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

by

Aleksandar Ignjatovič

November 1991

Report CMU-PHIL-22

Carnegie Mellon

Philosophy
Methodology
Logic

Pittsburgh, Pennsylvania 15213-3890

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

Aleksandar Ignjatović

November 5, 1991

Abstract

In this paper we characterize the well-known computational complexity classes of the Polynomial Time Hierarchy as classes of provable functions of some second order theories with weak comprehension. Our formalism is somewhat different from Leivant's, who was the first to introduce such a theory for delineating polynomial time computable functions. Besides being, in our view, foundationally advantageous, our formalism also has significant technical advantages: it enables us to characterize all the classes of the Polynomial Time Hierarchy within our theories and also to relate these theories very naturally to Buss' theories of bounded arithmetic 5^. The latter feature enables us to bypass both a complicated cut-elimination procedure or a difficult model-theoretic argument usually used to characterize provable functions of a theory, and a tedious proof of representability of functions from various complexity classes in the theories we consider, reducing both problems to such theorems about bounded arithmetic.

1 Introductory remarks-

Our work is motivated by Daniel Leivant's [4] pioneering work in introducing polynomial time computable functions in a theory with comprehension

***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. I am also grateful to my colleagues at the Philosophy Department at CMU for their continuous support.**

for open (quantifier-free) *positive* formulas; nevertheless, we choose to use a somewhat different foundational framework. Instead of using new functional symbols and Herbrand - Gödel equations to represent algorithms, we treat algorithms as definable partial functions, which is the more common way of investigating provably recursive functions of a theory. Not only does the formalism which corresponds to this foundational framework facilitate applications of results from bounded arithmetic, but we also believe that such a framework also has foundational advantages. Within the framework of set-theory, we define natural numbers in a highly impredicative way, as the intersection of all sets which contain the empty set and are closed for the successor function $S(x) = x \cup \{x\}$. On the other hand, complex algorithms on natural numbers are usually introduced in a very predicative way, using only previously defined and justified algorithms and already calculated values of the new algorithm; we never use the whole "graph" of the algorithm being introduced and being proved to be correct. We use notation and definitions from Buss' [1], Ferreira's [2] and Leivant's [4].

2 Base Theory $L_2^p(\overline{\Sigma}_0^b)$

In this paper we deal with the second order theories of binary strings. Unlike Leivant's theory $L_2(QF^+)$ which has a comprehension scheme restricted to *positive open* formulas on a language containing new functional symbols for the algorithms being considered, our base theory has the comprehension scheme for all *sharply bounded* formulas of a fixed language L_2^p, independent of the algorithm which we consider. Symbols of L_2^p include: a constant symbol ε for the empty string, the relation symbol $\preceq$ with the intended meaning "of smaller or equal length than", the relational symbol $\subseteq$ with the intended meaning "an initial segment of", the symbol for the membership relation $\in$, and a functional symbol for each polynomial-time computable function. In particular, L_2^p contains symbols S^0 and S^1 for the two successor functions which "concatenate 0 and 1" respectively at the end of a string. We have two kinds of variables; the first order ranging over strings and the second order ranging over sets of strings. We will use "real sets" rather than just elements of the domain for the second order variables in models of our theories; we will denote them by boldface letters. Thus, such objects do not have to be coextensive with any "internal" set in a model of one of our theories. Sharply bounded formulas (denoted as $\overline{\mathbf{\Sigma}}_{\mathbf{0}}^{\mathbf{b}}$ formulas) are defined similarly as in [2], i.e. they are the closure of atomic formulas under Boolean operations and sharply bounded quantifiers $(\forall x \subseteq t(\vec{y}))\varphi(x, \vec{y})$ and $(\exists x \subseteq t(\vec{y}))\varphi(x, \vec{y})$, where t is an arbitrary term of L_2^p. The only difference is that the set of atomic formulas also includes *second order* atomic formulas of the form $t(\vec{x}) \in X$. Notice that if a $\overline{\mathbf{\Sigma}}_{\mathbf{0}}^{\mathbf{b}}$ formula does not contain second order variables, then it defines a predicate which is polynomial-time decidable. We now define our base theory.

Definition 1 *$L_2^p(\overline{\Sigma}_0^b)$ is a theory of the language L_2^p which contains:*

1. *A few basic properties of common functions and predicates, like the successor functions, $x \oplus y$ (concatenation of the string y to the string x) and $x \otimes y$ (concatenation of the string x to itself length of y many times).*

2. ***Definitions of polynomial time computable functions*** *by limited recursion* ***and*** *composition, exactly as* ***given in Ferreira*** *'s [2].*

3. *Comprehension Axiom Schema:*

$$\mathbf{V\vec{F}V\vec{y}3XVx(x \text{ € } \mathit{X} \text{ «> } \mathit{<p\{\vec{x},y,\vec{Y}))}}$$

where <p is **$\overline{a}$ $£_0$** *formula* ***not containing variable X.***

Definition 2 *Let M be a model of L$(l?$_0$), and letC be the collection of all elements of the second order part of the domain of M, denoted by Set(Ai), (i.e. sets in the sense of A4), which contain the empty string and are closed under all functions f^M, for f £ L\. Thus, C is the collection of all elements V* ***e*** *Set(M) such that e* 6 *V and that for all $\vec{x}$ € V and any f 6 L\ also $f^M(x)$* ***$\vec{e}$*** *V. We then define* **W** *= {x\ for all X in C,x 6^M X}.*

Obviously W need not be the extension of any set in the sense of *M*; more over, since the collection *C* is a collection of objects closed under infinitely many functions, it is not clear that W is definable in *M* at all. Thus, to make our statements simpler, we add to the language *L* a first order unary predicate symbol *W(x)* and interpret it always as W defined above. The structure obtained in this way we denote by *M^w*. We will show that in fact W is definable in any theory containing ij$\overline{C\wedge o}$)-

We now prove two important properties of structures *M^w*, where *M* is a model of i^$\overline{C\wedge o}$)? ^{an}d *W(x)* is interpreted as above.

Lemma 1 *Let M^w be as above. Then*

(i)

$$M^w \ \backslash= \ \mathrm{Vx(Vy} \ \underline{C} \ x)(W(x) \rightarrow \boldsymbol{W(y)});$$

(ii) W *equals to the intersection of all sets which contain the empty string e and which are closed under the successor functions* $S°(x)$ *and* $S^x(x)$.

Proof: We use a trick that can be called "speed-up induction method"; it is the basis for quite a few of our proofs. Let *x Q y* denote the polynomial time function which cuts off the initial segment *y* of a segment x; if *y* is not an initial segment of x then *x Q y* equals the empty string. Also, let x © *y* denotes the string obtained by concatenating string *y* to the string x. Assume xo 6 W i.e. *W{XQ)* and let *T* be any set which contains the empty string *e* and is closed under both successor functions. Consider formula, denoted by 0(z,xo), given by

(Vx $\subseteq$ x_o)(Vy $\subseteq$ x_o)(y $\subseteq$ xA(x9y *1* *)A(V* $\subseteq$ *y){t* G f) - ^ (V* $\subseteq$ *x)(t € ?)).*

Let TO = 5^0(5°(...5°(£)...)), with m iterations of 5°(x).

Claim 1 *The following are true in* M^w:

(i)

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

(ii) *for arbitrary natural number m,*

$$\forall z(\Theta(z, x_0) — Q(z \circledast \underline{m}, x_0)).$$

Part (i) of the Claim follows immediately from the definition of 0. To prove (ii), assume 0(z,xo) and fix arbitrary substrings x and *y* of x_o such that *x Q y* $\leq$ *z* ®*m.* Consider the sequence to,^i, ...,^_m, such that t_0 = y, *U+i* = *U* © z, *i* <TO;we now apply TO times $0(z,x_o)$ to get (ii).

Coming back to the proof of Lemma 1 consider now formula $\Psi(w, x_0)$ given by

$(\forall z_1 \preceq x_0)(\forall z_2 \preceq x_0)(z_1$ -< z_2 A *(z2_<Zi®w)A* 0(*i,x$_o$) -> 0(*2,x$_0$)).

Recall that *x* ®*y* denotes the result of concatenating *x* to itself length of *y* many times, and is consequently an equivalent of the "smash" function of the "standard " bounded arithmetic.[1] Let also w^k = *w* ® *w*... ®*w,k* times, Kit.

Claim 2 *The following are true in* M^w

(i)

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

(ii) *for all natural numbers* &, m *and n,*

*(£, x$_0$) A Vw(¥(w, *x$_0$)* -+ *V((w^k* ® m) 0 n, x$_0$)),

To prove Claim 2, part (i) follows from the definition of $ and the corresponding property of 0; to prove (ii) notice that $(£,xo) holds trivially. Assume $(w;,xo), and let *z\\,z$_2$* and *w* be arbitrary elements such that the antecedent of the instance of the matrix of *ty((w^k* ® m) © ri, xo) holds. If length of *w* is 0 or 1, then the Claim we are proving follows from (ii) of Claim 1. If length of *w* is at least two, take *p* such that *(w^k* (g)TO)© *n* < tt;^{p}, and consider the sequence *Vo* = *z*, v,+i = *v$_x$*® iy, for 0 < *i* < *p*. Using *$(W,XQ)* we get 0(t>t,x$_o$) ~^ 0(^{v}t+i,x$_o$) for all *i* < p, which implies *#(w^p,x$_o$)*. Now we just use part (i) to get (ii) of our Claim.

---

[1] Of course 0, 0, ©, are defined by limited recursion and a few basic properties of them needed in our proof are included in part (1) of Definition 1.

Coming back to the proof of Lemma 1, we note that $\Theta(z, x_0)$ and $\Psi(w, x_0)$ are both $\overrightarrow{\Sigma}_0^b$ formulas; thus, there is an element X_Ψ in the second order part of the universe of $\mathcal{M}^W$ such that $\forall w(w \in X_\Psi \leftrightarrow \Psi(w, x_0))$. Claim 2 implies that X_Ψ belongs to $\mathcal{C}$, because $\varepsilon \in X_\Psi$ and for all $f \in L_2^p$ and any $\vec{w} \in X_\Psi$, $f(\vec{w}) \preceq ((max\{\vec{w}\})^k \otimes \underline{m}) \oplus \underline{n}$, for some natural numbers k, m and n. Consequently, by (i), $f(\vec{w}) \in X_\Psi$. Thus, the following holds in $\mathcal{M}^W$:

$$\forall x(W(x) \rightarrow x \in X_\Psi).$$

This implies $x_0 \in X_\Psi$, i.e. the following is true in $\mathcal{M}$:

$$(\forall z_1 \subseteq x_0)(\forall z_2 \subseteq x_0)(z_1 \subseteq z_2 \wedge (z_2 \preceq z_1 \otimes x_0) \wedge \Theta(z_1, x_0) \rightarrow \Theta(z_2, x_0)).$$

Take $z_2 = x_0$ and $z_1 = S^0(\varepsilon)$; then from the last formula

$$\mathcal{M}^W \models \Theta(S^0(\varepsilon), x_0) \rightarrow \Theta(x_0, x_0).$$

But $\Theta(S^0(\varepsilon), x_0)$ holds iff for all initial segments x and y of x_0

$$y \subseteq x \wedge (x \ominus y \preceq S^0(\varepsilon)) \wedge (\forall t \subseteq y)(t \in \mathcal{F}) \rightarrow (\forall t \subseteq x)(t \in \mathcal{F}),$$

which is true because of the fact that $\mathcal{F}$ is closed for the successor functions. Thus $\Theta(x_0, x_0)$ holds, i.e. for all initial segments x and y of x_0

$$y \subseteq x \wedge (x \ominus y \preceq x_0) \wedge (\forall t \subseteq y)(t \in \mathcal{F}) \rightarrow (\forall t \subseteq x)(t \in \mathcal{F}).$$

Taking the instance of $\Theta(x_0, x_0)$ with $x = x_0$, $y = \varepsilon$, and using that $\varepsilon \in \mathcal{F}$, we get $(\forall t \subseteq x_0)(t \in \mathcal{F})$. Since x_0 is an arbitrary element of **W** and $\mathcal{F}$ is an arbitrary set containing ε and closed for S^0 and S^1, this clearly implies both (i) and (ii) of our Lemma.

Corollary 1 *Set* **W** *is definable in any theory containing* $L_2^p(\overline{\Sigma}_0^b)$ *by the usual definition (see e.g. Leivant's [4])*

$$W(x) \equiv \forall Q(\varepsilon \in Q \wedge \forall y(y \in Q \rightarrow (S^0(y) \in Q \wedge S^1(y) \in Q)) \rightarrow x \in Q).$$

Thus, instead of having to speak model-theoretically about **W**, we can speak about theeory $L_2^p(\overline{\Sigma}_0^b)$ proving facts about $W(x)$, where $W(x)$ is the above formula. One of the most important such facts is the following immediate corollary of Lemma 1; it can be proved by induction on complexity of sharply bounded formulas where Lemma 1 is used to handle sharply bounded quantifiers.

Corollary 2 *All sharply bounded formulas are absolute between the universe and* **W**, *i.e. for any sharply bounded formula* φ,

$$L_2^p(\overline{\Sigma}_0^b) \vdash \forall \vec{x}(\bigwedge_{x_i \in \vec{x}} W(x_i) \rightarrow (\varphi(\vec{x}) \leftrightarrow \varphi^W(\vec{x}))).$$

Let $init(x, y)$ be the initial substring of x of length equal to the length of the string y, or just string x if $x \preceq y$.

Theorem 1 *(Induction in W) Let* φ *be a sharply bounded formula with free variables* $x, y_0, ..., y_n, Y_0, ..., Y_k$; *then* $L_2^p(\overline{\Sigma}_0^b)$ *proves*

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

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

Proof: The same as proof of Lemma 1, with $\varphi(t)$ in place of $t \in \mathcal{F}$. Notice that the only fact about the formula $t \in \mathcal{F}$ used in the proof was that it is a sharply bounded formula, that *e* G *T* and that (V* < *x)(init(x,t)* G *T* → ***init*($x, S^0(t)$) ∈ $\mathcal{F}$).**

Corollary 3 *L%(!?$_0$) interprets PTCA of Ferreira's [2].*

Proof: Recall that *PTCA* is basically like the first order part of Z£($\overline{\text{E}}$J), plus the Polynomial Induction Schema for sharply bounded formulas in the form *(p(s)* A *\/x((p(x)* -• *(<p(S°(x))* A *(p(S^1(x))))* -• Vxy>(x), where <p can have free variables besides x. We wiU show that l£($\overline{\text{s}}$j) h PTCA^{VK}. All universal axioms of *PTCA* are clearly true in *W.* To check the induction fix a xo in W. Notice that since W is closed for initial segments and since sharply bounded formulas are absolute (Corollary 2), induction relativized on W follows from

<p(e) A (V* < *x_o)(<p(init(x_o,t))* - *<p(init(x_0,S°(t)))* -> *<p(x_0).*

But this is clearly a consequence of Theorem 1.

Corollary 4 X5(2j) h Vx(Vy ^ ***x*)(*W*(*x*) → *W*(*y*)).**

Proof: Let again xo be an arbitrary element such that *W{XQ)* holds. Consider an arbitrary *y* such that *y* ⪯ so, and let ^* be an arbitrary set which contains the empty string *e* and is closed for successor functions; it is enough to show that *y* G *T.* But obviously

init(y,e) G *T* A (V* -< *x_o)(init(y,t) eT^ init(y,S°(t)) 6 T).*

Thus, since the formula *init(y,t)* £ *T* is sharply bounded, Theorem 1 implies *init(y,* x) G .F. Now we use *y* ⪯ *x* to conclude *y* £ *T.*

Corollary 4 implies that theory $L_2\wedge\overrightarrow{i\wedge o})$ h*^{8} ^{a} rice property that W is an initial segment of the universe not only in the sense that it is closed for taking the substrings of any string in W, but also for taking all strings of length smaller or equal to the length of a string in W. Thus, W is just a piece of the complete binary tree "up to" a certain height. Recall that W is closed under all functions of *L*. These two facts are extremely useful and have the following direct consequence.

Corollary 5 *In* $\wedge(\overrightarrow{S\,Q})$ ^{an}*V bounded formula (i.e. any formula obtained by closing first and second order atomic formulas for Boolean operations, sharply bounded quantifiers and bounded quantifiers) is absolute between* W *and the universe, i.e. for any such formula* $\wedge$(xo, ...£&),

$$L^*_2\{\%) \; h \; \nabla x(\bigwedge_{xi \in \vec{x}} W(xi) \; - \; (tff) \; - \; <p(g)^{w})).$$

We are now ready to characterize the levels of polynomial hierarchy as classes of provable functions of theories extending theory $Z\wedge\overrightarrow{\wedge o})$ by stronger comprehension and with an inductive definition of sequences which are "numbers".

3 Delineating The Polynomial Time Hierarchy

In order to delineate all the levels of the Polynomial Time Hierarchy we need stronger Comprehension Schema. Intuitively, stronger comprehension allows us to construct and prove correctness of algorithms which have more complex properties (recall that sets can be seen as extensions of properties in Frege's sense). This, on the other hand, can cause further restriction on what sequences are "numbers", because there might be more sets in C to intersect and get $\mathbf{W}$. Intuitively, this is not surprising. Recall that by our Corollary 4, in any theory extending $L_2^p(\overline{\Sigma}_0^b)$ the collection of "numbers" $\mathbf{W}$ is the collection of sequences of "sufficiently small" length. Some sequences, which could be treated as "numbers" for simpler algorithms, might be too long to allow more complex procedures definable in stronger theories to be correctly performed on them. Thus, to describe more complex algorithms, we need more properties (sets) rather than the *whole* first order universe satisfying more induction as is the case in theories of bounded arithmetic like S_2^i. We feel that when it comes to defining more complex computations, having more properties (sets) appears to be a more natural requirement than the requirement that whole universe satisfies more induction. Of course one can take cuts in models of S_2^1 which satisfy stronger theories of bounded arithmetic, but this is purely technical device with dubious foundational interpretation.

Definition 3 *The class of formulas* $\overline{\Sigma}_0^b(\Sigma_i^b)$ *is obtained as a closure for Boolean operations and sharply bounded quantifiers of the first* and second order *atomic formulas and* **arithmetic** *(i.e. without second order variables)* Σ_i^b *formulas.*[2]

Definition 4 $L_2^p(\overline{\Sigma}_0^b(\Sigma_i^b))$ *is the theory obtained from* $L_2^p(\overline{\Sigma}_0^b)$ *by adding the Comprehension Schema for* $\overline{\Sigma}_0^b(\Sigma_i^b)$ *formulas.*

[2]Arithmetic Σ_i^b formulas are first order formulas which have all quantifiers either bounded or sharply bounded, but only alternations of bounded quantifiers are counted. See, for example, Ferreira's [2].

Definition 5 *A function f mapping n-tuples of binary strings into binary strings is provable in $L_2^p(\overline{\Sigma}_0^b(\Sigma_i^b))$ if there is a Σ_i^b formula $\varphi_f(\vec{x}, y)$ such that*

$$L_2^p(\overline{\Sigma}_0^b(\Sigma_i^b)) \vdash \forall \vec{x}(\bigwedge_{x_i \in \vec{x}} W(x_i) \rightarrow \exists! y(W(y) \wedge \varphi_f(\vec{x}, y))),$$

and on the standard structure of binary strings $\forall \vec{x} \varphi_f(\vec{x}, f(\vec{x}))$ is true.

Note that by our absoluteness result (Corollary 5) the first condition is equivalent to

$$L_2^p(\overline{\Sigma}_0^b(\Sigma_i^b)) \vdash (\forall \vec{x} \exists! y \varphi_f(\vec{x}, y))^W.$$

Definition 6 *S_2^i is the "binary-string version" of fragments of bounded arithmetic as introduced by Buss [1], but on the language L^p which contains a functional symbol for each polynomial time computable function and relations $\subseteq$ and $\preceq$.*[3] *It can be obtained from Ferreira's PTCA by adding $\Sigma_i^b - PIND$. Here $\Sigma_i^b - PIND$ is the usual Polynomial Induction Schema, formulated for strings: $\varphi(\varepsilon, \vec{y}) \wedge \forall x(\varphi(x, \vec{y}) \rightarrow (\varphi(S^0(x), \vec{y}) \wedge \varphi(S^1(x), \vec{y}))) \rightarrow \forall x \varphi(x, \vec{y})$.*

Thus, Ferreira's $PTCA^+$ is in our notation S_2^1. Recall also that $\square_{i+1}^p$ is the collection of all functions computable in polynomial time with a Σ_i^b oracle.

[3] Despite the fact that in theories stronger than $L_2^p(\overline{\Sigma}_0^b)$ we do not need all symbols for the polynomial time computable functions but only those that correspond to the language of Buss' S_2^1 , we keep them for uniformity reasons. Their presence in the case of $L_2^p(\overline{\Sigma}_0^b)$ is crucial in order to have sufficiently strong induction in the domain **W** of "number-like" sequences of $L_2^p(\overline{\Sigma}_0^b)$. It is easy to see that our techniques of building models of theories with comprehension from models of bounded arithmetic and the main Theorem from Section 2 of Chapter 2 in Ferreira's [2] imply that restricting the language without adding more comprehension produces an unsuitably weak theory, in which not all polynomial time functions are provable. On the other hand, theory obtained from the theory $L_2^p(\overline{\Sigma}_0^b(\Sigma_1^b))$ by restricting its language so that it corresponds to the language of S_2^1, with $x \otimes y$ playing the role of the "smash" function $x \# y$, produces a theory of which $L_2^p(\overline{\Sigma}_0^b(\Sigma_1^b))$ is an extension by definitions.

Theorem 2 *Provable functions of L^^oi^)) are exactly U^1 functions. In particular, provable functions of* ZJJC^o) ore *exactly polynomial time computable functions.*

To prove this Theorem we need several lemmas.

Lemma 2 *Theory* Sj *is interpretable in the theory* Z£(E$_0$(S*)) *witfl* w *as the domain of interpretation; functions and relations of* 5£ *are interpreted as restrictions to* W *of the corresponding functions and relations of* $L_2^p(\overline{\Sigma}_0^b(\Sigma_i^b))$.

Proof: Obviously all universal axioms of 5^ hold relativized on W. Thus it suffices to show Z5(Ē£(l£)) h *(Z't-PIND)*™. The proof that this induction schema holds is again similar to the proof of Corollary 1, using the "speed-up induction method". First of all, our absoluteness result from Lemma 5 and the fact that W is closed for initial segments (Lemma 1) imply that it is enough to prove in i^^oC^!)) that for any x_0 € W,

<p(e,y) A (V* < x_o)(<p(init(x_o,t),y) - <p(init(x_o,S°(t)),y)) -> v>(*$_0$,ȳ).

Consider again *Q^(z,x_0)* given as

(Vx ⊆ x_o)(Vy ⊆ x_o)(y ⊆ x A (x 0 y ^) A (W ⊆ y)<p(t, ȳ) - (V« ⊆ x)ip(t, ȳ)),

and ^ (w , *xo)* given as

$$(\forall z_1 \subseteq x_0)(\forall z_2 \subseteq x_0)(z_1 \subseteq z_2 \wedge (z_2 \preceq z_1 \otimes w) \wedge \Theta_\varphi(z_1, x_0) \rightarrow \Theta_\varphi(z_2, x_0)).$$

The inductive hypothesis for *(p* implies that (V* < x_Q)(<p(init(x_0,t),ȳ) -± <p(init(x_o,S°(t)),y). On the other hand 0^ and 4^ are both sJ(Ej) formulas, and so we can apply an instance of the Comprehension Schema on

$^(it;,xo). An inspection of the proof of Lemma 1 shows that these are the only conditions needed to carry out the same kind of proof here.

Corollary 6 *For any formula a of the language of* $S^{\%}_{2}$, *if* $S\backslash$ •" & *then* $L_2^p(\overline{\Sigma_0^b}(\Sigma_i^b)) \vdash \sigma^W$.

The other direction is obtained in the following Lemma.

Lemma 3 *For any first order formula a, if* L5($\overline{E_0^b}$(S*)) •" <$?^W$, *then* S_2^i I- *a.*

Proof: Let *A* be any model of 5£. Consider the class of all subsets of *A* which are parametrically definable in *A* by £ô(S*) formulas, i.e. formulas which are the closure of £* formulas for Boolean operations and sharply bounded quantifiers.[4] This class of sets can be taken as the second order part *Set(A)* of the universe for a structure A^2 of the language *L* whose first order part of the universe is the universe of *A.* It is easy to see that A^2 satisfies axioms of Z?J($\overline{E_0^b}$(E*)) because £ô(£*) formulas are closed for Boolean operations and sharply bounded quantifiers. As it is well known, S^{l}_{2} proves induction for £ô(S*) formulas (see [3]). Thus, the only set containing the empty sequence and closed for successor functions in our collection of EQ(S{) parametrically definable sets is the whole universe. This implies that *W{x)* is true of any point *x* in the universe, and so for any first order formula cr, A^2 (= a^w if and only if *A* f= *a.* Thus, if S_2 ${}^iV^a$-> then for some *A* which

[4]**Notice that the only difference between £$(£•*) and $\overline{EQ}$(E?) 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 quantification.**

is **a** model **of Sj,** ***A*** \|= ***-KT,*** **and consequently also** A^2 ^ **-><r. But** this implies $L_2^p(\overline{\Sigma}_0^b(\Sigma_i^b)) \nvdash \sigma$.

In particular, we get the following Corollary.

Corollary 7 *Let <p be* a £* *formula, then*

$$L\wedge\wedge))!- \qquad (Vx3ly<p(x,y))^w$$

1/ *and only if*

$$S^{l'}_2 \vdash Vx3\,y<p(x,y).$$

The last Corollary and the fundamental result of Buss [1] clearly implies the claim of Theorem 2.

It is interesting to note that adding the $\overline{E}_2^b$ Comprehension Schema (i.e. the Comprehension Schema for all formulas obtained from the first and second order atomic formulas closing for Boolean operations, sharply bounded quantifiers and existential bounded quantifiers) to £2(^0) produces a theory (which we denote by X^C^i)) *n which every instance of the Comprehension Schema for bounded formulas is provable. This is because in this theory we can replace the inner-most bounded quantifier, say *(3x •≤ t{y))il)(x, y)* of any bounded formula *(p* with E$_2^b$ matrix *rp* (in the prenex normal form of *<p)* by *< yo,...,yk >€ X^,* where *X^* is obtained by applying an instance of the $\overline{S}_2^b$ Comprehension Schema. By our results above, this implies that if we add to our base theory $\overline{S}_{19}$ then W satisfies S2 (= Ut€u/ ^2) an(* so ^ functions from all levels of the Polynomial Time Hierarchy are provable in this theory. On the other hand, since any model of £2 can be expanded to a model of $L_2^p(\overline{\Sigma}_1^b)$ by adding all sets parametrically definable by bounded formulas (and again, due to induction schema, **W** is equal the whole universe), we get as before that provable functions of $L_2^p(\overline{\Sigma}_1^b)$ are exactly all functions from all levels of the Polynomial Time Hierarchy.

On the other hand, let $\overline{\Sigma}_1^{b+}$ 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*[5]. Consider a theory which besides the basic *first order* axioms has the Comprehension Schema for all $\overline{\Sigma}_1^{b+}$ formulas of L_2^p; denote it by $L_2^p(\overline{\Sigma}_1^{b+})$. Then provable 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 $\overline{\Sigma}_1^{b+}$ Comprehension (positiveness requirement is here crucial). Again, the only closed definable set which contains the empty string is the whole universe, and thus we get that for any model $\mathcal{A}$ of S_2^1 there is a model of $L_2^p(\overline{\Sigma}_1^{b+})$ with $\mathcal{A}$ as **W**. But this clearly implies that all provable functions of $L_2^p(\overline{\Sigma}_1^{b+})$ are provably total functions in S_2^1, and thus polynomial time computable.

References

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

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

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

[3] P. Hájek, P. Pudlák: *Metamathematics of first-order arithmetic*, the manuscript for a forthcoming book prepared at the Mathematical Institute in Prague, November 1990.

[4] Daniel Leivant, *A foundational delineation of computational feasibility*, Draft, July 1991.

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