Delineating Classes of Computational Complexity via Second Order Theories with Weak Set Existence Principles (I)

by

Aleksandar Ignjatović

February 1994

Report CMU-PHIL-49

Carnegie Mellon

Philosophy
Methodology
Logic

Pittsburgh, Pennsylvania 15213-3890

Delineating Classes of Computational Complexity via Second Order Theories with Weak Set Existence Principles (I)*

Revised Version

Aleksandar Ignjatović

December 27, 1993

Abstract

In this paper we characterize the well-known computational complexity classes of the polynomial time hierarchy as classes of provably recursive functions (with graphs of suitable bounded complexity) of some second order theories with weak comprehension axiom schemas but without any induction schemas (Theorem 6). We also find a natural relationship between our theories and the theories of bounded arithmetic *S*? (Lemmas 4 and 5). Our proofs use a technique which enables us to "speed up" induction without increasing the bounded complexity of the induction formulas. This technique is also used to obtain an interpretability result for the theories of bounded arithmetic 5^ (Theorem 4).

1. **Introductory** remarks

Our work is motivated by Daniel Leivant's pioneering work in introducing polynomial time computable functions in theories with the comprehension schema for quantifier-free *positive* formulas, presented in [11]. Leivant uses new function symbols and Herbrand - Gődel equations to represent algorithms. We take a different approach which enables us to obtain easily characterizations for a broader collection of computational complexity classes (Theorem 6) and to relate very naturally the theories we introduce to the theories of bounded arithmetic 5^ (Lemmas 4 and 5). This is accomplished by using theories which contain comprehension schemas for formulas with limited quantifier complexity but with no limitation on the logical connectives used in these formulas, and by treating algorithms as partial recursive functions with suitably definable graphs. Such representation of algorithms is along the lines of the usual method of approaching the problem of determining the class of provably recursive functions of a theory. For the purpose of delineating various computational complexity classes our formalism has some advantages over the original one

* This paper is dedicated to Alan G. Mallinger, M.D., Associate Professor of Pharmacology at the University of Pittsburgh Medical School, who enabled me to work and enjoy life again. The content of the first three sections of this paper was presented in the technical report [8].

used by Leivant, since it allows us to delimit easily every level of the polynomial time hierarchy, and to relate in a straight forward way the theories we introduce to the theories of bounded arithmetic S$\dot{\wedge}$. On the other hand, Leivant's original approach has initiated important research in the treatment of polynomial time computability by means of recursion theory and A-calculus.

In this paper we deal with second order theories of binary strings; the notation and definitions which we do not introduce ourselves are from Buss's [1], Cook's [3], Ferreira's [5] and Leivant's [11]. We first specify the languages of our theories.

The first order language with equality L^b includes two binary relation symbols *x* C *y* and *x* =^ *y* with the intended meanings "x is an initial segment of y" and "the length of x is smaller or equal than the length of y" respectively, as well as the constant symbol *e* denoting the empty string. The function symbols of L^b are: *S°(x)* and $S^l(x)$ for the two successor functions which "concatenate 0 and 1" respectively to the end of a string*, *x* 0 *y* for the function which concatenates the string *y* to the string *x*, *x* 0 *y* for the function which concatenates the string *x* to itself length of *y* many times and the symbol *x* \ *y* for the function which, if *y* -< x, produces the initial substring of the string *x* of length equal to the length of the string t/, or just the string *x* if *x* ^ *y*. The symbols in L^b we call *basic symbols.* We denote the term *S°(S°(. ..S°(e)...))* with m iterations of *S°(x)* by m and the term *w* 0 *(w* 0 … *(w* 0 *w)* • • •) with m iterations of 0 by w^m .

The language \J\ is a two sorted language; the first order variables of L| range over binary strings while the second order variables range over sets of binary strings.[2] The only symbol of a mixed sort is the membership relation E. The language L| also contains all symbols of the language L^b for the first order part. In particular, the equality is also restricted to strings only; we *do not* have the equality symbol for the sets of strings. These are all symbols of L^; thus, the only atomic formulas of this language which involve the second order variables are of the form $t(\vec{x})$ E *X*, where $t(\vec{x})$ is a term of the language L^b.

The language L| is sufficient to formulate a theory which can be easily "bootstrapped", i.e. a theory in which one can prove the basic properties of a few basic definable predicates and functions, and in which one can introduce (by suitable definitions) all other polynomial time computable functions, providing that the

[1] We do not have symbols for 0 and 1 in our language, but only the symbols for the corresponding successor functions.

[2] The presence of boldface letters in the notation for a notion indicates that this notion involves second order objects. When working with a model of a theory whose language contains second order variables for sets of strings, we will sometimes use "real" sets of strings rather than just elements of the second order part of the domain of the model. Thus, such objects do not have to be coextensional with any "internal" sets of the model. To stress this fact, we will usually call such sets collections or classes of elements.

comprehension schema is sufficiently strong. Roughly speaking, such a comprehension schema corresponds in strength to the induction schema of Buss's S^1_2 in the context of the theories of bounded arithmetic. However, for the purpose of a proof-theoretic analysis of our theories (see [10]), it is important for us to consider some theories which do not have a comprehension schema of such strength. Thus, we will also consider theories formulated in languages which are obtained by extending the languages $\mathbf{L}^b_2$ and L^b by adding a set of new function symbols. Two examples of such languages are $\mathbf{L}^p_2$ and L^p obtained from the languages $\mathbf{L}^b_2$ and L^b respectively by adding a (purely first order) function symbol for every polynomial time computable function; for the purpose of a Herbrand style proof-theoretic analysis of theories with weak set existence principles, as presented in [10], one further extends these languages by addition of new function symbols of mixed types.

Definition 1 *Let $\mathbf{L}$ be a language extending the language $\mathbf{L}^b_2$ and L a language extending the language L^b.*

1. *The set of sharply bounded formulas, or $\mathbf{\Sigma^b_0}$ formulas (Σ^b_0 formulas), of the language $\mathbf{L}$ (L) is the least closure of the set of atomic formulas of $\mathbf{L}$ (L) for Boolean connectives and sharply bounded first order quantifiers $\forall x \subseteq t$ and $\exists x \subseteq t$, where t is an arbitrary term of the language $\mathbf{L}$ (L).*
2. *The set of bounded formulas of the language $\mathbf{L}$ (L) is the least closure of the set of atomic formulas of $\mathbf{L}$ (L) for Boolean connectives, sharply bounded quantifiers and bounded first order quantifiers $\forall x \preccurlyeq t$ and $\exists x \preccurlyeq t$.*

Notice that by the above definition no second order quantifiers are allowed in sharply bounded or bounded formulas of the language $\mathbf{L}$, but such formulas can contain second order free variables, since the set of atomic formulas of $\mathbf{L}$ also includes second order atomic formulas. In the case of $\mathbf{L}^p_2$ or $\mathbf{L}^b_2$, the only second order atomic formulas are of the form $t(\vec{x}) \in X$ where $t(\vec{x})$ is a purely first order term. It is easy to see that if a formula φ is a Σ^b_0 formula of the languages L^b or L^p, then it defines a predicate which is decidable by a polynomial-time Turing machine, while $\mathbf{\Sigma^b_0}$ formulas of the languages $\mathbf{L}^b_2$ and $\mathbf{L}^p_2$ define predicates which are decidable by polynomial time Turing machines with the oracles for the set parameters involved (see [4] for the details). We can now define our base theory $\mathbf{C}^b$ and its extension $\mathbf{C}^p$.

2. Theories $\mathbf{C}^b$ and $\mathbf{C}^p$

We will not attempt to find the weakest possible base theory which allows us to prove that the basic predicates we define have the properties needed to carry out our constructions. Rather, we choose a theory (to be denoted by $\mathbf{C}^b$) which allows an elegant development of the basic tools. The main axioms of our second order theories of binary strings with weak set existence principles are comprehension axioms. If Φ is a class of formulas of a language $\mathbf{L}$, then the Φ-comprehension axiom schema consists of axioms

$$(\Phi - \mathbf{CA:}) \qquad (\forall \vec{y})(\forall \vec{Y})(\exists X)(\forall x)(x \in X \leftrightarrow \varphi(x, \vec{y}, \vec{Y})),$$

where φ is an arbitrary formula of the class Φ not containing variable X.

We recall that a function $f(\vec{x}, y)$, mapping sequences of binary strings into binary strings, is defined by *limited recursion* from functions $g(\vec{x}), h_0(\vec{x}, y, z), h_1(\vec{x}, y, z)$ and $k(\vec{x}, y)$ if:

$$\begin{aligned} f(\vec{x}, \epsilon) &= g(\vec{x}) \\ f(\vec{x}, S^0(y)) &= h_0(\vec{x}, y, f(\vec{x}, y)) \restriction k(\vec{x}, y), \\ f(\vec{x}, S^1(y)) &= h_1(\vec{x}, y, f(\vec{x}, y)) \restriction k(\vec{x}, y). \end{aligned}$$

Thus, for such a function $f(\vec{x}, y)$ and all $\vec{x}$ and y, $f(\vec{x}, y) \preccurlyeq k(\vec{x}, y)$.

Definition 2 *1. Theory BASIC is a finite open first order theory of the language L^b which contains just a few axioms*[3] *expressing elementary properties of the functions and relations of L^b.*

2. Theory $BASIC^p$ is an open first order theory of the language L^p which contains all axioms of BASIC and the definitions of all polynomial time computable functions by composition and limited recursion.

3. Theory $\mathbf{C}^b$ is a theory of the language $\mathbf{L}_2^b$ which consists of the axioms of BASIC and the comprehension axiom schema for the class of Σ_0^{b} formulas of the language $\mathbf{L}_2^b$.

4. Theory $\mathbf{C}^p$ is a theory of the language $\mathbf{L}_2^p$ which consists of the axioms of $BASIC^p$ and the comprehension axiom schema for the class of Σ_0^{b} formulas of the language $\mathbf{L}_2^p$.

[3] Instead of specifying yet another finite set of simple open axioms, we leave it to the reader to see from the further arguments what axioms should be included in our base theory. Roughly, these axioms are binary string versions of Buss's induction-free fragment of bounded arithmetic *BASIC* and so we use the same notation for our system.

Definition 3 *Let $\mathcal{M}$ be a model of a theory* $\mathbf{T}$ *of a language* $\mathbf{L} \supseteq \mathbf{L}_2^b$ *such that* $\mathbf{T}$ *extends* $\mathbf{C}^b$.

1. *We denote by* $\mathbf{Str}(\mathcal{M})$ *the first order part of the universe of* $\mathcal{M}$, *while* $\mathrm{Set}(\mathcal{M})$ *stands for the second order part of the universe of* $\mathcal{M}$. *Thus,* $\mathrm{Set}(\mathcal{M})$ *is the collection of "internal" sets of* $\mathcal{M}$.

2. $\mathbf{Ind}(\mathcal{M})$ *is the collection of all elements of* $\mathrm{Set}(\mathcal{M})$ *which contain the empty string and are closed under the two successor functions, i.e. if we define*

$$Ind(U) \stackrel{df}{=} \varepsilon \in U \ \wedge \ (\forall y)\,(y \in U \ \rightarrow \ (S^0(y) \in U \ \wedge \ S^1(y) \in U))\,,$$

then $\mathbf{Ind}(\mathcal{M}) = \{U \in \mathrm{Set}(\mathcal{M}) \mid \mathcal{M} \models Ind(U)\}$. *Elements of* $\mathbf{Ind}(\mathcal{M})$ *we call inductive sets.*

3. *We denote by* $\mathbf{W}$ *the intersection of all sets from* $\mathbf{Ind}(\mathcal{M})$, *i.e. if we define*

$$W(x) \stackrel{df}{=} (\forall U)(Ind(U) \rightarrow x \in U), \tag{1}$$

then $\mathbf{W} = \{x \in \mathbf{Str}(\mathcal{M}) \mid \mathcal{M} \models W(x)\}$.

4. *A function* $h : (\mathbf{Str}(\mathcal{M}))^k \mapsto \mathbf{Str}(\mathcal{M})$ *(not necessarily an interpretation of a function symbol of the language or even definable in* $\mathcal{M}$ *at all) has polynomial growth rate if there exist natural numbers* m, n *such that for every sequence* $\vec{s} = \langle s_0, \ldots, s_k\rangle$ *of elements of* $\mathbf{Str}(\mathcal{M})$ *and every sequence* $\vec{S}$ *of elements of* $\mathrm{Set}(\mathcal{M})$ *it holds that* $h(\vec{s}, \vec{S}) \preccurlyeq (s_0 \oplus \ldots \oplus s_k)^m \oplus \underline{n}$.

5. $\mathrm{Cl}(\mathcal{M})$ *is the collection of all elements of* $\mathrm{Set}(\mathcal{M})$ *which contain the empty string* ε *and are closed for all functions* f *with polynomial growth rate. Thus,* $\mathrm{Cl}(\mathcal{M})$ *is the collection of all elements* $V \in \mathrm{Set}(\mathcal{M})$ *such that* $\varepsilon \in V$ *and such that for all* $\vec{s} \in V$, *all* $\vec{S} \in \mathrm{Set}(\mathcal{M})$ *and any function* f *with polynomial growth rate also* $f^{\mathcal{M}}(\vec{s}, \vec{S}) \in V$. *We then define*

$$\overline{\mathbf{W}} = \{x \mid (\forall X)(X \in \mathrm{Cl}(\mathcal{M}) \rightarrow x \in^{\mathcal{M}} X)\}.$$

6. $\mathcal{M}^1$ *is the first order part of the structure* $\mathcal{M}$. *Thus,* $\mathcal{M}^1$ *consists of the set* $\mathbf{Str}(\mathcal{M})$ *together with the interpretations of the purely first order symbols of the language* $\mathbf{L}$.

The class $\mathbf{W}$ is the collection of all "number-like" sequences, i.e. $\mathbf{W}$ is defined in a way analogous to the way in which the set of natural numbers is defined in, say, ZF set theory. In fact, $\mathbf{W}$ has properties analogous to the properties of the set of natural numbers. For example, from the definition of $\mathbf{W}$ it is clear that $\varepsilon \in \mathbf{W}$ and that $\mathbf{W}$ is closed for both successor functions. Moreover, we will show that $\mathbf{W}$ is an "initial segment" of the universe (Lemma 1) closed for all functions with polynomial growth rate (Lemma 2) and that induction for I)|?, formulas of the language L£ holds for elements of W. If T contains the comprehension schema for all £jj formulas of the whole language L, then the induction schema also holds for all S_g^h formulas of the language L (Theorem 1).

On the other hand, since the collection *Cl(M)* is a collection of objects closed under infinitely many functions, not necessarily themselves definable in *M*, it is not immediately clear that $\overline{W}$ is definable in *M* at all, but we show that W = $\overline{W}$ in any theory extending the theory C^h. Since *C\(M)* ⊆ Ind(Af), clearly W ⊆ $\overline{W}$; thus, we only have to prove the other inclusion. Notice also that W need not be coextensional with any element of Set(A^).

Lemma 1 *Let W(x) be as in Definition 3.3; then*

$$C^6 1\text{-}\ \mathbf{(Vz)(Vy} \wedge x)(W(x) \to W(y)).$$

Thus, W(x) defines a complete binary subtree of the complete binary tree consisting of all sequences of the ***universe.***

Proof: Assume that for two strings a, 6 we have *(b* ^ a) A *W(a)* A ~^*W(b).* This means that there exists an element *U* such that both *Ind(U)* and 6 §* *U* hold. We now use an instance of the comprehension schema to obtain the set *V* = *{x \ (By* ⊆ *b)(y eU* A *x* ^ y)}. Then clearly *e £V.* Assume *x* G V, and let *y* G *U* be such that *x* ^ *y* and *y* ⊆ 6; since 6 ^ [/, we have *y db.* Thus,

$$x \prec S^i(x) \preccurlyeq (b \restriction S^0(y)) \subseteq b\wedge a \tag{2}$$

for ĭ = 0,l- Since *y* G *U* and *Ind(U)* hold, we get that 6 \ *S°(y)* is in *U.* Consequently, both *S°(x)* and $S^1(x)$ are in *V,* which, together with *e eV,* implies *Ind(V).* On the other hand, (2) implies that for all *x* G V, *x* < *a.* Thus, *a £ V,* which contradicts our assumption that *W(a)* holds. •

In the course of the proof of the next Lemma, we develop a technique that can be quite appropriately called the "speed-up" induction method. We now briefly describe this method applied to the (more common) formalism of the theories of bounded arithmetic. Roughly speaking, given a formula <*f*> and an element *a* such that <*j*> satisfies the premise (induction hypothesis) of the L-induction axiom for the formula <*j*> up to the value *a*\, i.e. such that

$$\phi(0) \wedge \forall x \wedge < |a| . \wedge (x + 1)) \tag{3}$$

the speed-up induction method enables us to replace this formula *<j>{x)* by another formula *ip(x)* such that (Vx < |a|)(V>(z) —• *<t>{x))* and such that *ip(x)* satisfies *all* instances of (prima facie) much stronger induction hypotheses: for *every* polynomial time computable function /

ψ(0) A (Vx < |a|)(V>(x) - tf(/(x))). (4)

It is important that if the formula *<p* is a 2b(S?) formula (i.e. built from Ej formulas by using Boolean connectives and sharply bounded quantifiers; see Definition 8), then the formula *tp* produced by our construction is also a XJQ(SJ) formula.

The speed-up induction method is, when interpreted model-theoretically, very closely related to the cut-shortening method.[4] The cut-shortening method, useful for many purposes (see e.g. [13] and [12]), was originally introduced by R. Solovay in [13]. Of course, here even if *<f>* satisfies (3), *<j>* does not necessarily define a cut in the standard sense, since (Vx,y < *\a\)(y < xA<f>(x) —> <j>(y))* need not necessarily hold. Also, it is possible that *<f>(x)* holds for all x_< |a|, and, moreover, that the set {x | (Vy *<_x)</>(y)}* has a top element >_ *\a*. Replacing formula *<j>* by another formula which does define a cut complicates applications of this technique in proof-theory (see [2]). Also, Solovay's cut-shortening technique increases the quantifier complexity of the formula which defines the shortened cut by addition of unbounded quantifiers. Solovay's technique has been modified to suit applications in bounded arithmetic by P. Pudlák in [12]. His version of the cut shortening technique, if applied to a cut defined by a bounded formula *I(x)*, produces a cut which is closed for all polynomial time computable functions, but this cut is defined by a bounded formula which has higher bounded quantifier complexity than the formula /(x). This makes Pudlák's version of the cut-shortening technique (formulated for binary strings) impossible to use in the proof of our Lemma 2, since we would get formulas for which we do not have comprehension axioms. The speed-up induction technique, formulated for formulas of the language of bounded arithmetic, will also be used in the proof of Theorem 4 to obtain an interpretability result; other applications can be found in [2] and [9].

Lemma 2 *Let M be a model of a theory* T *of a language* L D L∮ *such that* T *extends the theory* C^b *and let* W *and* $\overline{W}$ *be as in Definition 3.3 and 3.5. Then also* $\overline{W}$ C W, *and consequently* $\overline{W}$ = W.

[4] The fact that the speed-up induction method is related to the cut-shortening method was pointed out to me by S. Buss; instead of having this model-theoretic interpretation in mind, my motivation was the induction axioms themselves. I want to thank Sam Buss also for reading this manuscript and an early version of it, and for making many helpful suggestions.

Proof: Let x_0 be an arbitrary element of $\overline{\mathbf{W}}$ and let $\mathcal{F}$ be an arbitrary element of $\mathbf{Ind}(\mathcal{M})$. We have to show that $x_0 \in \mathbf{W}$; for this it is enough to show that $x_0 \in \mathcal{F}$. Consider the formula $\Theta(z, x_0)$ such that

$$\Theta(z, x_0) \overset{df}{=} (\forall x \subseteq x_0)(\forall y \subseteq x_0)((y \subseteq x) \wedge (x \preccurlyeq y \oplus z) \wedge (y \in \mathcal{F}) \rightarrow (x \in \mathcal{F})).$$

Claim 1 *The following are true in* $\mathcal{M}$:

(i)

$$(\forall z)(\forall u \preccurlyeq z)(\Theta(z, x_0) \rightarrow \Theta(u, x_0));$$

(ii) for an arbitrary natural number m,

$$(\forall z)(\Theta(z, x_0) \rightarrow \Theta(z \otimes \underline{m}, x_0)).$$

Proof: Part (i) of Claim 1 follows immediately from the axioms of $BASIC$ and the definition of Θ. To prove (ii), assume $\Theta(z, x_0)$ and fix arbitrary substrings x and y of x_0 such that $x \preccurlyeq y \oplus (z \otimes \underline{m})$. If $m = 0$ or $m = 1$, Claim 1 is trivial, thus, we can assume that $m \geq 2$. Consider the sequence $t_0, \ldots, t_m$, such that $t_0 = y$ and $t_{i+1} = x_0 \upharpoonright (t_i \oplus z)$ for all $i < m$; we now apply $\Theta(z, x_0)$ m times instantiating its quantifiers with the pairs $\langle t_i, t_{i+1} \rangle$ to get part (ii) and thus finish the proof of Claim 1.

Consider the formula $\Psi(w, x_0)$ such that

$$\Psi(w, x_0) \overset{df}{=} (\forall z_1 \subseteq x_0)(\forall z_2 \subseteq x_0)((z_2 \preccurlyeq z_1 \otimes w) \wedge \Theta(z_1, x_0) \rightarrow \Theta(z_2, x_0)).$$

Claim 2 *The following are true in* $\mathcal{M}$

(i)

$$(\forall w)(\forall v \preccurlyeq w)(\Psi(w, x_0) \rightarrow \Psi(v, x_0));$$

(ii) for all natural numbers k *and* n,

$$\Psi(\varepsilon, x_0) \wedge (\forall w)(\Psi(w, x_0) \rightarrow \Psi(w^k \oplus \underline{n}, x_0)),$$

Proof: Part (i) of this claim again follows from the axioms of $BASIC$ and the definition of Ψ. To prove (ii) notice that $\Psi(\varepsilon, x_0)$ holds trivially. Assume $\Psi(w, x_0)$, and let z_1, z_2 and w be arbitrary elements such that the antecedent of the corresponding instance of the matrix of $\Psi(w^k \oplus \underline{n}, x_0)$ holds. If w is ε, $S^0(\varepsilon)$ or $S^1(\varepsilon)$, then the Claim we are proving follows from (ii) of Claim 1. One can prove in $BASIC$ that there is a natural number p such for any other string w, w^k 0 n_^ t i / . Thus we consider the sequence vo = $z\backslash$ and Ui+i = 22 f (vi ® w) f°r a^ 0 $\leq$ i < p. Using ty(tu,x_0) we get 0(t;$_t$-,x_o) —* 0(v-,+i,x_o) for all i < p, which implies ^(tx;^{P},x_0). Now we just use part (i) to get part (ii) and finish the proof of Claim 2.

Notice that we *have not* used the assumption that T is inductive in the proofs that our formulas have the closure properties stated in Lemmas 1 and 2. If T is not inductive, then 0(z,xo) holds only for z = e> and so, since for all w we have e ⊗ w = e, ^(w, xo) holds for all w, in which case the four properties given in Lemma 1 and Lemma 2 trivially hold.

Finally, to prove Lemma 2, we note that 0(z, xo) and *£(«;, xo) are S$^b_0$ formulas. Thus, the comprehension axiom for *rp* implies that there is an element *Xy* £ Set(Ai) such that *(Vw)(w £ X** ⟺ \£(u;,xo)). Since for all functions / with polynomial growth rate there are natural numbers k and n such that *f(w,Y)* ^ w^k 0 n, Claim 2 implies that if u; 6 A* then *f(w,Y)* £ A"^; also, clearly e £ X* (all of this this easily generalizes to functions with several first order variables). Thus, *Xy* belongs to Cl(Af). Since $\overline{W}$ is the intersection of all U such that U £ *C\(M)* and since by our assumption *XQ* £ $\overline{W}$, we have xo £ *Xy* , i.e. the following is true in *A4:*

$$(\forall z_1 \subseteq xo)(V22 \subseteq x_o)((z_2 \wedge z\backslash\ 0\ x_0)\ A\ 0(zi, x_0) — 0(z_2, x_0)).$$

Take 22 = xo and $z\backslash$ = xo f 5°(5); then from the last formula it follows that

$$M\backslash = e(x_0 \quad \backslash S°(e),x_o)\text{-}{*}Q(x_o,x_o).$$

But clearly

$$(Vx \subseteq x_o)((x \text{ £ } T) - ((5°(x) \text{ £ } T)\ A\ (5^x(x) \text{ £ } /*))) - 0(x_o\ f\ S°(e), x_0).$$

Thus, since .T^7 is inductive (and this is the only place in this proof in which we use this fact), 0(x_o,x_o) holds, i.e. for all initial segments x and y of xo we have

$$(y\ Q^x)\ A\ (x \wedge y\ 0\ x_0)\ A\ y \text{ £ } T \text{-}\bullet x \text{ £ } T.$$

Taking x = x_{Oj} y = e and using the fact that e £ T, we get x_0 £ $T\backslash$ this, as we noted, implies (2) of our Lemma 2. •

Corollary 1 *Let M be a model of a theory* T *of a language* L_D L|, *such that* T *extends the theory* C^b. *Then* W ts *an initial segment (i.e. a complete binary subtree of the first order part Str(M) of the universe of M.) which is closed for all functions with polynomial growth rate.*

Proof: This is an immediate consequence of the following facts: (i) W is an initial segment of the whole first order part of the universe of *M* (Lemma 1); (ii) $\overline{W}$ = W (Lemma 2); (iii) $\overline{W}$ is closed for all functions with polynomial growth rate because it is the intersection of sets which have this property. •

Definition 4 *Let* T *be a theory of a language* L*; then the following set of conditions we denote by C.*

1. *The language* **L** *of the theory* **T** *extends the language \J\.*
2. *Theory* **T** *extends the theory* C^b*; thus,* **T** *contains the comprehension schema for all* **EQ** *formulas of the language JJ\ .*
3. *It is provable in* **T** *that every /i*($\vec{x}$, $\vec{X}$) *£L has polynomial growth rate, i.e. if* $\vec{x}$ = (x$_0$,..., x*) *then*

$$\mathbf{T\ h\ (v\vec{x})(V\vec{x})(/i(\vec{x}, \vec{x}) \wedge (x_0\ e \ldots e\ {*}{*})^m\ e\ R).}$$

Corollary 1 enables us to introduce the following definition.

Definition 5 *Let M be a model of a theory* **T** *of a language* **L** *such that* **T** *satisfies condition C.*

1. W^1 **15** *the substructure of the first order part* M^l *of the structure Ai which consists of the set* **W** *together with the restrictions of the interpretations of the purely first order symbols of the language* **L** *to the set* **W**.
2. W^2 **is** *the substructure of M. whose domain is the pair of sets* **(W,Set(.M))** *together with the restrictions of all relations and functions of the language* **L** *to the sub-universe* **(W,Set(jM)).**

Clearly, the structure W^2 satisfies all universal consequences of the theory T, while the structure W^1 satisfies all purely first order universal consequences of T. In particular, if T is our theory C^6 (C^p), then W^1 satisfies all axioms of *BASIC (BASIC?).*

Let <*p* be an arbitrary formula; then <p^w denotes the formula obtained from <*p* by relativizing all first order quantifiers of <*j*> to the universe W defined by the formula *W(x).* Thus, if <*p* is of the form (Vx $\underline{C}$ *t) 9,* (Vx ^ *t)* (9, (Vx) (9, (3x$\underline{\ }$C *t) 9,* (3x ^ *t) 9,* or (3x) *9,* then <p^w is of the form (Vx$\underline{\ }$C *t)(W(x)* — 0^w), ***(Vx ^t)(W(x) ^ 9^W), (Vx)(W(x) -+ 9^w)$_y$ (3x_Ct)(W(x)A9^w), (3x ^t)(W(x)A9^w)* or *(3x)(W(x)A9^w)***

respectively. Thus, for an arbitrary formula $\varphi(\vec{x},\vec{X})$, an arbitrary sequence $\vec{s}$ of elements of $\mathbf{W}$ and an arbitrary sequence $\vec{S}$ of elements of $\mathbf{Set}(\mathcal{M})$, $\mathcal{W}^2 \models \varphi(\vec{s},\vec{S})$ if and only if $\mathcal{M} \models \varphi^W(\vec{s},\vec{S})$.

Condition (3) of $\mathcal{C}$ implies that all terms of the language $\mathbf{L}$ define (provably in $\mathbf{T}$) functions with polynomial growth rate. Combining this with the closure properties of $\mathbf{W}$ given by Lemmas 1 and 2, the following Lemma can be easily proved by an induction on the complexity of bounded formulas.

Corollary 2 *Let* $\mathbf{T}$ *be a theory of a language* $\mathbf{L}$ *satisfying conditions* $\mathcal{C}$. *Then all bounded formulas of the language* $\mathbf{L}$ *are absolute between the universe and the substructure* $\mathcal{W}^2$, *i.e. for an arbitrary bounded formula* φ *with free variables* $\vec{X},\vec{x}$

$$\mathbf{T} \vdash (\forall\vec{X})(\forall\vec{x})\left(\bigwedge_{x_i\in\vec{x}} W(x_i) \rightarrow (\varphi(\vec{x},\vec{X}) \leftrightarrow \varphi^W(\vec{x},\vec{X}))\right).$$

We now formulate a strengthening $\mathcal{C}^*$ of the set of conditions $\mathcal{C}$ for theories extending our base theory $\mathbf{C}^b$.

Definition 6 *Let* $\mathbf{T}$ *be a theory of a language* $\mathbf{L}$. *We denote by* $\mathcal{C}^*$ *the set of conditions consisting of conditions* (1) *and* (2) *together with the the following strengthening* (3*) *of the condition* (3) *of* $\mathcal{C}$.

3*. *Theory* $\mathbf{T}$ *contains the comprehension axiom schema for all* $\mathbf{\Sigma_0^b}$ *formulas of the whole language* $\mathbf{L}$.

Examples of theories satisfying condition $\mathcal{C}^*$ are our theories $\mathbf{C}^b$ and $\mathbf{C}^p$. Also, some of the theories defined in [10] in the course of a proof-theoretic analysis of theories $\mathbf{C}^b(\Sigma_i^b)$ also satisfy condition $\mathcal{C}^*$. We now want to show that in any model of a theory $\mathbf{T}$ satisfying condition $\mathcal{C}^*$ the corresponding structure $\mathcal{W}^2$ satisfies an appropriate fragment of induction. Thus, $\mathbf{W}$ indeed resembles the set of natural numbers as defined in set theory, not only by its definition but also by its properties.

Definition 7 *The polynomial induction schema for a class of formulas* Φ, *denoted by* $\Phi - PIND$, *is the following schema:*

$$\phi(\varepsilon,\vec{y},\vec{Y}) \wedge (\forall x)(\phi(x,\vec{y},\vec{Y}) \rightarrow (\phi(S^0(x),\vec{y},\vec{Y}) \wedge \phi(S^1(x),\vec{y},\vec{Y}))) \rightarrow (\forall x)\varphi(x,\vec{y},\vec{Y}), \qquad (5)$$

where $\varphi(x,\vec{y},\vec{Y})$ *is a formula from the class* Φ.

Theorem 1 *Let* $\mathbf{T}$ *be a theory satisfying conditions* C^* *and let* φ *be a* $\Sigma_0^{\mathbf{b}}$ *formula of the language* $\mathbf{L}$, *with free variables* $x, y_0, \ldots, y_n, Y_0, \ldots, Y_k$; *then* $\mathbf{T}$ *proves*

$$(\forall \vec{y})(\forall \vec{Y})(\forall x)(W(x) \wedge \varphi(\varepsilon, \vec{y}, \vec{Y}) \wedge (\forall s \prec x)(\varphi(s, \vec{y}, \vec{Y}) \rightarrow (\varphi(S^0(s), \vec{y}, \vec{Y}) \wedge \varphi(S^1(s), \vec{y}, \vec{Y}))) \rightarrow \varphi(x, \vec{y}, \vec{Y})).$$

Notice that parameters $\vec{y}$ need not be in $\mathbf{W}$.

Proof: Let x_0 be an arbitrary element of $\mathbf{W}$; consider the formula $((x \preccurlyeq x_0) \wedge \varphi(x, \vec{y}, \vec{Y})) \vee (x_0 \prec x)$. This formula is clearly also a $\Sigma_0^{\mathbf{b}}$ formula of the language $\mathbf{L}$ and so using the comprehension axiom we get a set X which contains ε and which is closed for both successor functions. Since $x_0 \in \mathbf{W}$ we get $x_0 \in X$, and so $\varphi(x_0)$ holds. ■

Corollary 3 *Let theory* $\mathbf{T}$ *be a theory satisfying conditions* C^*; *then* $\mathbf{T}$ *proves the induction schema for all* $\Sigma_0^{\mathbf{b}}$ *formulas of the language* $\mathbf{L}$ *relativized on* $\mathbf{W}$.

Proof: Using the closure properties of $\mathbf{W}$ (Lemma 1) and the absoluteness of bounded formulas (Corollary 2), it is easy to see that induction relativized on $\mathbf{W}$ follows from Theorem 1. ■

Thus, if $\mathcal{M}$ is a model of the theory $\mathbf{C}^p$, our remark after Definition 5 together with Corollary 3 imply that $\mathcal{W}^1$ is a model of the theory *PTCA*, introduced by Ferreira in [5] (see also [4]).[5] If $\mathbf{T}$ is our theory $\mathbf{C}^b$, then $\mathcal{W}^1$ satisfies only a weak fragment of the theory *PTCA* consisting of the axioms of *BASIC* together with the induction schema for sharply bounded formulas of the language L^b. In this theory one cannot define all polynomial time functions; see our remark after Corollary 6.

The above propositions provide us with the basic properties of the predicate $W(x)$ which defines the collection of the "number-like" sequences in theories extending our base theory $\mathbf{C}^b$. Thus, these propositions provide an adequate "bootstrapping" of our base theory $\mathbf{C}^b$, and we are now ready to characterize all the levels of the polynomial time hierarchy as classes of provably recursive functions (with graphs of suitable bounded complexity) of theories extending theory $\mathbf{C}^b$.

[5] Essentially, *PTCA* is a binary-string version of Cook's theory *PV*. Cook was the first to introduce polynomial time computable functions in a formal theory containing definitions by composition and limited recursion of such functions (see [3]). However, instead of a theory for binary strings $\{0,1\}^*$, Cook defined an arithmetical theory and in the definitions by limited recursion he used strings $\{1,2\}^*$ corresponding to the dyadic notation of a natural number.

3. Delineating the Polynomial Time Hierarchy

We now define some extensions of our base theory $\mathbf{C}^b$ which will be used to delineate the levels of the polynomial time hierarchy of functions. Intuitively, a stronger comprehension schema allows us to construct and prove convergence of algorithms which have more complex properties (recall that sets can be seen as extensions of properties in Frege's sense). On the other hand, having stronger comprehension implies having more sets in the second order part of the universe (the first order part i.e. the collection of all binary strings remains the same); this in turn places further restrictions on what sequences are "numbers", because there might be more sets in $\mathbf{Ind}(\mathcal{M})$, so their intersection $\mathbf{W}$ might be smaller. Intuitively, this is not surprising: some sequences which could be treated as "numbers" for simpler algorithms might be too long to allow more complex procedures to be correctly performed on them. Recall that by our Lemma 2, in any theory extending $\mathbf{C}^b$ the collection of "numbers" $\mathbf{W}$ is the collection of sequences of "sufficiently small" length. Thus, in our foundational approach, to secure the convergence of more complex algorithms we add more sets, which automatically appropriately redefines the universe of the number-like sequences $\mathbf{W}$, restricting it to only those that are sufficiently short to allow performing these more complex algorithms. This is why we feel that our approach is quite natural and intuitive from the foundational perspective. For models $\mathcal{A}$ of purely first order theories of bounded arithmetic such as S_2^i, in order to get a model in which more complex algorithms are convergent, we must either take a cut in $\mathcal{A}$ which satisfies stronger induction or replace the whole structure $\mathcal{A}$ by another one satisfying such stronger induction. However, from the foundational perspective, this approach does not seem to be suggested either by the usual definitions of the set of natural numbers or of an algorithm.

To delineate various computational complexity classes we must suitably restrict the class of formulas which are allowed to appear in the comprehension schema. There are several ways to do so; here we present one of them, based on limiting not only the bounded quantifier complexity, but also the appearance of the second order parameters in the formulas allowed in the comprehension schema. This approach appears to be the simplest one which results in theories of an appropriate strength. Another approach will be presented in the second part of this paper.

Definition 8 *Let* $\mathbf{L}$ *be a language extending the language* L^b. *The classes of (purely first order)* Σ_i^b, Π_i^b *and* $\Sigma_0^b(\Sigma_i^b)$ *formulas are defined (simultaneously) inductively as follows:*

1. *The classes of* $\overset{b}{\mathrm{E}}\mathrm{Q}_;$ $^{b}\mathrm{HQ}$ *and* $\overset{b}{£}\mathrm{o}(£\mathrm{o})$ $f^{ormu}\wedge^{as\ are\ a}\wedge\ ^{e}Q^{ua}\wedge\ t^{\circ}\ \wedge^{e}\ \wedge^{easi\ sei}$ *of formulas which contains all* first order *atomic formulas and which is closed for all Boolean connectives and sharply bounded quantifiers 3x* $\underline{\mathrm{C}}$ $t(\vec{y})$ *and* Vx $\underline{\mathrm{C}}$ $t(\vec{y})$.

2. *The class of* $\mathrm{E}_{i}^{*}{}_{+1}$ *is the least set of formulas containing all* $\mathrm{E}\overset{b}{\mathrm{Q}}(\mathrm{E}_{i}^{*})$ *formulas which is closed for* A, V, *sharply bounded quantifiers and bounded existential quantifiers 3x* =3: $t(\vec{y})$.

3. *The class of* $\mathrm{H}_{i}^{*}{}_{+1}$ *formulas is the least set of formulas containing all* $\mathrm{E}\overset{b}{\mathrm{Q}}(\mathrm{E}_{i}^{*})$ *formulas which is closed for* A, V, *sharply bounded quantifiers and bounded universal quantifiers* Vx =3: $t(\vec{y})$.

4. *The class of* $£\overset{b}{\mathrm{Q}}(\mathrm{E}_{i}^{*}{}_{+1})$ *formulas is the least set of formulas containing all* $\mathrm{E}_{i}^{*}{}_{+1}$ *and* $\mathrm{n}_{i}^{*}{}_{+1}$ *formulas which is closed for all Boolean connectives and sharply bounded quantifiers.*

Definition 9 *Let* L *be a language extending the language* $\backslash j^{h}{}_{2}$. *The class* $\mathrm{O/S}\overset{b}{\mathrm{Q}}(\mathrm{EJ})$ *formulas of the language* L *is the least set of formulas which contains both first and second order atomic formulas of the language* L *and (purely first order)* E_{i}^{*} *formulas which is closed for all Boolean connectives and sharply bounded quantifiers.*[6]

Definition 10 *Let* T *be a theory of the language* L *such that* T *satisfies condition (C*); then* T(Ef) *is the theory obtained from* T *by adding the comprehension schema for the class of purely first order* Ej *formulas of the language* L.

Clearly, T(£$) is just T itself.

Lemma 3 *Let* T *be a theory as in Definition 10, and let* T(S^(Ef)) *be the theory obtained from the theory* T *by replacing the comprehension schema for the class of* $\mathrm{S}\overset{b}{\mathrm{Q}}$ *formulas of the language of* $\mathrm{T}_;$ *with the comprehension schema for* $\mathrm{S}\overset{b}{\mathrm{Q}}(\mathrm{E}^{*}_{i})$ *formulas of the same language. Then the theory* T(Ef) *and the theory* $\mathrm{T}(\Sigma_{0}^{b}(\mathrm{E}_{i}^{*}))$ *have the same set of consequences.*

Proof: Clearly, theory T(Ej) is a sub-theory of the theory T(S^(Ef)), since all instances of both schemas of T(Ef) are also instances of the comprehension schema of the theory $\mathrm{T}(\mathrm{E}\overset{b}{\mathrm{Q}}(\mathrm{E}^{*}_{i}))$. In the other direction, consider an instance of the comprehension schema for a $\mathrm{S}\overset{b}{\mathrm{Q}}$ (E_{i}^{*}) formula $0(x, \vec{I}, \vec{Y})$, and let $\wedge fc(\wedge, \vec{z}, \vec{y})$, $k \leq n$,

[6] Notice that the difference between Dj(Ef) and $\mathrm{Sj}_{i}^{*}(£\mathrm{f})$ formulas is that the former are purely first order formulas, while the latter ones include second order *atomic* formulas in the set of formulas which we close for Boolean combinations and sharply bounded quantifiers.

be all E;* sub-formulas of the formula $0(x,\vec{y},\vec{Y})$, such that 0 is built from atomic formulas and formulas *il)k{x,z̄,ȳ),* $k \leq$ n, using only Boolean connectives and sharply bounded quantifiers. We now consider purely first order formulas **l>*_k{v̄,y)* such that T h *xl>k{x̄,z,ȳ)* <-• *ipl((x,* $(\vec{z})$),ȳ), where *(z̄)* stands for *(zi,* (z$_2$,..., *(zm-i,* z$_m$))...). We now fix parameters $\vec{y}, \vec{Y}$ and apply instances of the E; comprehension schema for all formulas *i/>l(v,ȳ)* to obtain sets X_k such that for all v, v G X_k «-• V^^?!7)- Let J? = ^o,...X_n, and let the formula $Q^*(x_y\vec{y},\vec{X}_1\vec{Y})$ be obtained from the formula $Q(x_1\vec{y}_y\vec{Y})$ by replacing subformulas *tl>k{x,*z,y,y) by formulas (x, $(\vec{z})$) G X_k. We now apply the instance of the SQ comprehension schema for the formula 0*(x, ȳ, $\vec{X}_{\}}$ $\vec{Y}$) to obtain a set Xe* such that for all x, *x* G Xe* <> 0*(ar, ȳ, $\vec{X}$, $\vec{Y}$). Clearly, for such a set *X* and ail x, x G A'e* <> $0(x,\vec{y},\vec{X},\vec{Y})$. I

In this section we will also establish some natural connections between our theories and a version of the well known fragments of bounded arithmetic S^x_2, formulated for binary strings.

Definition 11 Sĵ *is a theory of the language* L^h *obtained from the theory BASIC by adding the polynomial induction schema for the class of* Ef *formulas of the language L\,.*

Thus, for i $\geq$ 1, Ŝ2 is basically a binary-string version of the fragments of bounded arithmetic *S* as introduced by Buss in [1]. On the other hand, if we add to $BASIC^P$ the polynomial induction schema for Sô formulas of the language *IP*, we get Ferreira's *PTC A*, while his *PTCA+* (see [5] and [4]) is obtained by adding to $BASIC^9$ the Ej-PIND induction schema. Theories $S\hat{*}_2$ (with a different notation) were also introduced in [6].

We now formalize the notion of a provably recursive function for our theories C^6(Ej). This notion certainly applies to functions of mixed type (usually called functionals); however, since here we are primarily interested in characterizing classes of the polynomial time hierarchy, we will restrict ourselves to purely first order functions. In the second part of this paper we deal with functions of mixed type, where the second order variables range over functions of arbitrary growth rate, rather than over sets. However, for that reason, the comprehension schema will be restricted in a different way.

Definition 12 *The set of all finite binary strings B* = {0,1}*, *together with its usual operations and relations is called* the standard first order structure of binary strings *and is denoted by* B^1.

Definition 13 *A function* $f(\vec{x}): B^k$ -» *B is* Ej*-definable in the theory* C*(Ej) *if there is a* $E^b_{\{}$ *formula*

$\varphi_f(\vec{x}, y)$ *such that the following holds:*

$$\mathbf{C}^b(\Sigma^b_i) \vdash ((\forall \vec{x})(\exists! y)\varphi_f(\vec{x}, y))^W,$$

$$\mathcal{B}^1 \models (\forall \vec{x})\varphi_f(\vec{x}, f(\vec{x})).$$

Note that by our absoluteness result (Corollary 2) the first condition is equivalent to

$$\mathbf{C}^b(\Sigma^b_i) \vdash (\forall \vec{x})(\bigwedge_{x_i \in \vec{x}} W(x_i) \rightarrow (\exists! y)(W(y) \wedge \varphi_f(\vec{x}, y))).$$

We use the usual definitions of the notions from bounded arithmetic, except that here numbers are replaced by binary strings. In particular, $\square^p_{i+1}$ is the collection of all functions computable in polynomial time with a Σ^b_i-oracle (see [1]), and a function $f(\vec{x})$ is Σ^b_i-definable in the theory $\hat{S}^i_2$ if there exists a Σ^b_i formula $\varphi_f(\vec{x}, y)$ such that $\hat{S}^i_2 \vdash (\forall \vec{x})(\exists! y)\ \varphi_f(\vec{x}, y)$ and $\mathcal{B}^1 \models (\forall \vec{x})\varphi_f(\vec{x}, f(\vec{x}))$.

Theorem 2 *For all $i \geq 0$ theories $\mathbf{C}^b(\Sigma^b_i)$ and $\hat{S}^i_2$ have the same classes of Σ^b_i-definable functions.*

To prove Theorem 2 we need several lemmas.

Lemma 4 *For any model $\mathcal{M}$ of the theory $\mathbf{C}^b(\Sigma^b_i)$, the corresponding structure $\mathcal{W}^1$ is a model of the theory $\hat{S}^i_2$. Thus, theory $\hat{S}^i_2$ is interpretable in the theory $\mathbf{C}^b(\Sigma^b_i)$.*

Proof: As we noted after Definition 5, axioms of $BASIC$ hold in $\mathcal{W}^1$. Thus, it suffices to show that also $\mathbf{C}^b(\Sigma^b_i) \vdash (\Sigma^b_i - PIND)^W$. First of all, our absoluteness result and the closure properties of $\mathbf{W}$ (Lemma 2) imply that it is enough to prove in $\mathbf{C}^b(\Sigma^b_i)$ that for any $x_0 \in \mathbf{W}$,

$$\varphi(\varepsilon, \vec{y}) \wedge (\forall t)(\varphi(t, \vec{y}) \rightarrow (\varphi(S^0(t), \vec{y}) \wedge \varphi(S^1(t), \vec{y}))) \rightarrow \varphi(x_0, \vec{y}). \tag{6}$$

We now fix values for parameters $\vec{y}$ and use the corresponding instance of the Σ^b_i-comprehension axiom schema to get the set $X_{\varphi,\vec{y}}$ such that $X_{\varphi,\vec{y}} = \{x \mid \varphi(x, \vec{y})\}$. Then (6) is equivalent to

$$(\varepsilon \in X_{\varphi,\vec{y}}) \wedge (\forall t)((t \in X_{\varphi,\vec{y}}) \rightarrow ((S^0(t) \in X_{\varphi,\vec{y}}) \wedge (S^1(t) \in X_{\varphi,\vec{y}}))) \rightarrow (x_0 \in X_{\varphi,\vec{y}}),$$

which immediately follows from the fact that $x_0 \in \mathbf{W}$. ■

Corollary 4 *For any formula σ of the language of $\hat{S}^i_2$, if $\hat{S}^i_2 \vdash \sigma$ then $\mathbf{C}^b(\Sigma^b_i) \vdash \sigma^W$.*

The converse of Lemma 4 is also true. Unfortunately, with a definition of $C^6(E_t^b)$ in which the comprehension schema asserts the existence of infinite sets, we must use an expandability property of models, rather than interpretability of theories. One can replace our comprehension schemas by ones that assert only the existence of appropriately defined *finite* sets, i.e. by schemas of the form

$$(V\bar{y})(V\vec{Y})(Vz)(3X)(Vx)(x \text{ G } X \text{ «> } (x \leq z) \text{ A } y{>}(x, \bar{y}, \vec{Y}))$$

where *<p* is a formula of the appropriate class not containing variable *X*. However, this approach would make our definition of W awkward and is not very useful in any other way, except that such theories are in fact interpretable in the corresponding theories S_2^i • This can be easily proved using the partial truth predicates $/i_t$- for E_i^* formulas which we use in the proof of Theorem 4.

Lemma 5 *Any model A of* S_2^{l} *is expandable to a model* A^2 *of* $C^6(E_i^*)$ *with the same first order domain by adding only a suitable set of second order objects.*

Proof: Let *A* be any model of 5^. Consider the class of all subsets of *A* which are parametrically definable in *A* by $E\dot{Q}(E_i^*)$ formulas, i.e. formulas which are the closure of Ej formulas for Boolean connectives and sharply bounded quantifiers. This class of sets we take as the second order part Set(^4) of the universe for a structure A^2 of the language L| whose first order universe is the universe of *A*. The structure A^2 satisfies the axioms of $C^*(E_i^*)$ because $E\dot{Q}(E_i^*)$ formulas are closed for Boolean operations and sharply bounded quantifiers. Moreover, in such a structure W is the whole first order part of the universe, because S_2^{l} proves induction for $E\dot{Q}(E_i^*)$ formulas (see [7]). Thus, the only set containing the empty sequence and closed for successor functions which belongs to our collection of $E\dot{Q}$(E^) parametrically definable sets is the whole universe, which implies that W is equal to the whole universe. •

Corollary 5 *For any first order formula a, if* C*(Ef) h a^w , *then* S^*_2 h *c.*

Proof: Immediate consequence of the previous Lemma and the Completeness Theorem. •

From Corollary 4 and Corollary 5 we get the following Theorem.

Theorem 3 *Let (p be a* E_i^* *formula, then*

$$C^b(\Sigma_i^b) \vdash ((\forall x)(\exists! y)\varphi(x, y))^W$$

if and only if

$$\hat{S}_2^i \vdash (\forall x)(\exists! y)\varphi(x, y).$$

As an immediate corollary of the previous theorem and the binary string version of the Main Theorem of Buss's [1], in the form proved by Ferreira in [6], we get the main result of this paper:

Corollary 6 *For all i* $\geq$ 1, Ej *-definable functions of the theory* C^6(Ef) *are exactly* Df *functions.*

For *i* = 0, it is easy to see that our technique of building models of theories with comprehension axioms from models of bounded arithmetic (Lemma 5) and the main Theorem from Section 2 of Chapter 2 in Ferreira's [5] imply that the structure W^1 in models of C^6 satisfies only a weak theory, in which not all polynomial time functions are definable. This is why, in order to have a theory with a comprehension schema for EQ formulas only, which is sufficiently strong to delineate the class of polynomial time computable functions, we have to extend the language *JJ* by adding a symbol for every such function and thus obtain our language *lf*$_2$ and theory C^p. In fact, in [10] we further extend the language *\7*$_2$ by adding a new mixed type function symbol for every function computable in polynomial time with oracles for the set-variables.

Finally, we want to explain our choice of the classes of formulas allowed in the comprehension schemas of the theories C^6(E*). It is easy to see that addition of the comprehension schema for all SJj* formulas (i.e. all formulas obtained from the first and second order atomic formulas closing for Boolean operations, both sharply bounded quantifiers and existential bounded quantifiers) to C* produces a theory (which we denote by C^6(S^)) in which every instance of the comprehension schema for bounded formulas is provable. In this theory for any bounded formula *(p* with a EQ-matrix *rp* we can replace the inner-most bounded quantifier and the matrix, say *(3x ^ t(y))tp(x*$_1$ *y)* with (t/o,..., t/jt) £ *X$* , where *X^* is obtained by applying the appropriate instance of the S/b comprehension schema. We can repeat this procedure until we get a EQ formula. It is not difficult to show that if we have comprehension for all bounded formulas, then W satisfies 52 *(=\Ji E uS^*) and so all functions from all levels of the polynomial time hierarchy are provably recursive in this theory. On the other hand, since any model of *S2* can be expanded to a model of C^6(E??) by adding all sets parametrically definable by bounded formulas (due to the induction schema, the only set in Ind(At) is just the whole first order universe and so W is equal to the whole universe). Thus, we get that the *T*-definable functions of C^6(S^) are exactly the functions from all levels of the polynomial time hierarchy. This is why, in older to get a theory whose E*-definable functions are exactly the functions from the i^{th} level of the polynomial hierarchy ($i \geq 1$), restriction of the bounded quantifier complexity of the formulas allowed in the comprehension schema is not enough.

Another way to restrict the comprehension schema is along the lines of Leivant's original work. Let $\mathbf{\Sigma_1^{b+}}$ be all formulas obtained as the closure for Boolean operations, sharply bounded quantification and bounded existential quantification of atomic first and second order formulas, but in which all *second order* atomic formulas appear *positively*[7]. Consider a theory which, besides the axioms of $BASIC$ has the Comprehension Schema for all $\mathbf{\Sigma_1^{b+}}$ formulas of $\mathbf{L}_2^b$; denote it by $\mathbf{C}^b(\mathbf{\Sigma_1^{b+}})$. Then Σ_1^b-definable functions of this theory are again only polynomial time computable functions. To see this, consider any model of S_2^1, and notice that the collection of all sets parametrically definable by Σ_1^b formulas (with the usual definition of such first order formulas) satisfy $\mathbf{\Sigma_1^{b+}}$ Comprehension (the positiveness requirement is here crucial). Again, the only definable set in $\mathbf{Ind}(\mathcal{M})$ is the whole universe, and thus we get that for any model $\mathcal{A}$ of S_2^1 there is a model of $\mathbf{C}^b(\mathbf{\Sigma_1^{b+}})$ with $\mathcal{A}$ as $\mathbf{W}$. But this clearly implies that all Σ_1^b-definable functions of $\mathbf{C}^b(\mathbf{\Sigma_1^{b+}})$ are Σ_1^b-definable functions of S_2^1, and thus polynomial time computable functions.

4. Interpretability and Fragments of Bounded Arithmetic

In this section we want to give another application of the speed-up induction method, this time to obtain (essentially) an interpretability result. Even though an analogous result also holds for the comprehension theories which we considered in the previous section, we formulate and prove it for more familiar theories of bounded arithmetic.

To make our proofs easier, we will use $\Sigma_i^b - LIND$ rather than $\Sigma_i^b - PIND$ to axiomatize S_2^i. Buss proved in [1] that over S_2^1 these two axiomatizations are equivalent. Recently this result was improved by replacing S_2^1 by $BASIC$ (see [2]); thus we have no loss of generality. Recall that in $BASIC$ we can prove that $(\langle x,y\rangle)_1 = x$, $(\langle x,y\rangle)_2 = y$ and $\langle (x)_1,(x)_2\rangle = x$. Thus, in $BASIC$, every formula for every value of its parameters is equivalent to a formula of the same bounded quantifier complexity which contains only one parameter. Let $BASIC^*$ be the set of axioms of $BASIC$ (as introduced by Buss in [1]) together with the following simple extra axioms: $|x \cdot y| \leq |x| + |y|$, $|x| \leq x$.

[7] Informally, these are formulas such that after we push all negations inside to the atomic subformulas and cancel double negations, all second order atomic subformulas will have no negations in front of them.

Theorem 4 *For every $i \geq 1$ there exists a Π^b_{i+1} formula $\Omega_i(w,v)$ such that for every model $\mathcal{M}$ of $BASIC^*$ either $\mathcal{M} \models S^i_2$ or there exists an element $c \in |\mathcal{M}|$ such that the set $\Omega_i(c) = \{z \mid \mathcal{M} \models \Omega_i(z,c)\}$ is closed for all functions of L^b and is a model for S^i_2, with functions and relations of $\mathcal{M}$ restricted of to $\Omega_i(c)$.*

Proof: Let $\#^n(x)$ be a sequence of terms defined inductively as follows: $\#^0(x) = x$, $\#^{(k+1)}(x) = x\#(\#^k(x))$. Then one can find an appropriately defined Σ^b_i formula μ_i and a finite fragment F^i_2 of S^i_2 (see [7] for the details) such that one can prove in F^i_2 that μ_i has the properties of a partial truth predicate for the class of Σ^b_i formulas. By this we mean that for every Σ^b_i formula $\psi(x,y)$ there exist natural numbers e_ψ and m_ψ such that:

$$F^i_2 \vdash (\forall x)(\forall y)(\forall z)((z \geq \#^{m_\psi}(\langle x,y\rangle)) \rightarrow (\psi(x,y) \leftrightarrow \mu_i(\underline{e_\psi}, \langle x,y\rangle, z))). \qquad (7)$$

Thus, we let $\{\sigma_s \mid s \leq n\}$ be a finite set of formulas such that

1. For all $s \leq n$ (the universal closure of) the formula σ_s is the $\Sigma^b_i - LIND$ induction axiom for a formula $\phi_s(x,y)$, i.e. $\sigma_s(x,y)$ is of the form

$$\phi_s(\underline{0}, y) \wedge (\forall x < |z|)(\phi_s(x,y) \rightarrow \phi_s(x+1,y)) \rightarrow \phi_s(|z|,y).$$

2. The (universal closure of the) formula σ_n is the induction axiom for the formula $\phi_n \equiv \mu_i(e, \langle x,y\rangle, z)$ with e, y, z as parameters.

3. $F^i_2 = BASIC^* \cup \{\sigma_p \mid p \leq n\}$.

Let $\mathcal{M} \models BASIC^*$. If $\mathcal{M} \models F^i_2$ then for arbitrary ψ there exists a number m_ψ such that (7) holds. Consider an instance of the $\Sigma^b_i - LIND$ induction axiom for the formula ψ, with y and a as fixed parameters:

$$\psi(0,y) \wedge (\forall x < |a|)(\psi(x,y) \rightarrow \psi(x+1,y)) \rightarrow \psi(|a|,y). \qquad (8)$$

Let $z = \#^{m_\psi}(\langle |a|, y\rangle)$. Then $(\forall x \leq |a|)(\psi(x,y) \leftrightarrow \mu_i(\underline{e_\psi}, \langle x,y\rangle, z))$, and so (8) follows from the corresponding instance of σ_n for the above value of the parameter z. Thus, in this case $\mathcal{M} \models S^i_2$.

If $\mathcal{M} \not\models F^i_2$ then there exists at least one $k \leq n$ and elements a, b from $\mathcal{M}$ such that the induction axiom σ_k fails for a, b:

$$\mathcal{M} \models \phi_k(\underline{0}, b) \wedge (\forall x)(\phi_k(x,b) \rightarrow \phi_k(x+1,b)), \qquad (9)$$

and

$$\mathcal{M} \models \neg\phi_k(|a|, b). \tag{10}$$

Let for $j \leq n$

$$\Theta_j(z, v, u) \overset{df}{=} (\forall x \leq |v|)(\forall y \leq |v|)((x \leq y) \wedge (y \leq x + z) \wedge \phi_j(x, u) \rightarrow \phi_j(y, u)) \tag{11}$$

$$\Psi_j(t, v, u) \overset{df}{=} (\forall z \leq |v|)(\forall z^* \leq |v|)((z^* \leq z \cdot t) \wedge \Theta_j(z, v, u) \rightarrow \Theta_j(z^*, v, u)) \tag{12}$$

$$\Phi_j(w, v) \overset{df}{=} (\forall u \leq v)\Psi_j(|w|, v, u) \tag{13}$$

$$\Omega_i(w, v) \overset{df}{=} \bigwedge_{j \leq n} \Phi_j(w, v) \tag{14}$$

Clearly, Ω_i is a Π^b_{i+1} formula. Now let $c = max\{a, b\}$; we now prove that

$$\mathbf{\Omega}_i(c) = \{m \mid \mathcal{M} \models \Omega_i(m, c)\}$$

is a set closed for all functions of the language of bounded arithmetic and that it defines a model of S^i_2; this model we will also denote by $\mathbf{\Omega}_i(c)$.

Claim 3 *For every $g \in |\mathcal{M}|$ set $\mathbf{\Omega}_i(g)$ is a cut (not necessarily proper) in the universe of the model $\mathcal{M}$ which is closed for all functions with polynomial growth rate.*

Proof: As in the proof of Lemma 2, for every two natural numbers n, m one can prove in $BASIC^*$ the universal closure of the following formulas:

$$\Theta_j(0, u, v) \wedge (\forall z)(\forall z' \leq z)(\Theta_j(z, u, v) \rightarrow (\Theta_j(\underline{n} \cdot z, u, v) \wedge \Theta_j(z', u, v))), \tag{15}$$

$$\Psi_j(\underline{n}, u, v) \wedge (\forall w)(\forall w' \leq w)(\Psi_j(w, u, v) \rightarrow (\Psi_j(w^n + \underline{m}, u, v) \wedge \Psi_j(w', u, v))). \tag{16}$$

These proofs can be carried out in $BASIC$ *without* using any assumptions on formulas ϕ_j. In fact, if (9) fails for some values of u, v, then for these values $\Theta_j(z, u, v)$ holds if and only if $z = 0$, but this implies that for such values of u, v, the formula $\Psi_j(w, u, v)$ holds for *all* w. Thus, the formula $\Psi_j(w, u, v)$ always defines an initial segment which contains all the standard numerals and is closed for the squaring function. Using the fact that in $BASIC^*$ we have $|x\#y| = |x|\cdot|y|+1$, $|x\cdot y| \leq |x|+|y|$, $|x| \leq x$, $x \leq y \rightarrow |x+y| \leq |2\cdot y| = |y|+1$, and (16), is easy to show that formula $\Psi_j(|w|, v, u)$ defines an initial segment closed for all functions with polynomial growth rate. This clearly implies that the same holds for the set $\{m \mid \mathcal{M} \models \Omega_i(m, g)\}$ for every $g \in |\mathcal{M}|$. ■

Thus, as in the case of $\mathbf{W}$ in the Lemma 1, we get the following absoluteness property of $\mathbf{\Omega}_i(c)$.

Lemma 6 *It is provable in BASIC* that for every g* G *\M\ all bounded formulas are absolute between fti(g) and the whole universe M, i.e. for any value of parameters from fli(g), any bounded formula is true in the substructure Cli(g) if and only if it is true in M.*

Clearly *Cli(c)* satisfies all the axioms of *BASIC**. We now want to show that ft;(c) also satisfies all axioms of S*2. For this purpose we first prove the following Claim.

Claim 4 *One can prove in BASIC* that for every natural number j <_n and arbitrary elements g,* A, m

(h ≤ g) A (m_< *g)* A *Qi(h*$_{i9}$*)* A ^(0,m) A (V*_ < |/i|)(^(s,m) -> ^(x + l,m)) - *;(|A|,ro) (17)

Proof: Assume ft$_t$-(A,m) holds, then, since m ≤ *g,* we get from (13) that *j(|A|,<7,m) holds, i.e.

(Vz ≤ |<7|)(Vz*_< |,|)((z*_< z • *\h\) Aej(z,g,m)* - e^z'.y.m)).

Since *h* ≤ *g we* get for z = 1 and z* = |/i| that 0j(l,(/,m) —• 6j(|A|,flf, m). From this and the second conjunct of (9) we get 0j(|A|, <7,wi). For *x* = 0, y = |/i| we get ^j(0,m) —• ^j(|A|}m), and so the second conjunct of (9) implies ^(|/i|,m).

Recall that by our assumption the Ej — *LIND* induction axiom for the formula *<f>k* fails in *M*:

M }= «^$_t$(0,6) A (Vx)(*$_{fc}$(*. 6) - ^(a: + 1, 6)) A -.^(|o|, 6),

and that c was chosen so that a, 6 ≤ c. Thus, the above Claim implies that the set fi»(c) is a proper cut in *M* in particular, a ^ fit(c). Consequently, for all m G Af if m 6 *fti(c)* then m < c. From this and 17 we get

n,-(m, c) A fi,-(A, c) A ^(0, m) A (Vx < |/i|)(^(x, m) -, ^;(x + 1, m)) -> ^(|/i|, m). (18)

This, together with Lemma 6 implies that *fl{(c)* satisfies all the axioms of 5$^{i}_{2}$, which finishes our proof of Theorem 4. •

Other applications of the speed-up induction method can be found in [2], where it is used to demonstrate the unprovability of consistency statements in theories of bounded arithmetic, while in [9] it is used to establish the equivalence of certain axiomatizations of these theories.

Bibliography:

[I] Samuel R. Buss: Bounded Arithmetic. Bibliopolis, 1986.

[2] Samuel Buss and Aleksandar Ignjatović: *Unprovability of consistency statements in fragments of bounded arithmetic*, Technical Report CMU-PHIL-43, January 1994.

[3] Stephen Cook: *Feasibly constructive proofs and the propositional calculus*, in the Proceedings of the 7-th Annual ACM Symposium on Theory of Computing, 1975, pp. 83-97.

[4] Fernando J. I. Ferreira: *Polynomial time computable arithmetic*, in Contemporary Mathematics, Vol. 106 (1990) pp. 137-156.

[5] Fernando J. I. Ferreira: *Polynomial Time Computable Arithmetic and Conservative Extensions*, Ph.D. Thesis, The Pennsylvania State University, 1988.

[6] Fernando J. I. Ferreira: *Stockmeyer induction*, in S.R. Buss and P.J. Scott, ed. Feasible Mathematics, proceedings of the Mathematical Sciences Institute Workshop, Ithaca, New York, June 1989, Birkhäuser, 1990, pp. 161-180.

[7] P. Hájek, P. Pudlák: Metamathematics of first-order arithmetic, Springer-Verlag, 1992.

[8] Aleksandar Ignjatović: *Delineating classes of computational complexity via second order theories with weak set existence principles (I)*, Technical report CMU-PHIL-22, November 1991.

[9] Aleksandar Ignjatović: *Induction in theories of bounded arithmetic*, manuscript in preparation.

[10] Aleksandar Ignjatovic and Wilfried Sieg: *Herbrand analysis of some theories with weak set existence principles*, manuscript in preparation.

[II] Daniel Leivant, *A foundational delineation of computational feasibility*, draft, July 1991.

[12] Pavel Pudlák: *A note on bounded arithmetic*, **Fundamenta Mathematicae** 136 (1990) pp. 85-89.

[13] Robert Solovay: *Letter to P. Hdjek, August 1976.*

Department of Philosophy
Carnegie Mellon University
Pittsburgh, PA 15213, USA