

# Characterizing polynomial time computable functions using theories with weak set existence principles

Aleksandar Ignjatović and Phuong Nguyen

September 15, 2002

## Abstract

In this paper we define a sequence of second order theories (with one sort of variables ranging over natural numbers and another sort ranging over sets of natural numbers) whose provably recursive functions from **the domain of sets into sets** (with a naturally restricted complexity of the graphs) are exactly functions of the corresponding levels of polynomial hierarchy. In particular, the collection of provably recursive functions of the first theory of this sequence is exactly the class of polynomial time time computable functions. Our theories are most natural, without any special operations, capturing computational complexity classes using a weak comprehension principles for formulas of a simple and natural class, defined by purely set theoretic means. In this way we capture polynomial time computable functions using set theoretic definition without any concepts in any direct way related to polynomial time computability. This explains the “robustness” of the notion of polynomial time computability: it can be defined without any reference to any particular computational model, using “old” mathematical concepts unrelated to the notion of computation and unrelated to any explicit bound on resources. This work is a starting point for a project whose aim is to extend the notion of feasibility to arbitrary sets (of any cardinality) with a hope that such an extension will shed more light on the standard notion of feasibility for natural numbers, by considering feasible operations on infinite sets as limits of such operations on the standard, finite domain.

## 1 Introduction

We assume familiarity with Buss’s theories of bounded arithmetic  $S_2^i$ , see [1]. Our theories will have two sorts: (finite) sets  $X, Y, Z, \dots$  and numbers  $x, y, z, \dots$ . Operations and relations on numbers are  $+$ ,  $\cdot$ ,  $0, 1$  and  $\leq$  **only**. There is one operation mapping sets into numbers,  $/X/ = \max\{x : x \in X\} + 1$  if  $X$  is nonempty and with  $/\emptyset/ = 0$ , and the membership relation  $x \in X$ . First order quantifiers of the form  $\forall x \in X$ ,  $\forall x \leq y$  and the corresponding existential quantifiers are called *sharply bounded quantifiers*. Second order quantifiers of the form  $\forall X (/X/ \leq z)$  and  $\exists X (/X/ \leq z)$  are called *bounded quantifiers*. The hierarchies of bounded formulas are obtained as usual, by ignoring the sharply bounded quantifiers and counting only alternations of bounded quantifiers. Thus, a  $\Sigma_0^B$  formula is one which is logically equivalent to a formula which belongs to the least set

of formulas containing atomic and negated atomic formulas, closed for conjunctions, disjunctions and sharply bounded quantifiers; a  $\Sigma_{i+1}^B$  formula is one which is logically equivalent to a formula which belongs to the least set of formulas containing  $\Sigma_i^B$  and negated  $\Sigma_i^B$  formulas, closed for conjunctions, disjunctions, sharply bounded quantifiers and the existential bounded quantifier of the form  $\exists X(/X/ \leq z)$ .

Axioms of  $A^i$  consist of the basic properties of  $+, \cdot, 0, 1, =, \leq$  which are the axioms of bounded arithmetic  $S_2^i$  (see [1]), restricted to the language  $\{+, \cdot, 0, 1, =, \leq\}$ , plus

- extensionality

$$X = Y \leftrightarrow \forall x(x \in X \leftrightarrow x \in Y)$$

- finiteness:

$$\forall X \exists w \forall y(y \in X \rightarrow y < w)$$

- definition of the length function  $/X/$ :

$$x = /X/ \leftrightarrow (X = \emptyset \wedge x = 0) \vee (X \neq \emptyset \wedge \forall y \in X(y < /X/) \wedge \exists y \in X(y + 1 = /X/))$$

- the finite  $\Sigma_i^B$  comprehension axiom:

$$\exists X \forall x(x \in X \leftrightarrow x \leq z \wedge \varphi(x, \vec{Y}, \vec{y}))$$

for a  $\Sigma_i^B$  formula  $\varphi$  not containing variable  $X$ .

The least element principle:

$$X \neq \emptyset \rightarrow \exists x \in X(\forall z < x(z \notin X))$$

is a consequence of the finite  $\Sigma_i^B$  comprehension axiom and the defining axiom for the length function. This can be seen as follows. Given  $z \in X$ , form the set  $Y = \{x : x < z \wedge \forall u \leq x(u \notin X)\}$  then it is easy to show that  $/Y/$  is the minimal element in  $X$ .

We want to show that  $S_2^i$  is interpretable in  $A^i$  with the domain of sets as the domain of interpretation, as well as that  $A^i$  is interpretable in  $S_2^i$  with numbers as sets of  $A^i$  and with lengths of numbers as numbers of  $A^i$ .

**Theorem 1**  $A^i$  is interpretable in  $S_2^i$ .

**Proof:** Let  $\mathcal{N}$  be a model for  $S_2^i$  with domain  $N$ , we construct a model  $\mathcal{M}$  for  $A^i$  as follows. The domain of set of  $\mathcal{M}$  is the same as  $N$ , while the domain of numbers in  $\mathcal{M}$  is the image of  $N$  under the length function  $||$ . The relation  $x \in^{\mathcal{M}} X$  is defined as “ $x$  appears in the binary expansion of  $X$ ” which is definable by a  $\Delta_1^b$  formula (i.e.,  $x \in X \leftrightarrow \text{Bit}(x, X) = 1$ , see Buss 1986<sup>1</sup>). The length function  $//$  in  $\mathcal{M}$  is the same as the length function  $||$  in  $\mathcal{N}$ . Functions and relations on numbers of  $\mathcal{M}$  are the same as those in  $\mathcal{N}$ .

Extensionality and definition of length function are easily seen to hold. We need to show that the finite  $\Sigma_i^b$ -comprehension axiom is provable in  $S_2^i$ :

$$\exists X (/X/ \leq^{\mathcal{M}} z) \forall u (u \in^{\mathcal{M}} X \leftrightarrow u <^{\mathcal{M}} z \wedge \varphi(u, \vec{Y}, \vec{y}))$$

or in interpretation, taking into account that numbers get mapped into lengths:

$$\exists x (|x| \leq^{\mathcal{N}} |w|) \forall u (\text{Bit}(u, x) = 1 \leftrightarrow u <^{\mathcal{N}} |w| \wedge \varphi^*(u, \vec{h}, |\vec{g}|))$$

where  $\varphi^*$  is obtained from  $\varphi$  by interpretation. It is easy to show that if  $\varphi$  is  $\Sigma_i^B$ , then its interpretation is  $\Sigma_i^b$ .

The above formula is clearly equivalent to the formula

$$\exists x (|x| \leq^{\mathcal{N}} |w|) \forall u < |w| (\text{Bit}(u, x) = 1 \leftrightarrow u <^{\mathcal{N}} |w| \wedge \varphi^*(u, \vec{h}, |\vec{g}|))$$

which can be proved by using  $\Sigma_0^b(\Sigma_i^b) - PIND$  which holds in  $S_2^i$ , as follows. For  $w = 0$ , we can take  $x = 0$ . Now suppose that  $x$  is the witness for  $|w|$ . Then if  $\neg\varphi^*(|w|, \vec{v})$  holds then  $x$  is also the witness for  $|2w|$ . Otherwise, if  $\varphi^*(|w|, \vec{v})$  holds then  $2^{|w|} + x$  is the witness for  $|2w| = |w| + 1$ . Before we prove the main result which, together with the previous theorem implies that provably total functions of  $A^i$  which map sets into sets are exactly the polynomial time computable functions, we prove the following Lemma.

**Lemma 1** Set of numbers in  $A^i$  satisfies  $\Sigma_i^B$ -induction:

$$\varphi(0, \vec{X}, \vec{x}) \wedge \forall z < a (\varphi(z, \vec{X}, \vec{x}) \rightarrow \varphi(z + 1, \vec{X}, \vec{x}) \rightarrow (\varphi(a, \vec{X}, \vec{x}))$$

where

---

<sup>1</sup>bibtex entry

**Proof:**

Assume  $\varphi(0, \vec{X}, \vec{x})$  and  $\forall z(\varphi(z, \vec{X}, \vec{x}) \rightarrow \varphi(z+1, \vec{X}, \vec{x}))$ , and that  $\neg\varphi(a, \vec{X}, \vec{x})$ . Then by finite comprehension principle there exists the set  $W = \{x \mid x \leq a \wedge (\forall u \leq x)\varphi(u, \vec{X}, \vec{x})\}$ . Clearly  $a \notin W$  and  $W \neq \emptyset$  so  $0 < |W| \leq a$ . But then  $(\varphi(|W| - 1, \vec{X}, \vec{x}) \rightarrow \varphi(|W|, \vec{X}, \vec{x}))$  fails, which is a contradiction.

The above lemma allows us to use basic notions of bounded arithmetic, formulated using only multiplication, addition and inequality.

**Theorem 2**  $S_2^i$  is interpretable in  $A^i$ .

**Proof:** Let  $\mathcal{M}$  be an arbitrary model of  $A^i$  with the domain of numbers  $M_1$  and the domain of finite sets  $M_2$ . We construct a model  $\mathcal{N}$  for  $S_2^i$  as follows. The domain  $N$  of  $\mathcal{N}$  is the same as  $M_2$  where a number is identified with the finite set of numbers appearing as exponents in its binary expansion, and  $0^{\mathcal{N}}$  is defined to be the empty set  $\emptyset$ . We need now to define the functions and relations in  $\mathcal{N}$ .

$$X \# Y = \{ /X/ \cdot /Y/ \}$$

$$|X| = \{x : x \text{ appears as an exponent in the binary expansion of } /X/\}$$

This definition is correct because, by Lemma 1  $A^i$  satisfies enough induction to formalise the relation “appears in binary expansion of”.

$$\lfloor \frac{1}{2} X \rfloor = \{x - 1 : x > 0 \wedge x \in X\}.$$

We define the ordering on (finite) sets as the lexicographical ordering:

$$X <^{\mathcal{N}} Y \leftrightarrow X = \emptyset \vee (/Y/ > /X/) \vee (/Y/ = /X/ \wedge \exists y \in Y (y \notin X \wedge \forall z < /Y/ (z > y \rightarrow (z \in X \leftrightarrow z \in Y))))$$

and

$$X \leq^{\mathcal{N}} Y \leftrightarrow X = Y \vee X <^{\mathcal{N}} Y$$

Successor is defined as a “bit-wise” operation:

$$\begin{aligned} Y = S(X) \leftrightarrow & (\forall x < /X/ (x \in X \wedge /X/ \in Y \wedge \forall z \in Y (z = /X/)) \vee \\ & (/X/ = /Y/ \wedge \exists y \in Y (y \notin X \wedge \forall x < y (x \in X \wedge x \notin Y) \wedge \\ & \forall z < /Y/ (z > y \rightarrow (z \in X \leftrightarrow z \in Y)))) \end{aligned}$$

Addition is defined “by recursion on bits” using the standard algorithm for summation of numbers written in binary, with an auxiliary set  $W$  encoding the carry:

$$\begin{aligned}
X +^N Y = Z \leftrightarrow & \exists W (/W/ \leq /X/ + /Y/ + 1)(0 \notin W \wedge \forall u \leq /X/ + /Y/ \\
& ((u \in X \wedge u \in Y \wedge u \in W \rightarrow u \in Z \wedge u + 1 \in W) \wedge \\
& (u \notin X \wedge u \in Y \wedge u \in W \rightarrow u \notin Z \wedge u + 1 \in W) \wedge \\
& (u \in X \wedge u \notin Y \wedge u \in W \rightarrow u \notin Z \wedge u + 1 \in W) \wedge \\
& (u \in X \wedge u \in Y \wedge u \notin W \rightarrow u \notin Z \wedge u + 1 \in W) \wedge \\
& (u \notin X \wedge u \notin Y \wedge u \in W \rightarrow u \in Z \wedge u + 1 \notin W) \wedge \\
& (u \notin X \wedge u \in Y \wedge u \notin W \rightarrow u \in Z \wedge u + 1 \notin W) \wedge \\
& (u \in X \wedge u \notin Y \wedge u \notin W \rightarrow u \in Z \wedge u + 1 \notin W) \wedge \\
& (u \notin X \wedge u \notin Y \wedge u \notin W \rightarrow u \notin Z \wedge u + 1 \notin W) \wedge \\
& (u > /X/ + 1 \wedge u > /Y/ + 1 \rightarrow u \notin))
\end{aligned}$$

We will use the pairing function (on numbers of  $\mathcal{M}$ ):

$$\langle x, y \rangle = \lfloor \frac{1}{2}((x^2 + y^2 + 2xy + x + 1) \div y) \rfloor$$

Multiplication is also defined as a bitwise operation, using the standard multiplication algorithm. Note that the way that we normally carry out the multiplication is to add the rows of either a  $/X/ \times (/X/ + /Y/ - 1)$  matrix or a  $/Y/ \times (/X/ + /Y/ - 1)$  matrix. To make multiplication commutative directly by its definition, we “stretch out” these matrices to a  $Max\{/X/, /Y/\} \times (/X/ + /Y/ - 1)$  matrix. First we introduce some auxiliary operations as follows

$$\begin{aligned}
X \times Y = P \iff & (\forall x < /X/)(\forall y < /Y/)(\forall z < /Y/ + /Y/ - 1)(\forall u < Max\{/X/, /Y/\}) \\
& (\langle u, z \rangle \in P \leftrightarrow (y \in Y \wedge x \in X) \wedge z = x + y \wedge u = Max\{x, y\})
\end{aligned}$$

$P$  can be seen as a  $Max\{/X/, /Y/\} \times (/X/ + /Y/ - 1)$  matrix of digits, where the presence of  $\langle z, w \rangle$  in  $P$  indicate the bit 1 at the position  $(z, w)$ . We now define another auxiliary operation which sums the members of  $P$  seen as exponents of powers of 2:

$$X \otimes Y = Q \iff \langle 0, 0 \rangle \in Q \leftrightarrow \langle 0, 0 \rangle \in P \wedge (\forall u < Max\{/X/, /Y/\})$$

$$(u > 0 \rightarrow \{w|w < /X/ + /Y/ \wedge \langle u, w \rangle \in Q\} = \\ \{w|w < /X/ + /Y/ \wedge \langle u - 1, w \rangle \in Q\} + \{z|z < /X/ + /Y/ \wedge \langle u, z \rangle \in P\})$$

Finally

$$X \cdot^{\mathcal{N}} Y = \{z : \langle \text{Max}\{/X/, /Y/\}, z \rangle \in X \otimes Y\} \quad (1)$$

It is routine to check that all axioms of  $S_2^i$  are satisfied with this interpretation. For convenience, we omit the superscripts  $\mathcal{M}$  and  $\mathcal{N}$  for the functions and relations when it is clear from the context.

**Remark:** For an  $x \in M_1$ , denote by  $\text{Bin}(x)$  the set  $\{i : i \text{ appears in the binary representation of } x\}$ . Let  $x, y$  be numbers in  $\mathcal{M}$  then it is easy to check that  $\text{Bin}(x) +^{\mathcal{N}} \text{Bin}(y) = \text{Bin}(x + y)$  and  $\text{Bin}(x) \cdot^{\mathcal{N}} \text{Bin}(y) = \text{Bin}(x \cdot y)$ .

Details of the proofs for BASIC are as follows.

1.  $Y \leq X \rightarrow Y \leq S(X)$ . It is straightforward from the definition of  $<$  (i.e.,  $<^{\mathcal{N}}$ ) above that  $X < S(X)$ . Thus, the formula follows from transitivity of  $\leq$  below.
2.  $X \neq S(X)$ . This is trivial.
3.  $0^{\mathcal{N}} \leq X$ . From the definition of  $\leq$  above.
4.  $X \leq Y \wedge X \neq Y \leftrightarrow S(X) \leq Y$ .

Let  $Z = S(X)$ . For the “only if” direction, suppose first that

$$\forall x < /X/ x \in X \wedge /X/ \in Z \wedge \forall z \in Z (z = /X/)$$

Since  $Y > X$ , in this case we must have  $/Y/ > /X/$ . Now either  $/Y/ > /X/ + 1$ , in which case let  $y_0 = /Y/ - 1$  and we have

$$y_0 \in Y \wedge y_0 \notin Z \wedge \forall y < /Y/ (y > y_0 \rightarrow (y \in Z \leftrightarrow y \in Y))$$

or  $/Y/ = /X/ + 1$ , in that case  $/X/ \in Y$ , and it is trivial to check that either  $Y = \{/X/\}$  (therefore  $Y = Z$ ) or  $\exists y_0 \in Y (y_0 \neq /X/)$  (and therefore  $Y > Z$ ).

Suppose now that

$$/X/ = /Z/ \wedge \exists z_0 \in Z (z_0 \notin X \wedge \forall x < z_0 (x \in X \wedge x \notin Z) \wedge \forall w < /Z/ (w > z_0 \rightarrow (w \in X \leftrightarrow w \in Z)))$$

If  $/Y/ > /X/$ , then  $/Y/ > /Z/$ , qed. Otherwise, if  $/Y/ = /X/$  and

$$\exists y_0 \in Y \wedge y_0 \notin X \wedge \forall y < /Y/ (y > y_0 \rightarrow (y \in X \leftrightarrow y \in Y))$$

If  $y_0 > z_0$  then since  $y_0 \notin X$  we have  $y_0 \notin Z$ , thus

$$y_0 \in Y \wedge y_0 \notin Z \wedge \forall y < /Y/ (y > y_0 \rightarrow (y \in Z \leftrightarrow y \in Y))$$

and hence  $Y > Z$ . If  $y_0 = z_0$  then either  $\exists a \in Y (a < z_0)$ , in that case

$$a \in Y \wedge a \notin Z \wedge \forall y < /Y/ (y > a \rightarrow (y \in Z \leftrightarrow y \in Y))$$

and therefore  $Z < Y$ , or  $\forall z < z_0 (z \notin Y)$ , in that case  $Z = Y$ . Otherwise  $y_0 < z_0$  then  $y_0 \notin Z$  and hence

$$y_0 \in Y \wedge y_0 \notin Z \wedge \forall y < /Y/ (y > y_0 \rightarrow (y \in Z \leftrightarrow y \in Y))$$

Thus we have proved that  $Y \geq Z$ .

For the reverse direction, suppose first that

$$\forall x < /X/ (x \in X \wedge /X/ \in Z) \wedge \forall z \in Y (z = /X/)$$

then  $/Z/ > /X/$ , and since  $Z < Y$  we have  $/Y/ \geq /Z/$ , thus  $/Y/ > /X/$  and therefore  $Y > X$ .

Now suppose that

$$/X/ = /Z/ \wedge \exists z_0 \in Z (z_0 \notin X \wedge \forall x < z_0 (x \in X \wedge x \notin Z) \wedge \forall w < /Z/ (w > z_0 \rightarrow (w \in X \leftrightarrow w \in Z)))$$

If  $Y = Z$  then it is trivial that  $Y > X$ . Suppose that  $Y > Z$ . If  $/Y/ > /Z/$  then  $/Y/ > /X/$ , qed. Otherwise,

$$/Y/ = /Z/ \wedge \exists y_0 \in Y (y_0 \notin Z \wedge \forall z < /Y/ (z > y_0 \rightarrow z \in Z \leftrightarrow z \in Y))$$

If  $y_0 < z_0$  then since  $z_0 \in Z$  we have  $z_0 \in Y$ , and thus

$$/Y/ = /X/ \wedge z_0 \in Y \wedge z_0 \notin X \wedge \forall y < /Y/ (y > z_0 \rightarrow (y \in X \leftrightarrow y \in Y))$$

Otherwise if  $y_0 > z_0$  then since  $y_0 \notin Z$ ,  $y_0 \notin X$ , and thus

$$/Y/ = /X/ \wedge y_0 \in Y \wedge y_0 \notin X \wedge \forall y < /Y/ (y > y_0 \rightarrow (y \in X \leftrightarrow y \in Y))$$

5.  $X \neq 0^{\mathcal{N}} \rightarrow 2^{\mathcal{N}}X \neq 0^{\mathcal{N}}$ . This follows from the fact that  $2^{\mathcal{N}}X = \{x + 1 | x \in X\}$ , which is easy to prove.

6.  $Y \leq X \vee X \leq Y$ . Suppose  $\neg(X < Y)$ , then

$$X \neq \emptyset \wedge (/Y/ \leq /X/) \wedge (/Y/ \neq /X/ \vee \forall y \in Y (y \in X \vee \forall z \leq /Y/ (z > y \wedge \neg(z \in X \leftrightarrow z \in Y))))$$

Thus if  $/Y/ \neq /X/$  then  $/Y/ < /X/$  and therefore  $Y < X$ . Otherwise we have

$$/Y/ = /X/ \wedge \forall y \in Y (y \in X \vee \forall z \leq /Y/ (z > y \wedge \neg(z \in X \leftrightarrow z \in Y)))$$

If for all  $y \in Y$  we have  $y \in X$  then clearly  $Y \leq X$ . Otherwise, let  $y_0$  be the largest element of  $Y$  such that  $y_0 \notin X$ , then we have  $\forall y \in Y (y > y_0 \rightarrow y \in X)$ . Also,  $\exists z \leq /Y/ (z > y_0 \wedge \neg(z \in Y \leftrightarrow z \in X))$ . Let  $z_0$  be the largest such number, then we have  $z_0 \in X \wedge z_0 \notin Y$ , and

$$z_0 \in X \wedge z_0 \notin Y \wedge \forall z \leq /Y/ (z > z_0 \rightarrow z \in X \leftrightarrow z \in Y)$$

Thus  $Y < X$ .

7.  $X \leq Y \wedge Y \leq X \rightarrow X = Y$ . If  $X = \emptyset$  then since  $Y \leq X$ ,  $Y = \emptyset$ , and thus  $X = Y$ .

Similarly, if  $Y = \emptyset$  then  $X = Y$ . Now suppose that  $X, Y \neq \emptyset$  and that  $X \neq Y$ . Then we have  $/X/ = /Y/$  and

$$\begin{aligned} \exists y_0 \in Y (y_0 \notin X \wedge \forall z \leq /Y/ (z > y_0 \rightarrow z \in X \leftrightarrow z \in Y)) \\ \exists x_0 \in X (x_0 \notin Y \wedge \forall z \leq /X/ (z > x_0 \rightarrow z \in Y \leftrightarrow z \in X)) \end{aligned}$$

Comparison of  $x_0$  and  $y_0$  leads to contradiction.

8.  $X \leq Y \wedge Y \leq Z \rightarrow X \leq Z$ . This is trivial from the definition.

9.  $|0^{\mathcal{N}}| = 0^{\mathcal{N}}$ . This is trivial from the definition.

10.  $X \neq 0^{\mathcal{N}} \rightarrow |2^{\mathcal{N}} \cdot^{\mathcal{N}} X| = S(|X|) \wedge |2^{\mathcal{N}} X +^{\mathcal{N}} 1^{\mathcal{N}}| = S(|X|)$ . We have  $2^{\mathcal{N}} = \{1\}$ , and it is easy to check that in the definition of  $\cdot^{\mathcal{N}}$ ,

$$\begin{aligned} 2^{\mathcal{N}} \times X &= \{\langle x, 1 + x \rangle : x \in X\} \\ 2^{\mathcal{N}} \otimes X &= \{\langle x, 1 + x \rangle : x \in X\} \end{aligned}$$

and so

$$\begin{aligned} 2^{\mathcal{N}} \cdot^{\mathcal{N}} X &= \{1 + x : x \in X\} \\ 2^{\mathcal{N}} \cdot^{\mathcal{N}} X +^{\mathcal{N}} 1^{\mathcal{N}} &= \{0\} \cup \{1 + x : x \in X\} \end{aligned}$$

Thus  $|2^{\mathcal{N}} \cdot^{\mathcal{N}} X| = |X| + 1$  (as number addition) and so  $|2^{\mathcal{N}} \cdot^{\mathcal{N}} X| = S(|X|)$  by the remark (qed).

11.  $|1^{\mathcal{N}}| = 1^{\mathcal{N}}$ . This is trivial from definition.

12.  $X \leq Y \rightarrow |X| \leq^{\mathcal{N}} |Y|$ . This is trivial from definition and the remark.

13.  $|X \# Y| = S(|X| \cdot^{\mathcal{N}} |Y|)$ . Since  $X \# Y = \{ /X / \cdot / Y / \}$  we have (by definition of  $||$ )  $|X \# Y| = /X / \cdot / Y / + 1$

Other open (or universal) axioms are proved in a similar manner;  $\Sigma_i^b - PIND$  follows easily from  $\Sigma_i^B$  finite comprehension. (see Lemma 1)

Our main theorem easily follows from the above.

**Theorem 3** *Provably total functions of  $A^1$  with  $\Sigma_1^B$  graphs are exactly polynomial time computable functions, i.e.,*

$$A^i \vdash \forall X \exists Y \varphi(X, Y)$$

for a  $\Sigma_1^B$  formula  $\varphi(X, Y)$  if and only if there exists a polynomial time computable function  $f(X)$  such that

$$\mathcal{P}(N) \models \varphi(X, f(X))$$

**Proof:** Immediately from the corresponding fact for  $S_2^1$  and our interpretability results.

Note that the above result is more natural than those in [2] and [3], since we do not have  $\#$  operation or product of strings which is introduced to capture polynomial growth rate. Nothing in our theories is in any way related to polynomial time computability; all operations and relations as well as complexity classes are general set theoretic notions studied in contexts other than polynomial time computability. This indicates how fundamental polynomial time computable functions are.

## References

- [1] Samuel R. Buss, Bounded Arithmetic, Bibliopolis 1986.
- [2] Aleksandar Ignjatovic, Delineating computational complexity classes via second order theories with weak set existence principles. I, The Journal of Symbolic Logic, Volume 60, Number 1, March 1995,
- [3] Daniel Leivant, A foundational delineation of computational feasibility, LICS 1991 2-11.

School of Computer Science and Engineering

University of New South Wales

Sydney, NSW 2052, Australia