bar{p}, \bar{u})), \bar{u}, rm(w; d(\bar{p}, \bar{u})))$ and $A(\bar{p}, qt(w; d(\bar{p}, \bar{u})))$. There are two cases to consider. If there is $w_0 < qt(w; d(\bar{p}, \bar{u}))$ such that $A(\bar{p}, w_0)$ is true, pick $w_1 < d(\bar{p}, \bar{u})$ satisfying $B'(\bar{p}, w_0, \bar{u}, w_1)$. We get $B(\bar{p}, \bar{u}, w')$, where $w' = w_0 d(\bar{p}, \bar{u}) + w_1 < w$. The second case takes place when there exists $w_1 < rm(w; d(\bar{p}, \bar{u}))$ such that $B'(\bar{p}, qt(w; d(\bar{p}, \bar{u})), \bar{u}, w_1)$ holds. In this situation, we conclude $B(\bar{p}, \bar{u}, w')$, where $w' = qt(w; d(\bar{p}, \bar{u}))d(\bar{p}, \bar{u}) + w_1 < w$. □

Notice that the lemma is also true for $A \in \Sigma^b_k$. In effect, it is well known that the theory S^k_2, and *a fortiori* the theory T^k_2, proves the Σ^b_k-replacement axioms. This entails that every Σ^b_k-formula A is equivalent to a $\check{\Sigma}^b_k$-formula $\check{A}$ in T^k_2. Furthermore, the theory PV_1 proves the implication "$\check{A} \rightarrow A$". The claim follows.

3 The cases T^1_2 and T^2_2

In the introduction we posed the question of characterizing the $\forall\Sigma^b_1$-consequences of T^k_2, and we proposed that a sensible first answer would be to perspicuously describe a collection of $\forall\Sigma^b_1$-sentences that, together with the theory PV_1, forms the $\forall\Sigma^b_1$-theory of T^k_2. The main lemma of the previous section suggests a way of tackling this question. The key idea can be briefly described. Suppose that $T^k_2 \vdash \forall x \exists y A(x, y)$, where $A \in \Sigma^b_1$. Part 3 of the main lemma guarantees the existence of $B \in \check{\Pi}^b_{k-1}$ such that the theory PV_1 proves both $\forall x \exists w B(x, w)$ and

$$\forall x \forall w (B(x, w) \rightarrow \exists y A(x, y) \vee \exists w' < w B(x, w'))$$

By Herbrand analysis, we know that $PV_1 \vdash H$, where H is the quantifier-free Herbrand normal form of the above statement (we mean by H the Herbrand normal form which is stated in the *same* language). The final step consists in trying to extract from the particular form of H a $\forall\Sigma_1^b$-condition (provable in T_2^1) which entails the sentence $\forall x \exists y A(x, y)$ in the theory PV_1. This strategy is perfectly general, but we will only effect an *ad-hoc* study for the cases of the theories T_2^1 and T_2^2. We believe that the general case should yield to the above method, although this surely must involve careful work and the introduction of some intelligent definitions.

Proposition. *The following $\forall\Sigma_1^b$-scheme is provable in T_2^1:*

$$(M_1) \qquad \forall x \forall u(B(x, u) \to \exists w \leq u(B(x, w) \land (h(x, w) < w \to \neg B(x, h(x, w)))))$$

where $B \in \check{\Pi}_0^b$ and $h \in \square_1^p$.

Moreover, all the $\forall\Sigma_1^b$-consequences of T_2^1 are provable in PV_1 plus the above scheme.

Proof : (M_1) is obviously a consequence of the $\check{\Pi}_0^b$-minimization scheme. Suppose, now, that $T_2^1 \vdash \forall x \exists y A(x, y)$, with $A \in \check{\Pi}_0^b$ (it is clear that this latter assumption does not represent a loss of generality). By part 3 of the main lemma, and by Herbrand analysis, there are $B \in \check{\Pi}_0^b$ and $g, f, h \in \square_1^p$ such that

$$(*) \qquad PV_1 \vdash \forall x B(x, g(x))$$

$$(**) \qquad PV_1 \vdash \forall x \forall w(B(x, w) \to A(x, f(x, w)) \lor (h(x, w) < w \land B(x, h(x, w))))$$

We reason inside PV_1. Take any x. By $(*)$, $B(x, g(x))$ is true. Thus, according to (M_1), there is w such that $B(x, w) \land (h(x, w) < w \to \neg B(x, h(x, w)))$ is true. This entails $A(x, f(x, w))$. So, $\exists y A(x, y)$. □

A comment by the anonymous referee suggested to me a particularly elegant reformulation of the above proposition:

Proposition (ameliorated version). *The following $\forall\Sigma_1^b$-scheme is provable in T_2^1:*

$$\forall x \forall u(g(x, u) < u \to \exists w \leq u(g(x, w) < w \land g(x, g(x, w)) \geq g(x, w)))$$

where $g \in \square_1^p$.

Moreover, all the $\forall\Sigma_1^b$-consequences of T_2^1 are provable in PV_1 plus the above scheme.

Proof : (M_1) is obviously a consequence of the $\check{\Pi}_0^b$-minimization scheme. Conversely, we show that the above scheme entails, within PV_1, the scheme (M_1). By the previous lemma, this suffices for concluding the proof of the proposition.

Let $B \in \check{\Pi}_0^b$, $h \in \square_1^p$, and define

$$g(x, u) = \begin{cases} h(x, u) & \text{if } B(x, u) \land B(x, h(x, u)) \\ u & \text{otherwise} \end{cases}$$

It is clear that $g \in \square_1^p$. We reason inside PV_1. Assume that $B(x, u)$ holds. If $g(x, u) \geq u$, then (M_1) is true with $w = u$. Otherwise, according to (M_1), there is $w' \leq u$ such that,

$$g(x, w') < w' \land g(x, g(x, w')) \geq g(x, w')$$

In this case, (M_1) is true with $w = g(x, w')$. □

Proposition. *The following $\forall\Sigma_1^b$-scheme is provable in T_2^2:*

$$(M_2') \qquad \forall x \forall u \{\forall z B(x,u,z) \to \exists w \leq u \exists z_0 \exists z_1 \ldots \exists z_n \bigwedge_{i=0}^{n} [B(x,w,k_i(x,w,z_0,z_1,\ldots,z_{i-1})) \wedge$$

$$\wedge (h_i(x,w,z_0,z_1,\ldots,z_{i-1}) < w \to \neg B(x,h_i(x,w,z_0,z_1,\ldots,z_{i-1}),z_i))]\}$$

where $B(x,u,z)$ is of the form "$z \leq t(x,u) \to C(x,u,z)$", with t a term of the language of PV_1, $C \in \check{\Pi}_0^b$, and where both $(i+2)$-ary functions k_i, h_i $(0 \leq i \leq n)$ are in $\Box_1^p$.

Moreover, all the $\forall\Sigma_1^b$-consequences of T_2^2 are provable in PV_1 plus the above scheme.

Proof : It is not difficult to argue that (M_2') is provable in the theory T_2^2: the crucial step consists in using the $\check{\Pi}_1^b$-minimization scheme to pick the least w such that $\forall z B(x,w,z)$. Suppose, now, that $T_2^2 \vdash \forall x \exists y A(x,y)$, with $A \in \check{\Pi}_0^b$. By part 3 of the main lemma, there is $B' \in \check{\Pi}_1^b$ such that $PV_1 \vdash \forall x \exists w B'(x,w)$ and

$$PV_1 \vdash \forall x \forall w (B'(x,w) \to \exists y A(x,y) \vee \exists w' < w B'(x,w'))$$

Write $B'(x,w)$ as $\forall z B(x,w,z)$, where $B(x,w,z)$ is $z \leq t(x,w) \to C(x,w,z)$ for a certain term t of the language of PV_1, and a certain $C \in \check{\Pi}_0^b$. Using this new notation, we can rewrite the above condition as

$$PV_1 \vdash \forall x \forall w \exists z \exists y \exists w' \forall z' (B(x,w,z) \to A(x,y) \vee (w' < w \wedge B(x,w',z')))$$

By Herbrand analysis (or, if the reader feels more sympathetic towards model theory, by a simple compactness argument as in the second proof of theorem A in [3]), there are $\Box_1^p$-functions $k_0,\ldots,k_n,f_0,\ldots,f_n,h_0,\ldots,h_n$ such that the theory PV_1 proves the following sentence:

$$\forall x \forall w \forall z_0 \ldots \forall z_n \bigvee_{i=0}^{n} [B(x,w,k_i(x,w,z_0,\ldots,z_{i-1})) \to A(x,f_i(x,w,z_0,\ldots,z_{i-1})) \vee$$

$$\vee (h_i(x,w,z_0,\ldots,z_{i-1}) < w \wedge B(x,h_i(x,w,z_0,\ldots,z_{i-1}),z_i))]$$

We reason inside PV_1. Take any x, and pick u such that $\forall z B(x,u,z)$ holds. Then, according to (M_2'), there are $w, z_0, \ldots, z_n$ such that, for all $0 \leq i \leq n$,

$$B(x,w,k_i(x,w,z_0,\ldots,z_{i-1})) \wedge (h_i(x,w,z_0,,\ldots,z_{i-1}) < w \to \neg B(x,h_1(x,w,z_0,,\ldots,z_{i-1}),z_i))$$

This entails $\bigvee_{i=0}^{n} A(x,f_i(x,w,z_0,\ldots,z_{i-1}))$. So, $\exists y A(x,y)$. □

It would be interesting to find an amelioration of the above proposition in the vein of the case T_1^1.

4 Digression on PLS-problems

The concept of a *polynomial local search* problem (a PLS-problem, for short) was introduced in [4]. The next definition follows closely the presentation of Buss and Krajíček in [5].

Definition. *A PLS-problem L consists of a family $F_L(x)$ of subsets of ω (one for each $x \in \omega$, called the set of* solutions *of the instance x of L), and functions $c_L(s,x)$ and $N_L(s,x)$, called (resp.) the* cost function *and the* neighborhood function, *such that:*

i. the binary predicate $s \in F_L(x)$ and the functions $c_L(s,x)$ and $N_L(s,x)$ are polynomial time computable;

ii. there is a polynomial p_L such that, for all $s \in F_L(x)$, $|s| \leq p_L(|x|)$;

iii. for all $s \in \omega$, $N_L(s,x) \in F_L(x)$;

iv. for all $s \in F_L(x)$, if $N_L(s,x) \neq s$ then $c_L(s,x) < c_L(N_L(s,x),x)$.

An optimal solution *of the instance x of the problem L is a natural number s such that $N_L(s,x) = s$.*

It is clear that a PLS-problem can be expressed by a $\forall\check{\Pi}_0^b$-sentence. If this sentence is provable in PV_1, then we say that L is a PLS-problem in PV_1. The formula $Opt(s,x)$ is the $\check{\Pi}_0^b$-formula $N_L(s,x) = s$. The following result is an inessential variation of a theorem at the end of [5].

Proposition. (Buss and Krajíček) *Suppose that $T_2^1 \vdash \forall x \exists y A(x,y)$, with $A \in \check{\Pi}_0^b$. Then there is a PLS-problem L in PV_1, and there is a polynomial time computable function f such that*

$$PV_1 \vdash \forall x \forall s (Opt_L(x,s) \rightarrow A(x, f(x,s)))$$

Proof : As we have pointed out in the proof of the first lemma of the previous section, there are $B \in \check{\Pi}_0^b$ and $g, f, h \in \square_1^p$ which satisfy both $(*)$ and $(**)$. Define,

$$F_L(x) = \{s : s \leq g(x) \wedge B(x,s)\}$$

$$N_L(x,s) = \begin{cases} g(x) & \text{if } s \notin F_L(x) \\ h(x,s) & \text{if } s \in F_L(x) \wedge \neg A(x, f(x,s)) \\ s & \text{if } s \in F_L(x) \wedge A(x, f(x,s)) \end{cases}$$

$$c_L(s,x) = g(x) \dot{-} s$$

where $\dot{-}$ is the modified subtraction. This defines a PLS-problem in PV_1 that satisfies the conclusion of the proposition. □

References

1. Buss, S.: *Bounded Arithmetic.* Napoli : Bibliopolis, 1986. Revision of a 1985 Princeton University Doctoral Thesis.

2. Ferreira, F.: *Polynomial Time Computable Arithmetic.* In: Sieg, W. (ed.) Contemporary Mathematics (pp. 137-156). American Mathematical Society, 1990.

3. Krajíček, J., Pudlák, P., Takeuti, G.: *Bounded Arithmetic and the Polynomial Hierarchy.* Annals of Pure and Applied Logic 52, pp. 143-153 (1991).

4. Johnson, D., Papadimitriou, C., Yannakakis, M.: *How Easy is Local Search?* Journal of Computer Systems Science 37, pp. 79-100 (1988).

5. Buss, S., Krajíček, J.: *An Application of Boolean Complexity to Separation Problems in Bounded Arithmetic.* Proceedings of the London Mathematical Society 69, pp. 1-21 (1994).

Universidade de Lisboa
Departamento de Matemática
Rua Ernesto de Vasconcelos, Bloco C1, 3
1700 Lisboa
PORTUGAL

(ferferr@lmc.fc.ul.pt)