CATS 2003 Preliminary Version

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

Aleksandar Ignjatovic [1]

School of Computer Science and Engineering
University of New South Wales, Sydney, Australia

Phuong Nguyen [2]

School of Computer Science and Engineering
University of New South Wales, Sydney, Australia
and
Department of Computer Science,
University of Toronto, Toronto, Canada

Abstract

Several authors have independently introduced second order theories whose provably total functionals are polynomial time computable functions on strings (e.g. [4], [6] and [7]), including the first author ([3], meant to be the second part of [2]). In this paper we give a detailed proof of the bi-interpretability result between such a second order theory and Buss' first order bounded arithmetic, based on an elegant definition of multiplication due to the second author.

1 Introduction

In this paper we consider 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 the polynomial hierarchy. In particular, the collection of provably recursive functions of the first theory of this sequence is exactly the class of polynomial time computable functions. These theories are most natural, without any special operations, capturing

[1] Email: `ignjat@cse.unsw.edu.au`
[2] Email: `ntp@cs.toronto.edu`

This is a preliminary version. The final version will be published in
Electronic Notes in Theoretical Computer Science
URL: `www.elsevier.nl/locate/entcs`

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 polynomial time computable functions are captured using set theoretic definitions without any concepts in any direct way related to polynomial time computability. Unlike the approaches to feasibility via weak set existence principles of [2] and [5], here the domain of feasible functions is the domain of second order variables, while the domain of first order variables is the auxiliary one. This approach provides a suitable 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 polynomial time computability.

2 Technical Preliminaries

We assume familiarity with Buss's theories of bounded arithmetic S_2^i, see [1]. Our theories will have two sorts: (finite) sets $X, Y, Z, \ldots$ and numbers $x, y, z, \ldots$. 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 Σ_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 Σ_{i+1}^B formula is one which is logically equivalent to a formula which belongs to the least set of formulas containing Σ_i^B and negated Σ_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 $\{+, \cdot, 0, 1, =, \leq\}$ ($<$ can be taken as symbol defined from $\leq$), 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 Σ_i^B comprehension axiom:

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

for a Σ_i^B formula φ not containing variable X.

Clearly the finite Σ_i^B comprehension principle implies comprehension principle for arbitrary Boolean combinations of Σ_i^B formulas (and, with a little more work, one can add closure for sharply bounded quantifiers as well).

The least element principle:

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

is a consequence of the finite Σ_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.

3 Bi-interpretability

Theorem 3.1 *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 Δ_1^b formula (i.e., $x \in X \leftrightarrow Bit(x, X) = 1$, see [1]). 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 Σ_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:

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

where φ^* is obtained from φ by interpretation. It is easy to show that if φ is Σ_i^B, then its interpretation is Σ_i^b.

The above formula is clearly equivalent to the formula

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

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 3.2 *Set of numbers in A^i satisfies Σ_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 φ is a Σ_i^B formula.

Proof:

As usual, it is enough to prove Π_1^B induction principle. Assume $\varphi(0,\vec{X},\vec{x})$ and $\forall z < a(\varphi(z,\vec{X},\vec{x}) \rightarrow \varphi(z+1,\vec{X},\vec{x}))$, and that $\neg\varphi(a,\vec{X},\vec{x})$. Then by finite comprehension principle there exists the set

$$W = \{x : x \leq a \wedge (\forall u \leq x)\varphi(u,\vec{X},\vec{x})\}$$

because $(\forall u \leq x)\varphi(u,\vec{X},\vec{x})$ is also a Π_1^B formula. 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 3.3 *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 $\mathcal{N}$.

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

$|X| = \{x : x$ appears as an exponent in the binary expansion of $/X/\}$
This definition is correct because, by Lemma 3.2 A^i satisfies enough induction to formalise the relation "appears in binary expansion of".

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

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

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

and

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

Successor is defined as a "bit-wise" operation:

$$Y = S(X) \leftrightarrow (/Y/ \leq /X/ + 1) \land \exists x \leq /X/[x \notin X \land \\ (\forall y < x(y \in X \land y \notin Y)) \land (\forall y \leq /X/(x < y \to (y \in X \leftrightarrow y \in Y))]$$

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 carries:

$$X +^{\mathcal{N}} Y = Z \leftrightarrow \exists W (/W/ \leq /X/ + /Y/) Sum(X, Y, Z, W)$$

where $Sum(X, Y, Z, W)$ stands for

$$0 \notin W \land (\forall u \leq /X/ + /Y/) CarryAdder(u, X, Y, Z, W)$$

and $CarryAdder(u, X, Y, Z, W)$ stands for the formula specifying the bit–wise addition rule to add the u^{th} bits of X and Y with carry in W. Details are as follows:

$$CarryAdder(u, X, Y, Z, W) \leftrightarrow \\ (u \in X \oplus u \in Y \oplus u \in W \leftrightarrow u \in Z) \land \\ ((u \in X \land u \in Y) \lor (u \in X \land u \in W) \lor (u \in Y \land u \in W) \leftrightarrow u + 1 \in W)$$

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

$$\langle x, y \rangle = (x + y)(x + y + 1) + x$$

We now define multiplication. 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 the mulplication symmetric with respect to X and Y, we "stretch out" these matrices to a $(2/X//Y/) \times (/X/ + /Y/)$ matrix. First we introduce some auxiliary operations as follows

$$z \in X \times Y \leftrightarrow \exists x \in X \exists y \in Y (z = \langle xy, x + y \rangle \lor \\ (x \neq y \land x \in Y \land y \in X \land z = \langle xy + /X//Y/, x + y \rangle))$$

$X \times Y$ can be seen as a $(2/X//Y/) \times (/X/ + /Y/)$ matrix of digits, where the presence of $\langle z, w \rangle$ in $X \times Y$ indicate the bit 1 at the position (z, w). We now define the sum of the rows in $X \times Y$:

$$X \otimes Y = Q \leftrightarrow (\forall z \leq /X/ + /Y/)(\langle 0, z \rangle \in Q \leftrightarrow \langle 0, z \rangle \in P) \land \\ \forall u \leq 2/X//Y/(0 \leq u \to Row(u, Q) +^{\mathcal{N}} Row(u + 1, P) = Row(u + 1, Q))$$

where $P = X \times Y$. Here $Row(x, X)$ stands for $\{y : y \leq /X/ \land \langle x, y \rangle \in X\}$. Finally

$$X \cdot^{\mathcal{N}} Y = Row(2/X/./Y/, X \otimes Y)$$

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 1: For an $x \in M_1$, denote by $Bin(x)$ 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

$$\begin{aligned} Bin(x) + Bin(y) &= Bin(x + y) \\ Bin(x) \cdot Bin(y) &= Bin(x.y) \\ x \le y \to Bin(x) &\le Bin(y) \end{aligned}$$

Remark 2: $1^{\mathbb{N}} = S0 = \{0\}$
Remark 3: $S(X) = X + S0$
Remark 4: $\{a\} \cdot X = \{a + x : x \in X\}$
Remark 5: $2^{\mathbb{N}} = SS0 = \{1\}$

Details of the proofs for BASIC are as follows.

1 $Y \le X \to Y \le S(X)$: It is straightforward from the definition of $<$ (i.e., $<^{\mathbb{N}}$) above that $X < S(X)$. Thus, the formula follows from transitivity of $\le$ below.

2 $X \ne S(X)$: This is trivial.

3 $0 \le X$: From the definition of $\le$ above.

4 $X \le Y \wedge X \ne Y \leftrightarrow S(X) \le Y$:
Let $Z = S(X)$. Let $x_0 \le /X/$ be such that $x_0 \notin X$ and

$$\forall x < x_0 (x \in X \wedge x \notin Z) \wedge \forall x \le /X/ (x_0 < x \to (x \in X \leftrightarrow x \in Z))$$

For the "only if" direction, let $y_0 \in Y$ be such that $y_0 \notin X$ and

$$\forall z \le /Y/ (y_0 < z \to (z \in X \to z \in Y))$$

then since $\forall x < x_0 (x \in X)$ it follows that $x_0 \le y_0$, hence $Z \le Y$.

For the reverse direction, it is trivial that $X < S(X)$. Thus it follows from transitivity (8) of $\le$ that $X \le Y$. Also, it follows from (2) and (7) that $X \ne Y$.

5 $X \ne 0 \to 2 \cdot X \ne 0$: This follows from remark 4.

6 $Y \le X \vee X \le Y$: Suppose $\neg(X < Y)$, then $\neg(/X/ < /Y/)$ and

$$/Y/ < /X/ \vee \forall y \in Y (y \in X \vee \exists z \le /Y/ (y < z \wedge z \in X \wedge z \notin Y))$$

If $/Y/ < /X/$ then $Y < X$. Otherwise we have

$$/Y/ = /X/ \wedge \forall y \in Y (y \in X \vee \exists z \le /Y/ (y < z \wedge z \in X \wedge z \notin Y))$$

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

$$\forall y \in Y(y > y_0 \to y \in X)$$

Also

$$\exists z \leq /Y/(y_0 < z \wedge z \in X \wedge z \notin Y)$$

Let z_0 be the largest such number, then we have $z_0 \in X \wedge z_0 \notin Y$, and hence

$$z_0 \in X \wedge z_0 \notin Y \wedge \forall z \leq /Y/(z_0 < z \to (z \in Y \leftrightarrow z \in X))$$

Thus $Y < X$.

7 $X \leq Y \wedge Y \leq X \to X = Y$: If $X = \emptyset$ then since $Y \leq X$, $Y = \emptyset$, and hence $X = Y$. 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

$$\exists y_0 \in Y(y_0 \notin X \wedge \forall z \leq /Y/(z > y_0 \to (z \in X \to z \in Y)))$$

$$\exists x_0 \in X(x_0 \notin Y \wedge \forall z \leq /X/(z > x_0 \to (z \in Y \to z \in X)))$$

Comparison of x_0 and y_0 leads to contradiction.

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

9 $|0| = 0$: This is trivial from the definition.

10 $X \neq 0 \to |2 \cdot X| = S(|X|) \wedge |2 \cdot X + 1| = S(|X|)$: From remark 4:

$$2 \cdot X = \{1 + x : x \in X\} \text{ and } 2 \cdot X + 1 = \{0\} \cup \{1 + x : x \in X\}$$

Therefore $|2 \cdot X| = Bin(/X/ + 1) = Bin(/X/) + Bin(1) = |X| + S0 = S(|X|)$ by remark 3. Also, $|2 \cdot X + 1| = |2 \cdot X|$ and hence $|2 \cdot X + 1| = S(|X|)$ (qed).

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

12 $X \leq Y \to |X| \leq^{\mathbb{N}} |Y|$: Suppose $X \leq Y$, by definition we have $/X/ \leq /Y/$. The conclusion then follows from remark 1.

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

14 $0\#Y = 1$: We have $0\#Y = \{0./Y/\} = \{0\} = 1$ (qed).

15 $X \neq 0 \to 1\#(2 \cdot X) = 2 \cdot (1\#X) \wedge 1\#(S(2 \cdot X)) = 2 \cdot (1\#X)$: We have (from remark 4) $1\#(2 \cdot X) = \{1(1 + /X/)\} = \{1 + /X/\}$ and $2 \cdot (1\#X) = 2 \cdot \{/X/\} = \{1 + /X/\}$. Also $1\#(S(2 \cdot X)) = \{1(1 + /X/)\} = \{1 + /X/\}$ (qed).

16 $X\#Y = Y\#X$: This is trivial from the definition.

17 $|X| = |Y| \to X\#Z = Y\#Z$: This is trivial.

18 $|X| = |U| + |V| \to X\#Y = (U\#Y) \cdot (V\#Y)$: From the definition:

$$U\#Y = \{/U//Y/\}, V\#Y = \{/V//Y/\}$$

From remark 4 we have

$$(U\#Y) \cdot (V\#Y) = \{/U//Y/ + /V//Y/\} = \{(/U/ + /V/)/Y/\}$$

Also, it follows from remark 1 that $/X/ = /U/ + /V/$ (qed).

19 $X \leq X + Y$: Let $Z = X + Y$ and W such that $Sum(X, Y, Z, W)$ (see definition of $+^{\mathcal{N}}$). If $Y = 0$ then $X+Y = X$. Otherwise, let $z = max(Y \cup W)$. Since $z \geq max(W)$ it follows that z belongs to exactly one of X, Y, W. Therefore $z \notin X$ and also $z \in Z$. In addition, for all $x > z$ we have $x \notin Y, x \notin W$, hence $x \in X \to x \in Z$. Thus $X \leq X + Y$ (qed).

Remark 6 $Y \neq 0 \to X < X + Y$.

20 $X < Y \to S(2 \cdot X) < 2 \cdot Y$: From remarks 2,3,4,5 we have $S(2 \cdot X) = \{0\} \cup \{1 + x : x \in X\}$. The conclusion then follows from definition of $<^{\mathcal{N}}$.

21 $X + Y = Y + X$: From definition of $+^{\mathcal{N}}$.

22 $X + 0 = X$: From definition of $+^{\mathcal{N}}$.

23 $X + SY = S(X + Y)$: This follows from number 21, 24 and remark 3.

24 $(X + Y) + Z = X + (Y + Z)$: We prove by induction on w that

$$\begin{aligned}
&w \in (X + Y) + Z \leftrightarrow \\
&\quad \exists W(/W/ \leq w + 1)\exists U_1(/U_1/ \leq w + 1)\exists U_2(/U_2/ \leq w + 1)[\\
&\quad 0 \notin U_1 \wedge 0 \notin U_2 \wedge 1 \notin U_2 \wedge \\
&\quad (\forall u \leq w)\, TripleCarryAdder(u, X, Y, Z, W, U_1, U_2)]
\end{aligned}$$

for $w \leq /X/ + /Y/ + /Z/$. Here $TripleCarryAdder(u, X, Y, Z, W, U_1, U_2)$ stands for the formula specifying the bit–wise rule to add the u^{th} bits of X, Y, Z using carries in U_1 and U_2. In other words, it is the conjunction of 32 formulas similar to the following formula

$$u \in X \wedge u \in Y \wedge u \notin Z \wedge u \in U_1 \wedge u \in U_2 \to u \notin W \wedge u + 1 \notin U_1 \wedge u + 2 \in U_2$$

The base case is trivial. The induction step follows from the definition of addition.

Similarly, for $w \leq /X/ + /Y/ + /Z/$ we have

$$\begin{aligned}
&w \in X + (Y + Z) \leftrightarrow \\
&\quad \exists W(/W/ \leq w + 1)\exists U_1(/U_1/ \leq w + 1)\exists U_2(/U_2/ \leq w + 1)[\\
&\quad 0 \notin U_1 \wedge 0 \notin U_2 \wedge 1 \notin U_2 \wedge \\
&\quad (\forall u \leq w)\, TripleCarryAdder(u, Y, Z, X, W, U_1, U_2)]
\end{aligned}$$

The conclusion follows from the fact that $\mathit{TripleCarryAdder}(u, X, Y, Z, W, U_1, U_2)$ and $\mathit{TripleCarryAdder}(u, Y, Z, X, W, U_1, U_2)$ are the same.

Now we will prove the following result:
Remark 7 $Y \leq Z \to \exists W(/W/ \leq /Z/)(Y + W = Z)$
If $Y = Z$ then $W = 0$. So suppose that $Y < Z$, it follows that $/Y/ \leq /Z/$ and there exists $z_0 \in Z$ such that

$$z_0 \notin Y \wedge \forall y \leq /Z/(y > z_0 \to (y \in Y \leftrightarrow y \in Z))$$

Let

$$W_1 = \{w : w < z_0 \wedge w \notin Y\} \text{ and } W_2 = \{w : w < z_0 \wedge w \in Z\}$$

Then it is easy to check that

$$((Y + W_1) + \{0\}) + W_2 = Z$$

By (24) we have

$$Y + ((W_1 + \{0\}) + W_2) = Z$$

and we can let $W = (W_1 + \{0\}) + W_2$.

25 $X + Y \leq X + Z \leftrightarrow Y \leq Z$: For the "only if" direction, by remark 7 we have $Y + W = Z$, therefore by (24):

$$(X + Y) + W = X + Z$$

By (19) it follows that $X + Y \leq X + Z$.

For the other direction, let $a = /X/ + /Y/ + /Z/$ and

$$U = \{u : u < a \wedge u \notin X\} + \{0\}$$

then

$$U + (X + Y) = (U + X) + Y = \{a\} \cup Y$$

and

$$U + (X + Z) = (U + X) + Z = \{a\} \cup Z$$

It follows that if $X + Y = X + Z$ then $U + (X + Y) = U + (X + Z)$ and hence $Y = Z$. Otherwise, if $X + Y < X + Z$ then by the previous direction,

$$U + (X + Y) \leq U + (X + Z)$$

Now the witness for $Y < Z$ is the same as the witness for $U + (X + Y) < U + (X + Z)$ (qed).

26 $X \cdot 0 = 0$: From definition.

27 $X \cdot (SY) = (X \cdot Y) + X$: From (29) and remarks 2,3,4.

28 $X \cdot Y = Y \cdot X$: This follows from the fact that $X \times Y = Y \times X$. To show this fact, observe that (i) $x + y = x' + y'$ and $xy = x'y'$ implies either

$x = x' \wedge y = y'$ or $x = y' \wedge y = x'$, and (ii) there do not exist x', y' such that $x' < /X/, y' < /Y/$ and $x'y' = xy + /X//Y/$.

29 $X \cdot (Y + Z) = X \cdot Y + X \cdot Z$: We will show the following results:

(i) $/X/ < a \to (X + \{a\}) \cdot W = X \cdot W + \{a\} \cdot W$

(ii) $\{a\} \cdot (Y + Z) = \{a\} \cdot Y + \{a\} \cdot Z$
This is traightforward from remark 4, since the carry set used for $\{a\} \cdot Y + \{a\} \cdot Z$ is $\{a\} \cdot U$, where U is the carry set for the addition of $Y + Z$.

(iii) Let $\varphi(x, U, Y, Z)$ be

$$/U/ \leq x \to (U \cdot (Y + Z) = U \cdot Y + U \cdot Z)$$

we will prove $\varphi(a, Y, Z)$ using lemma 3.2.
Base case: $x = 0$ then $/U/ \leq x$ implies $U = 0$ and the statement is trivial.
Induction step: Suppose the result is true for x, we will show it for $x + 1$. Let $/U/ = x + 1$, then $U = U' + \{x\}$, where $/U'/ \leq x$. By the induction hypothesis and (i), (ii):
$U \cdot (Y + Z) = U' \cdot (Y + Z) + \{x\} \cdot (Y + Z) = U' \cdot Y + U' \cdot Z + \{x\} \cdot Y + \{x\} \cdot Z$
hence by (ii) and (24):

$$U \cdot (Y + Z) = (U' + \{x\}) \cdot Y + (U' + \{x\}) \cdot Z = U \cdot Y + U \cdot Z$$

(iv) Finally, the conclusion follows from $\varphi(/X/, X, Y, Z)$.

30 $S0 \leq X \to (X \cdot Y \leq X \cdot Z \leftrightarrow Y \leq Z)$: For the "only if" direction, suppose that $Y \leq Z$, then by remark 7 let W be such that $Y + W = Z$. Then by (29), $X \cdot Z = X \cdot Y + X \cdot W$, thus from (19) we have $X \cdot Y \leq X \cdot Z$.

For the other direction, suppose that $\neg(Y \leq Z)$, then by (6) it follows that $Z < Y$. Then by remark 7, there exist W such that $Z + W = Y$ and $W \neq 0$. Then $X \cdot Y = X \cdot Z + X \cdot W$. Here $X \cdot W \neq 0$, hence by remark 6 $X \cdot Z < X \cdot Y$ (contradiction).

31 $X \neq 0 \to |X| = S(|\lfloor \frac{1}{2} X \rfloor|)$: We have

$$S(|\lfloor \tfrac{1}{2} X \rfloor|) = |\lfloor \tfrac{1}{2} X \rfloor| + S0 = Bin(max(X)) + Bin(1) = Bin(/X/) = |X|$$

(qed).

32 $X = \lfloor \frac{1}{2} Y \rfloor \leftrightarrow (2 \cdot X = Y \vee S(2 \cdot X) = Y)$: From definition of $\lfloor \frac{1}{2} Y \rfloor$ and remark 4 we have

$$2 \cdot X = \{y : y \in Y \wedge 0 < y\}$$

Therefore if $0 \in Y$ then $S(2 \cdot X) = Y$, otherwise $2 \cdot X = Y$ (qed).

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

The main consequence easily follows from the above interpretability results:

Theorem 3.4 *Provably total functions of A^1 with Σ_1^B graphs are exactly polynomial time computable functions, i.e.,*

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

for a Σ_1^B formula $\varphi(X, Y)$ if and only if there exists a polynomial time computable function $f(X)$ such that

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

Acknowledgment: We are grateful to Professor Stephen Cook for many helpful discussions and suggestions.

References

[1] Buss, S. *Bounded Arithmetic*, Bibliopolis, (1986).

[2] Ignjatovic, A. *Delineating computational complexity classes via second order theories with weak set existence principles (I)*, The Journal of Symbolic Logic, **60** (1995), 103–121.

[3] Ignjatovic, A. *Delineating computational complexity classes via second order theories with weak set existence principles (II)*, unpublished manuscript, 1994

[4] Krajicek, J. *Exponentiation and second order bounded arithmetic*, Anals of Pure and Applied Logic, **48** (1990), 261–276.

[5] Daniel Leivant, *A foundational delineation of computational feasibility*, LICS (1991), 2–11.

[6] Razborov, A. *An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic*, Arithmetic, proof theory and computational complexity (P. Clote and J. Krajicek, editors), Oxford University Press, Oxford, (1993) 247–277.

[7] Takeuti, G. *RSUV isomorphisms*, Arithmetic, proof theory and computational complexity (P. Clote and J. Krajicek, editors), Oxford University Press, Oxford, (1993) 364–386.