On Sharply Bounded Length Induction

Jan Johannsen

Universität Erlangen-Nürnberg, Germany
email: johannsen@informatik.uni-erlangen.de

Abstract. We construct models of the theory $L^0_2 := BASIC + \Sigma^b_0$-$LIND$: one where the predecessor function is not total and one not satisfying Σ^b_0-$PIND$, showing that L^0_2 is strictly weaker that S^0_2. The construction also shows that S^0_2 is not $\forall\Sigma^b_0$-axiomatizable.

Introduction

First we recall the definitions of the theories S^i_2 and T^i_2 of Bounded Arithmetic introduced by S. Buss [1]: The language of these theories is the language of Peano Arithmetic extended by symbols for the functions $\lfloor \frac{1}{2}x \rfloor$, the binary length $|x| := \lceil \log_2(x+1) \rceil$ and $x\#y := 2^{|x|\cdot|y|}$. The presence of # allows to express polynomial length bounds: if $|x| \leq p(|y|)$ for some polynomial p, then there is a term t containing # such that $x \leq t(y)$.

A quantifier of the form $\forall x \leq t$, $\exists x \leq t$ with x not occurring in t is called a *bounded quantifier*. Furthermore, a quantifier of the form $\forall x \leq |t|$, $\exists x \leq |t|$ is called *sharply bounded*. A formula is called sharply bounded if all quantifiers in it are sharply bounded.

The class of sharply bounded formulae is denoted Σ^b_0 or Π^b_0. For $i \in \mathbb{N}$, let Σ^b_{i+1} (resp. Π^b_{i+1}) be the least class containing Π^b_i (resp. Σ^b_i) and closed under conjunction, disjunction, sharply bounded quantification and bounded existential (resp. universal) quantification. In the standard model, Σ^b_i-formulae describe exactly the sets in Σ^P_i, the i^{th} level of the Polynomial Time Hierarchy, and likewise for Π^b_i-formulae and Π^P_i, for $i \geq 1$.

The theory T^i_2 is defined by a finite set $BASIC$ of quantifier-free axioms specifying the interpretation of the language, plus the induction scheme for Σ^b_i-formulae (Σ^b_i-IND). S^i_2 is defined by the $BASIC$ axioms plus the scheme of *polynomial induction*

$$\varphi(0) \wedge \forall x\, (\, \varphi(\lfloor \frac{1}{2}x \rfloor) \rightarrow \varphi(x)\,) \;\rightarrow\; \forall x \varphi(x)$$

for every Σ^b_i-formula $\varphi(x)$ (Σ^b_i-$PIND$). By the main result of [1], a function f with Σ^b_i-graph is provably total in S^i_2 iff $f \in FP^{\Sigma^P_{i-1}}$, for $i \geq 1$.

Now let L^i_2 denote the theory given by the $BASIC$ axioms and the scheme of *length induction*

$$\varphi(0) \wedge \forall x\, (\, \varphi(x) \rightarrow \varphi(Sx)\,) \;\rightarrow\; \forall x \varphi(|x|)$$

for each Σ^b_i-formula $\varphi(x)$ (Σ^b_i-$LIND$). Then for $i \geq 1$, we have $L^i_2 = S^i_2$ (see [3] for a proof).

The proof of the inclusion $L_2^i \subseteq S_2^i$ is fairly easy and also works for $i = 0$: to prove $LIND$ for a formula $\varphi(x)$, apply $PIND$ to $\varphi(|x|)$. The proof of the opposite inclusion rests mainly on the definability of certain functions in L_2^1, and thus can only be applied to the case $i = 0$ if the language is extended by symbols for these functions and axioms on them.

Therefore, in case $i = 0$, have $L_2^0 \subseteq T_2^0$, which is trivial, and $L_2^0 \subseteq S_2^0$. Furthermore the first inclusion is proper since Takeuti [6] showed that the following theorem of T_2^0

$$\forall x\, (x = 0 \vee \exists y\ \ x = Sy)$$

is unprovable in S_2^0 and hence in L_2^0. This shows that the predecessor and hence the modified subtraction function $\dot{-}$ cannot be provably total in either of these theories.

Note that $L_2^0 = S_2^0$ would imply that S_2^0 is (properly) contained in T_2^0, but it is not ruled out yet that these latter two theories are incomparable w.r.t. inclusion.

As the main result of this paper, we shall show below that $L_2^0 \subsetneqq S_2^0$. The question about the relationship between S_2^0 and T_2^0 remains unresolved. We also show that S_2^0 is not equivalent to any set of $\forall\Sigma_0^b$-axioms, i.e. axioms that are universal closures of sharply bounded formulae.

A Model-Theoretic Property of Σ_0^b-formulae

A property of sharply bounded formulae that we shall need is their absoluteness w.r.t. a certain class of extensions of models:

Definition. Let M and N be models of $BASIC$, M a substructure of N. Then we say M is *length-initial* in N, written $M \subseteq_\ell N$, if for all $a \in M$ and $b \in N$ with $b < |a|$ already $b \in M$ holds.

In the following, barred letters will always denote tuples of variables or elements whose length is either irrelevant or clear from the context.

Proposition 1. *If $M \subseteq_\ell N$, then sharply bounded formulae are absolute between M and N, i.e. for every Σ_0^b-formula $\varphi(\bar{x})$ and $\bar{a} \in M$*

$$M \models \varphi(\bar{a}) \text{ iff } N \models \varphi(\bar{a})\ .$$

Proof. This is proved easily by induction on the complexity of the formula $\varphi(\bar{x})$. The crucial case is $\varphi(\bar{x}) \equiv \forall y \le |t(\bar{x})|\, \theta(\bar{x}, y)$, where we have

$$\begin{aligned}
&M \models \forall y \le |t(\bar{a})|\, \theta(\bar{a}, y)\\
&\leftrightarrow \text{for all } b \in M \text{ with } b \le |t(\bar{a})|\ N \models \theta(\bar{a}, b)\\
&\leftrightarrow N \models \forall y \le |t(\bar{a})|\, \theta(\bar{a}, y)\ .
\end{aligned}$$

The first equivalence holds by the induction hypothesis, and the second one by $M \subseteq_\ell N$. □

Now over the $BASIC$ axioms, Σ_0^b-$LIND$ is equivalent to the following scheme

$$\forall a\ [\varphi(0) \land \forall x{<}|a|\ (\varphi(x) \to \varphi(Sx)) \to \varphi(|a|)]\ ,$$

for every sharply bounded formula $\varphi(x)$. Therefore L_2^0 is $\forall\Sigma_0^b$-axiomatizable, and hence from Proposition 1 we get

Corollary 2. *If $N \models L_2^0$ and $M \subseteq_\ell N$, then $M \models L_2^0$.*

A model of L_2^0 with a partial predecessor function

We already know from Takeuti's result for S_2^0 mentioned above and the inclusion $L_2^0 \subseteq S_2^0$, that the existence of predecessors is independent from L_2^0. We shall now construct a model witnessing this independence.

Let $M \models S_2^1$. An element $a \in M$ is called *small*, if $a \leq |b|$ for some $b \in M$, and *large* otherwise. Define

$$M_0 := \{\, a \in M\ ;\ a \text{ is small} \,\} \cup \{\, 1\#a\ ;\ a \in M \,\}\ .$$

Hence M_0 contains all small elements of M, plus a prototypical large element of each length. Let $\hat{M}$ be the closure of M_0 under addition and multiplication. We imagine $\hat{M}$ being built in stages: for $i \in \mathbb{N}$ we define

$$M_{i+1} := \{\, a+b\ ;\ a,b \in M_i \,\} \cup \{\, a \cdot b\ ;\ a,b \in M_i \,\}$$

and $\hat{M} := \bigcup_{i\in\mathbb{N}} M_i$.

Proposition 3. *$\hat{M}$ is closed under $|.|$, $\lfloor\frac{1}{2}\rfloor$ and $\#$.*

Proof. Closure under $|.|$ is clear since all small elements of M are in M_0 and hence in $\hat{M}$. Closure under $\#$ is also easy: for every $a, b \in M$, $a\#b$ is equal to $1\#\lfloor\frac{1}{2}a\#b\rfloor$, since both are powers of two of the same length, and thus $a\#b \in M_0$.

Now for closure under $\lfloor\frac{1}{2}\rfloor$: We first show that M_0 is closed under $\lfloor\frac{1}{2}\rfloor$. This follows from the fact that $\lfloor\frac{1}{2}a\rfloor$ is small iff a is small, and $\lfloor\frac{1}{2}(1\#a)\rfloor = 1\#\lfloor\frac{1}{2}a\rfloor$.

Now suppose that for every $a \in M_i$ $\lfloor\frac{1}{2}a\rfloor \in \hat{M}$, and let $b \in M_{i+1}$. Then there are $b_1, b_2 \in M_i$ such that $b = b_1 + b_2$ or $b = b_1 \cdot b_2$. Now we can calculate

$$\lfloor\frac{1}{2}(b_1+b_2)\rfloor = \begin{cases} \lfloor\frac{1}{2}b_1\rfloor + \lfloor\frac{1}{2}b_2\rfloor & \text{if } b_1 \cdot b_2 \text{ is even} \\ \lfloor\frac{1}{2}b_1\rfloor + \lfloor\frac{1}{2}b_2\rfloor + 1 & \text{else} \end{cases}$$

$$\lfloor\frac{1}{2}(b_1\cdot b_2)\rfloor = \begin{cases} \lfloor\frac{1}{2}b_1\rfloor \cdot b_2 & \text{if } b_1 \text{ is even} \\ \lfloor\frac{1}{2}b_1\rfloor \cdot b_2 + \lfloor\frac{1}{2}b_2\rfloor & \text{else} \end{cases}$$

and see that in either case $\lfloor\frac{1}{2}b\rfloor \in \hat{M}$. □

In particular, $\hat{M}$ is a substructure of M, and from the definition we see that $\hat{M} \subseteq_\ell M$, since $\hat{M}$ contains all small elements of M. Therefore $\hat{M} \models L_2^0$.

Lemma 4. *If there is $b \in \hat{M}$ with $Sb = 1\#a$, then a is bounded by $t(\bar{c})$ for some term $t(\bar{x})$ and some small $\bar{c} \in M$.*

Proof. Recall from [1] that in S^1_2 the function $Bit(x,i)$ giving the value of the i^{th} bit in the binary expansion of x and the operation of *length bounded counting* can be defined. Hence we can talk about the number of bits set in an element of M.

We shall show below that for every $b \in \hat{M}$, the number of bits set is very small, i.e. $\sharp i < |b|\ (Bit(b,i) = 1) \leq p(||\bar{c}||)$ for some polynomial p and $\bar{c} \in M$. On the other hand, if $Sb = 1\#a$, then $\sharp i < |b|\ (Bit(b,i) = 1) = |a|$, so we get $|a| \leq p(||\bar{c}||)$, and thus $a \leq t(|\bar{c}|)$ for some term $t(\bar{x})$.

We prove the above claim by induction, using the above defined M_i. If $b \in M_0$, then either b is small, or $b = 1\#d$ for some $d \in M$. In the first case, $|b| \leq ||c||$, and therefore $\sharp i < |b|\ (Bit(b,i) = 1) \leq |b| \leq ||c||$ for some $c \in M$. In the second case, $\sharp i < |b|\ (Bit(b,i) = 1) = 1$.

Now let $b \in M_{i+1}$, and suppose the claim holds for all elements in M_i. Then there are $b_1, b_2 \in M_i$ such that $b = b_1 + b_2$ or $b = b_1 \cdot b_2$. Let

$$\sharp i < |b_j|\ (Bit(b_j,i) = 1) \leq p_j(||\bar{c}_j||)$$

for $j = 1,2$. Then if $b = b_1 \circ b_2$,

$$\sharp i < |b|\ (Bit(b,i) = 1) \leq p_1(||\bar{c}_1||) \circ p_2(||\bar{c}_2||)$$

for $\circ \in \{+, \cdot\}$. Thus the claim follows. □

Recall the axioms Ω_2 stating that the function $x \#_3 y := 2^{|x|\#|y|}$ is total, which can be expressed in the language of S^1_2 as $\forall x \exists y\, |x|\#|x| = |y|$, and *exp* saying that exponentiation is total and hence there are no large elements. The consistency of the theory $S^1_2 + \Omega_2 + \neg exp$ follows from Parikhs Theorem, see e.g. [5]. Lemma 4 then yields

Theorem 5. *If $M \models S^1_2 + \Omega_2 + \neg exp$, then $\hat{M} \models L^0_2 + \exists x\, (x \neq 0 \wedge \forall y\, Sy \neq x)$.*

Proof. Since $M \models \Omega_2$, the small numbers are closed under $\#$, hence if there is $b \in \hat{M}$ with $Sb = 1\#a$, then Lemma 4 shows that a is small. But since $M \models \neg exp$, there are large elements in M and hence in $\hat{M}$. □

The independence of Σ^b_0-*PIND*

Let again $M \models S^1_2 + \Omega_2 + \neg exp$. From this model M, we construct a model $\tilde{M} \models L^0_2$ that does not satisfy S^0_2.

For $x \in M$ and $n \in \mathbb{N}$ we define $x^{\#n}$ inductively by $x^{\#0} := 1$, $x^{\#1} := x$ and $x^{\#(n+1)} := x^{\#n}\#x$ for $n \geq 1$. Choose a large $a \in M$. Then we define

$$\tilde{M} := \left\{\, b \in M\ ;\ b^{\#n} < a \text{ for all } n \in \mathbb{N} \,\right\} \cup \left\{\, b \in M\ ;\ b > a^{\#n} \text{ for all } n \in \mathbb{N} \,\right\}$$

We call the first set in the union the *lower part* of $\tilde{M}$ and the second set in the union the *upper part*. Note that the upper part is nonempty since $M \models \Omega_2$, for there must be an element b with $|b| = |a|\#|a|$. But then $b > a^{\#n}$ for every n since $b \leq a^{\#n}$ implies that $|b|$ is bounded by a polynomial in $|a|$.

Proposition 6. *$\tilde{M}$ is closed under $|.|$, $\lfloor\frac{1}{2}\rfloor$, $+$, $\cdot$ and $\#$.*

Proof. Since $M \models \Omega_2$, all small elements of M are in the lower part, since otherwise a would be small. Hence $\tilde{M}$ is closed under $|.|$.

If b is in the lower part, then of course $\lfloor\frac{1}{2}b\rfloor$ is in the lower part. On the other hand, the upper part is closed under $\lfloor\frac{1}{2}\rfloor$ since if $\lfloor\frac{1}{2}b\rfloor \leq a^{\#n}$, then $b \leq a^{\#(n+1)}$.

If at least one of b, c is in the upper part, then $b \circ c$ is in the upper part, for $\circ \in \{+, \cdot, \#\}$.

Finally, the lower part is closed under $\#$, and thus under $+$ and $\cdot$. To see this, let b and c be in the lower part. Then for every $n \in \mathbb{N}$, $(b\#c)^{\#n} \leq \max(b,c)^{\#2n} < a$, hence $b\#c$ is in the lower part. □

So $\tilde{M}$ is a substructure of M, and moreover $\tilde{M} \subseteq_\ell M$ since all small elements of M are in $\tilde{M}$, and thus $\tilde{M} \models L^0_2$. We show that there is a small element in $\tilde{M}$ that is not the length of any other element of $\tilde{M}$.

Proposition 7. *$\tilde{M} \models L^0_2 + \exists x, y\, (x < |y| \wedge \forall z \leq y\, |z| \neq x)$.*

Proof. We shall show the following: If b is in the lower part of $\tilde{M}$, then $|b| < |a|$, and if b is in the upper part of $\tilde{M}$, then $|b| > |a|$. Hence the element $|a| \in \tilde{M}$ is small, but there is no $b \in \tilde{M}$ with $|b| = |a|$.

So suppose $|b| \geq |a|$ for some b in the lower part. Then in particular $b\#b < a$, hence $|b\#b| \leq |a|$. But $|b\#b| = |b|^2 + 1 \leq |a| \leq |b|$ leads to a contradiction.

Dually, suppose $|b| \leq |a|$ for some b in the upper part. Then $a\#a < b$, hence $|a\#a| = |a|^2 + 1 \leq |b| \leq |a|$, which is likewise impossible. □

On the other hand, S^0_2 proves that every small element is the length of some other element.

Proposition 8. $S^0_2 \vdash \forall x, y\, (x \leq |y| \to \exists z \leq y\, |z| = x)$.

Proof. Consider the following case of Σ^b_0-$PIND$:

$$|0| < Sa \wedge \forall x\, (|\lfloor\frac{1}{2}x\rfloor| < Sa \to |x| < Sa) \to |b| < Sa$$

By taking the contrapositive of it and using the fact that $Sa \leq 0$ is refutable, we obtain

$$a < |b| \to \exists x\, (|\lfloor\frac{1}{2}x\rfloor| \leq a \wedge S|\lfloor\frac{1}{2}x\rfloor| > a)$$

and hence $a < |b| \to \exists x\, (|\lfloor\frac{1}{2}x\rfloor| = a)$, which implies $a < |b| \to \exists z\, |z| = a$. But if $|z| = a < |b|$, then $z < b$, so the existential quantifier can be bounded by b.

On the other hand, $a = |b| \to \exists z \leq b\, |z| = a$ is trivial, and combining these, we get

$$a \leq |b| \to \exists z \leq b\, |z| = a$$

as required. □

From Propositions 7 and 8 we immediately obtain our main result:

Theorem 9. *$L^0_2 \nvdash \Sigma^b_0$-$PIND$, hence $L^0_2 \subsetneq S^0_2$.*

This shows that the schemes of polynomial induction and length induction are not necessarily equivalent in all contexts; their equivalence depends on the class of formula they can be applied to and the surrounding theory. Furthermore the proof shows

Corollary 10. *S^0_2 is not axiomatizable by a set of $\forall\Sigma^b_0$-sentences.*

Proof. By the above results $\tilde{M}$ cannot be a model of S^0_2. If S^0_2 were $\forall\Sigma^b_0$-axiomatizable, $M \models S^0_2$ and $\tilde{M} \subseteq_\ell M$ would imply $\tilde{M} \models S^0_2$. □

Acknowledgements: The present paper was somehow inspired by work of Fernando Ferreira [4]. Sam Buss [2] used a model construction remotely similar to ours for a different purpose.

References

1. S. R. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.
2. S. R. Buss. A note on bootstrapping intuitionistic bounded arithmetic. In P. Aczel, H. Simmons, and S. S. Wainer, editors, *Proof Theory*, pages 149–169. Cambridge University Press, 1992.
3. S. R. Buss and A. Ignjatović. Unprovability of consistency statements in fragments of bounded arithmetic. *Annals of Pure and Applied Logic*, 74:221–244, 1995.
4. F. Ferreira. Some notes on subword quantification and induction thereof. Typeset Manuscript.
5. P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic.* Springer Verlag, Berlin, 1993.
6. G. Takeuti. Sharply bounded arithmetic and the function $a \dot{-} 1$. In *Logic and Computation*, volume 106 of *Contemporary Mathematics*, pages 281–288. American Mathematical Society, Providence, 1990.