A Model-Theoretic Property of Sharply Bounded Formulae, with some Applications*

Jan Johannsen
IMMD 1, Universität Erlangen-Nürnberg
email: `johannsen@informatik.uni-erlangen.de`

Abstract

We define a property of substructures of models of arithmetic, that of being *length-initial*, and show that sharply bounded formulae are absolute between a model and its length-initial submodels. We use this to prove independence results for some weak fragments of bounded arithmetic by constructing appropriate models as length-initial submodels of some given model.
Mathematics Subject Classification: 03F30, 03H15

Introduction

First we review the definitions of the theories S_2^i and T_2^i of Bounded Arithmetic introduced by S. Buss [2]: The language of these theories is the language of Peano Arithmetic extended by symbols for the functions $\lfloor \frac{1}{2}x \rfloor$, $|x| := \lceil \log_2(x+1) \rceil$ and $x\#y := 2^{|x|\cdot|y|}$. 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_0^b or Π_0^b. For $i \in \mathbb{N}$, let Σ_{i+1}^b (resp. Π_{i+1}^b) be the least class containing Π_i^b (resp. Σ_i^b) and closed under conjunction, disjunction, sharply bounded quantification and bounded existential (resp. universal) quantification. In the standard model, Σ_i^b-formulae describe exactly the sets in Σ_i^P, the i^{th} level of the Polynomial Time Hierarchy of computational complexity theory, and likewise for Π_i^b-formulae and

*The results of this paper are contained in the author's dissertation [8]. Some of the results were already announced in [7].

Π_i^P, for $i \geq 1$. (All the complexity-theoretic notions mentioned in this paper can be found in [9].)

The theory T_2^i is defined by a finite set $BASIC$ of quantifier-free axioms that specify the interpretation of the function symbols in the language, plus the induction scheme for Σ_i^b-formulae (Σ_i^b-IND). S_2^i is defined by the $BASIC$ axioms plus the scheme of *polynomial induction*

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

for every Σ_i^b-formula $\varphi(x)$ (Σ_i^b-$PIND$). By the main result of [2], a function f with Σ_i^b-graph is provably total in S_2^i iff $f \in F\Delta_i^P = FP^{\Sigma_{i-1}^P}$, for $i \geq 1$.

The theories R_2^i were defined in various disguises by several authors [4, 1, 11]. Their language is the same as that of S_2^i extended by additional function symbols for subtraction $\dot{-}$ and $MSP(x,i) := \lfloor \frac{x}{2^i} \rfloor$. The set $BASIC$ is extended by additional quantifier-free axioms on the new function symbols; we shall simply call the extended set $BASIC$ also, as it will always be clear from the context which set is meant. Now R_2^i is axiomatized by $BASIC$ plus the scheme of *polynomial length induction*

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

for every Σ_i^b-formula $\varphi(x)$ (Σ_i^b-$LPIND$). R_2^1 is related to the complexity class uniform NC, since the Σ_1^b-definable functions of R_2^1 are exactly those in this class.

Recall the axioms Ω_2 stating that the function $x \#_3 y := 2^{|x|\#|y|}$ is total, which is most conveniently expressed as $\forall x\, \exists y\, |x|\#|x| = |y|$, and exp saying that exponentiation is total, which we can express as $\forall x\, \exists y\, |y| = x$. We shall construct models as substructures of some model of the theory $S_2^1 + \Omega_2 + \neg exp$, whose consistency follows from Parikh's Theorem, see e.g. [5].

The model-theoretic property

A fact well-known and extensively used in the study of models of arithmetic is the absoluteness of bounded formulae between a model and an initial segment of it. In order to obtain an analogon for *sharply bounded* formulae, we introduce the following notion:

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

As usual, we call an element a of some model M *small*, if $a \leq |b|$ for some $b \in M$, and *large* otherwise. Hence $N \subseteq_\ell M$ iff the small elements in N form an initial segment of the small elements in M.

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

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

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

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

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

Actually, the analogy between Prop. 1 and the absoluteness of bounded formulae w.r.t. initial segments is more than a mere analogy, as the following considerations show.

A model M of some (sufficiently strong) theory of Bounded Arithmetic can be viewed as a second-order model $\mathfrak{M} = (\log M, M)$, where $\log M$ denotes the set of small elements in M and for $i \in \log M$ and $m \in M$ we say that $i \in m$ if the ith bit in m is 1. There is also a syntactical translation mapping a formula φ in the language of Bounded Arithmetic to a second-order formula $\varphi^\sharp$ such that $M \models \varphi$ iff $\mathfrak{M} \models \varphi^\sharp$. This correspondence between first- and second-order models together with the translation $\sharp$ is known as the *RSUV*-isomorphism [11].

Now $N \subseteq_\ell M$ holds iff $\mathfrak{N} = (\log N, N)$ is an initial segment of $\mathfrak{M}$, and sharply bounded formulae are mapped by $\sharp$ to first-order bounded formulae. Therefore the assertion of Prop. 1 and the absoluteness of bounded formulae are the same modulo the *RSUV*-isomorphism.

Our main applications of Prop. 1 will be of the following type: If a theory T has a $\forall\Sigma_0^b$-axiomatization, and we have a model $M \models T$ and a length initial submodel $N \subseteq_\ell M$, we can conclude $N \models T$.

Sharply bounded length induction

Let L^i_2 denote the theory in the language of S^i_2 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-$LIND$). For $i \geq 1$, we have $L^i_2 = S^i_2$ (see [3] for a proof).

The proof of the inclusion $L^i_2 \subseteq S^i_2$ 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 the functions $\dot{-}$ and MSP in L^1_2 and thus can only be applied to the case $i = 0$ in the extended language of R^i_2.

Therefore, in case $i = 0$, have $L^0_2 \subseteq T^0_2$, which is trivial, and $L^0_2 \subseteq S^0_2$. Furthermore the first inclusion is proper since Takeuti [10] showed that the following theorem of T^0_2

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

is unprovable in S^0_2 and hence in L^0_2. This shows that the predecessor and hence the modified subtraction function $\dot{-}$ cannot be provably total in either of these theories.

Note that $L^0_2 = S^0_2$ would imply that S^0_2 is (properly) contained in T^0_2, but it is not ruled out yet that these latter two theories are incomparable w.r.t. inclusion.

As one application of the model-theoretic property above, we shall show below that $L^0_2 \subsetneqq S^0_2$. We also show that S^0_2 is not $\forall\Sigma^b_0$-axiomatizable.

To make this possible, we need the following fact, which is easily proved: over the $BASIC$ axioms, Σ^b_0-$LIND$ is equivalent to the scheme

$$\forall a\;\,[\varphi(0) \wedge \forall x\!<\!|a|\;(\varphi(x) \rightarrow \varphi(Sx)) \rightarrow \varphi(|a|)]\;\;,$$

for every sharply bounded formula $\varphi(x)$. Therefore L^0_2 is $\forall\Sigma^b_0$-axiomatizable, and hence from Prop. 1 we get

Corollary 2 *If $M \models L^0_2$ and $N \subseteq_\ell M$, then $N \models L^0_2$.*

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. As an illustration of the method, we shall now construct a model witnessing this independence. Let $M \models S_2^1 + \Omega_2 + \neg exp$, and 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 since for every $a, b \in M$, $a\#b = 1\#\lfloor \frac{1}{2} a\#b \rfloor$, and hence $a\#b \in M_0$.

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 for $a \in M$ there is $b \in \hat{M}$ with $Sb = 1\#a$, then a is small.*

Proof: Recall from [2] that in S_2^1 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 define the function $Count(x) := \sharp i < |x|\ (Bit(x,i) = 1)$ for $x \in M$, and show in S_2^1 that $Count(a \circ b) \leq Count(a) \circ Count(b)$ for $\circ \in \{+, \cdot\}$.

We shall show below that for every $b \in \hat{M}$, the number of bits set is very small, i.e. $Count(b) \leq ||c||$ for some $c \in M$. On the other hand, if $Sb = 1\#a$, then $Count(b) = |a|$, so we get $|a| \leq ||c||$, and thus $a \leq 2|c|$, so a is small.

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 $Count(b) \leq |b| \leq ||c||$ for some $c \in M$. In the second case, $Count(b) = 1$.

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 $Count(b_j) \leq ||c_j||$ for $j = 1, 2$. Now if $b = b_1 + b_2$, then by the above

$$Count(b) \leq ||c_1|| + ||c_2|| \leq |\,|c_1| \cdot |c_2| + 1\,| \leq ||2(c_1\#c_2)||\ .$$

If on the other hand $b = b_1 \cdot b_2$, then we have

$$Count(b) \leq ||c_1|| \cdot ||c_2|| \leq |\,|c_1|\#|c_2|\,|\ ,$$

and by Ω_2 there is $c \in M$ with $|c_1|\#|c_2| \leq |c|$, and thus $Count(b) \leq ||c||$ for this c. □

From Lemma 4 we immediately get

Theorem 5 $\hat{M} \models L_2^0 + \exists x\ (x \neq 0 \wedge \forall y\ Sy \neq x)$.

Proof: 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 for large a the element $1\#a \in \hat{M}$ has no predecessor in $\hat{M}$. □

The independence of Σ_0^b-$PIND$

Let again $M \models S_2^1 + \Omega_2 + \neg exp$. From this model M, we construct a model $\tilde{M} \models L_2^0$ that does not satisfy S_2^0.

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

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

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 $a^2 > n \cdot a$ for every $n \in \mathbb{N}$.

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 $\lfloor \frac{1}{2} b \rfloor \leq n \cdot a$, then $b \leq (3n) \cdot a$.

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. $\square$

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 $2a < b$, hence $|a| + 1 = |2a| \leq |b| \leq |a|$, which is likewise impossible. $\square$

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

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

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

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

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

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

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

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

$$a \leq |b| \rightarrow \exists z \leq b\ |z| = a$$

as required. □

From Theorem 7 and Prop. 8 we immediately have the following

Theorem 9 $L^0_2 \not\vdash \Sigma^b_0$*-PIND, hence* $L^0_2 \subsetneqq S^0_2$.

This is the first example of a situation where the schemes of polynomial induction and length induction are not equivalent. Furthermore we obtain

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 $\tilde{M} \models S^0_2$. □

A further conclusion we can draw from this construction is the following:

Corollary 11 *The function* MSP *is not definable in* L^0_2.

Proof: The model $\tilde{M} \models L^0_2$ is not closed under MSP: since $a^2 \in \tilde{M}$, there is a $b \in \tilde{M}$ with $|b| = 2|a|$. For this b we have then $|MSP(b, |a|)| = |a|$, hence $MSP(b, |a|) \notin \tilde{M}$. □

Towards a model-theoretic proof of Takeuti's result

It would be nice if the method of length-initial submodels could be extended to yield a model-theoretic proof of Takeuti's independence result, the unprovability of the existence of predecessors in S^0_2. By Corollary 10 the method we have used above is not applicable.

Nevertheless, the possibility remains that the model $\hat{M} \models L^0_2$ defined above satisfies S^0_2, which would give the desired model-theoretic proof. A starting point could be the following property of $\hat{M}$.

Definition: Let $N \subseteq_\ell M$, then N is called *dense* in M if for each $a \in M$ such that $|a|$ is small in N there is $b \in N$ with $|b| = |a|$.

The property that the model $\tilde{M}$ is not dense in M was used above to show that $\tilde{M} \not\models S_2^0$. Hence the density of a model N in $M \models S_2^0$ might suffice for $\hat{M}$ to satisfy S_2^0, which would give the desired proof since $\hat{M}$ is dense in M.

This question remains open, but it is at least possible to prove that $\hat{M}$ satisfies some fraction of S_2^0 stronger than L_2^0. To state this, we need the following notion:

Definition: Let $M \models BASIC$, then a formula $\varphi(x)$ is called *stable* in M if for all $a, b \in M$ with $|a| = |b|$ it holds that $M \models \varphi(a)$ iff $M \models \varphi(b)$.

Hence stable properties only depend on the length of an element, in particular, a formula of the form $\varphi(|x|)$ is stable in every model. Now we can prove that $\hat{M}$ satisfies polynomial induction for stable Σ_0^b-formulae.

Proposition 12 *If $N \subseteq_\ell M \models S_2^0$ and N is dense in M, then N satisfies $PIND$ for stable Σ_0^b-formulae.*

Proof: Let $\varphi(x) \in \Sigma_0^b$ be stable in M, and let $N \models \varphi(0)$ and $N \models \varphi(\lfloor \frac{1}{2} b \rfloor) \to \varphi(b)$ for all $b \in N$. Now suppose there is an $a \in N$ such that $N \models \neg\varphi(a)$.

By absoluteness we have $M \models \varphi(0)$ and $M \models \neg\varphi(a)$, hence there is $b \in M$ with $M \models \varphi(\lfloor \frac{1}{2} b \rfloor) \wedge \neg\varphi(b)$. Since N is dense in M there is $b' \in N$ with $|b'| = |b|$, and thus $|\lfloor \frac{1}{2} b' \rfloor| = |\lfloor \frac{1}{2} b \rfloor|$.

Now the stability of $\varphi(x)$ yields $M \models \varphi(\lfloor \frac{1}{2} b' \rfloor) \wedge \neg\varphi(b')$, and by absoluteness this also holds in N, in contradiction to the above. $\square$

Now for the desired model-theoretic proof, it would suffice to show that S_2^0 is implied by $PIND$ for stable Σ_0^b-formulae. Note that the $PIND$ for stable Σ_0^b-formulae is strictly stronger than Σ_0^b-$LIND$: To prove $LIND$ for a formula $\psi(x)$, $PIND$ for the stable formula $\psi(|x|)$ is used. On the other hand, the model $\tilde{M} \models L_2^0$ does not satisfy $PIND$ for stable Σ_0^b-formulae, since the formula $|x| < Sa$ used in the instance of $PIND$ in the proof of Prop. 8 is stable in every model.

An independence result for R_2^0

In [11] it was shown that R_2^0 is equivalent to the theory given by the $BASIC$ axioms and Σ_0^b-$PIND$ in the language of R_2^0.

In [6] an independence result for (an extension of) R^0_2 was proved by proof-theoretic means similar to the method of [10]: Let $y = \lfloor \frac{1}{3}x \rfloor$ stand short for the formula $x = 3y \vee x = 3y+1 \vee x = 3y+2$.

Theorem 13 *$\forall x\, \exists y\, y = \lfloor \frac{1}{3}x \rfloor$ is not provable in R^0_2.*

As a corollary to the proof of this theorem given in [6], it follows that R^0_2 cannot Σ^b_1-define every function in the very small complexity class uniform NC^0. We now give a new proof of Theorem 13 using our model-theoretic technique. This proof yields the same corollary as the syntactic proof.

First, we need the fact that R^0_2 is $\forall\Sigma^b_0$-axiomatizable, namely by the $BASIC$ axioms and the scheme

$$\forall a\, \Big[A(0) \wedge \forall x \leq |a|\ (A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow \forall x \leq |a|\ A(x) \Big]$$

for every Σ^b_0-formula $A(x)$. This scheme obviously implies Σ^b_0-$LPIND$, and it can be proved by $PIND$ on the variable a in the Σ^b_0-formula $[\dots]$.

Let $M \models S^1_2 + \Omega_2 + \neg exp$, regarded as a structure for the language of R^0_2. For $a \in M$, let $\mathrm{blk}(a)$ denote the number of blocks of zeros and ones in a, i.e.

$$\mathrm{blk}(a) := \sharp i < |a|\ Bit(a,i) \neq Bit(a,i+1)\ ,$$

which is well-defined since this function is Σ^b_1-definable in S^1_2. We consider the set of those elements in M with a very small number of blocks

$$\breve{M} := \{\, a \in M\ ;\ \mathrm{blk}(a) \leq ||b|| \text{ for some } b \in M \,\}\ .$$

Proposition 14 *$\breve{M}$ is a substructure of M.*

Proof: The inequalities $\mathrm{blk}(|a|) \leq ||a||$, $\mathrm{blk}(a\#b) \leq 2$, $\mathrm{blk}(\lfloor \frac{1}{2}a \rfloor) \leq \mathrm{blk}(a)$ and $\mathrm{blk}(MSP(a,i)) \leq \mathrm{blk}(a)$ are trivial, hence $\breve{M}$ is closed under these operations. We shall now show that for $\circ \in \{+, \dot{-}, \cdot\}$, $\mathrm{blk}(a \circ b)$ is bounded by a polynomial in $\mathrm{blk}(a)$ and $\mathrm{blk}(b)$. The proofs can be formalized in S^1_2, and since $M \models \Omega_2$, this shows that $\breve{M}$ is closed under these operations.

Lemma 15 $\mathrm{blk}(a+1) \leq \mathrm{blk}(a) + 1$.

Proof: If a is even, then the last bit in a is changed to one, whereby at most one new block is introduced. If a is odd, then the last block of ones is changed to zero, and the rightmost zero is changed to one; this also introduces at most one new block. $\square$

Lemma 16 *If* $a \geq b$, *then* $\mathrm{blk}(a+b) \leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b) + 1$.

Proof: We first prove that $\mathrm{blk}(a+b) \leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b)$ in case that b is even, by induction on $\mathrm{blk}(b)$. The base case, $\mathrm{blk}(b) = 0$, is trivial. For the inductive step, let $LSP(a,i)$ denote $a \bmod 2^i$, the number consisting of the last i bits of a, and define

$$
\begin{gathered}
i_b := \mu i < |b| \; Bit(b,i) = 1 \\
j_b := \mu j < |b| \; j > i_b \wedge Bit(b,j) = 0 \\
a' := MSP(a, j_b) \qquad b' := MSP(b, j_b) \\
a_0 := LSP(a, i_b) \qquad a_1 := MSP(LSP(a, j_b), i_b)
\end{gathered}
$$

where we treat a_0 and a_1 as bit-strings, possibly with leading zeroes. Obviously, we have $\mathrm{blk}(a') + \mathrm{blk}(a_1) + \mathrm{blk}(a_0) \leq \mathrm{blk}(a) + 2$, and $\mathrm{blk}(b) = \mathrm{blk}(b') + 2$. Furthermore, since b' is even, the inductive hypothesis assures that $\mathrm{blk}(a' + b') \leq \mathrm{blk}(a') + 2\,\mathrm{blk}(b')$.

Now if a_1 consists entirely of zeroes, then $a+b$ is given by $a'+b'$ concatenated with a string of ones of length $|a_1|$ followed by a_0. This gives us

$$
\begin{aligned}
\mathrm{blk}(a+b) &\leq \mathrm{blk}(a'+b') + \mathrm{blk}(a_0) + 1 \\
&\leq \mathrm{blk}(a') + 2\,\mathrm{blk}(b') + \mathrm{blk}(a_0) + 1 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b') + 3 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b) \; .
\end{aligned}
$$

Otherwise, let $\tilde{a}_1$ result from a_1 by replacing the rightmost block of zeroes by ones, the rightmost one by a zero and leaving the rest unchanged. Then $a+b$ is given by $a' + b' + 1$ concatenated with $\tilde{a}_1$ followed by a_0. Since $\mathrm{blk}(\tilde{a}_1) \leq \mathrm{blk}(a_1) + 1$, we can calculate

$$
\begin{aligned}
\mathrm{blk}(a+b) &\leq \mathrm{blk}(a'+b'+1) + \mathrm{blk}(\tilde{a}_1) + \mathrm{blk}(a_0) \\
&\leq \mathrm{blk}(a'+b') + \mathrm{blk}(a_1) + \mathrm{blk}(a_0) + 2 \\
&\leq \mathrm{blk}(a') + 2\,\mathrm{blk}(b') + \mathrm{blk}(a_1) + \mathrm{blk}(a_0) + 2 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b') + 4 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b) \; .
\end{aligned}
$$

Now if b is odd, let

$$
\begin{gathered}
i_b := \mu i < |b| \; Bit(b,i) = 0 \\
a' := MSP(a, i_b) \qquad b' := MSP(b, i_b) \\
a_1 := LSP(a, i_b) \; ,
\end{gathered}
$$

where again we treat a_1 as a bit-string with possibly some leading zeroes. Then we have $\mathrm{blk}(a') + \mathrm{blk}(a_1) \leq \mathrm{blk}(a) + 1$ and $\mathrm{blk}(b) = \mathrm{blk}(b') + 1$, and since b' is even, we get $\mathrm{blk}(a' + b') \leq \mathrm{blk}(a') + 2\,\mathrm{blk}(b')$ from the above.

Now if a_1 consists entirely of zeroes, $a + b$ is given by $a' + b'$ concatenated with a string of ones of length $|a_1|$, hence

$$\begin{aligned}
\mathrm{blk}(a+b) &\leq \mathrm{blk}(a' + b') + 1 \\
&\leq \mathrm{blk}(a') + 2\,\mathrm{blk}(b') + 1 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b) + 1 \ .
\end{aligned}$$

Otherwise, let $\tilde{a}_1$ be defined as above, then $a + b$ is given by $a' + b' + 1$ concatenated with $\tilde{a}_1$, and we can calculate

$$\begin{aligned}
\mathrm{blk}(a+b) &\leq \mathrm{blk}(a' + b' + 1) + \mathrm{blk}(\tilde{a}_1) \\
&\leq \mathrm{blk}(a' + b') + \mathrm{blk}(a_1) + 2 \\
&\leq \mathrm{blk}(a') + 2\,\mathrm{blk}(b') + \mathrm{blk}(a_1) + 2 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b') + 3 \\
&\leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b) + 1 \ .
\end{aligned}$$

This completes the proof of the lemma. □

This upper bound is indeed optimal, as the following example shows: Let $b := \sum_{i=0}^{n} 7 \cdot 2^{6i}$ and $a := 2b$. Then in binary we calculate

$$\begin{aligned}
a &= \quad 1110(001110)^n \\
b &= \quad\;\; 111(000111)^n \\
a + b &= 10101(010101)^n
\end{aligned}$$

so we have $\mathrm{blk}(b) = 2n + 1$, $\mathrm{blk}(a) = 2n + 2$ and $\mathrm{blk}(a + b) = 6n + 5 = \mathrm{blk}(a) + 2\,\mathrm{blk}(b) + 1$.

Lemma 17 $\mathrm{blk}(a \dot{-} b) \leq \mathrm{blk}(a) + 2\,\mathrm{blk}(b) + 1$.

Proof: If $a < b$, then $a \dot{-} b = 0$, hence the claim is trivially true. So let $a \geq b$, let $c := 2^{|a|+1} - 1$ and calculate $a \dot{-} b = c - ((c - a) + b$. Then $\mathrm{blk}(c - a) = \mathrm{blk}(a) + 1$, and since $|c - a| = |c|$ we have $\mathrm{blk}(c - ((c - a) + b)) =$

$\text{blk}((c-a)+b)-1$, hence we can estimate

$$\begin{aligned}\text{blk}(a \dot{-} b) &= \text{blk}(c-((c-a)+b)) \\ &\leq \text{blk}((c-a)+b)-1 \\ &\leq \text{blk}(c-a)+2\ \text{blk}(b) \\ &= \text{blk}(a)+2\ \text{blk}(b)+1\ .\end{aligned}$$

□

Lemma 18 $\text{blk}(ab) \leq 3\,\text{blk}(a)\,\text{blk}(b)+6\,\text{blk}(a)+4\,\text{blk}(b)+6.$

Proof: We calculate $a \cdot b$ using the elementary school algorithm as

$$a \cdot b = \sum_{i=0}^{|b|} a \cdot Bit(b,i) \cdot 2^i\ .$$

Now let $A := \lceil \frac{\text{blk}(b)}{2} \rceil$, and define inductively for $k \leq A$

$$\begin{aligned}b_0 &:= b \\ i_k &:= \mu i < |b_k|\ Bit(b_k, i) = 1 \\ j_k &:= \mu j < |b_k|\ Bit(b_k, i_k + j) = 0 \\ b_{k+1} &:= MSP(b_k, i_k + j_k)\end{aligned}$$

and $s_k := i_k + \sum_{m=0}^{k-1} i_m + j_m$. Then the above sum can be rewritten as

$$\begin{aligned}a \cdot b &= \sum_{k=0}^{A} \sum_{m=0}^{j_k} a \cdot 2^{s_k+m} \\ &= \sum_{k=0}^{A} (2^{j_k+1}-1) \cdot a \cdot 2^{s_k} \quad =: \sum_{k=0}^{A} c_k\ .\end{aligned}$$

Now for each of the terms c_k we obtain

$$\begin{aligned}\text{blk}(c_k) &= \text{blk}((a \cdot 2^{j_k+1}-a) \cdot 2^{s_k}) \\ &\leq \text{blk}(a \cdot 2^{j_k+1}-a)+1 \\ &\leq \text{blk}(a \cdot 2^{j_k+1})+2\ \text{blk}(a)+2 \\ &\leq 3\ \text{blk}(a)+3\ ,\end{aligned}$$

hence we can calculate

$$
\begin{aligned}
\mathrm{blk}(a \cdot b) &= \mathrm{blk}(\sum_{i=0}^{A} c_k) \\
&\leq (1 + 2\,A)\ \mathrm{blk}(c_k) + A \\
&\leq (1 + 2\,A)\,(3\ \mathrm{blk}(a) + 3) + A \\
&= (6\,A + 3)\ \mathrm{blk}(a) + 7\,A + 3\ ,
\end{aligned}
$$

and using the definition of A we obtain

$$\mathrm{blk}(a \cdot b) \leq (3\ \mathrm{blk}(b) + 6)\ \mathrm{blk}(a) + 4\ \mathrm{blk}(b) + 6\ ,$$

which completes the proof of the lemma and Prop. 14. □

Hence $\breve{M}$ is a substructure of M, and since all small elements of M are in $\breve{M}$, we have $\breve{M} \subseteq_\ell M$, and thus $\breve{M} \models R^0_2$. Therefore the following proposition establishes Theorem 13.

Proposition 19 $\breve{M} \models \neg\forall x\, \exists y\; y = \lfloor \frac{1}{3} x \rfloor$.

Proof: Consider $b := 2^{|a|} - 1$ for some $a \in M$, then in b every bit is 1, and thus $\mathrm{blk}(b) = 1$ and so $b \in \breve{M}$. Let $c := \lfloor \frac{1}{3} b \rfloor \in M$, then c is the number with $|c| = |b| - 1$ with every other bit 1, as is easily seen by calculating $3c = 2c + c$. Hence $\mathrm{blk}(c) = |c|$, and so $c \in \breve{M}$ only if c and thus b is small. But $M \models \neg exp$, and thus for a large b as above $c = \lfloor \frac{1}{3} b \rfloor \notin \breve{M}$. □

From this proof of Theorem 13, as well as from the syntactic proof given in [6], we can furthermore conclude

Theorem 20 *There is a function in uniform NC^0 which is not Σ^b_1-definable in R^0_2.*

Proof: Consider the function g defined by $g(x) := \lfloor \frac{1}{3}(2^{|x|} - 1) \rfloor$. The value $g(x)$ is the number y with $|y| = |x| - 1$ in which every other bit is 1. This function is easily seen to be in uniform NC^0.

For the numbers b with $\mathrm{blk}(b) = 1$ used in the above proof $b = 2^{|b|} - 1$ holds, hence for these numbers $g(b) = \lfloor \frac{1}{3} b \rfloor$. Hence the proof also shows that the function g is not provably total in R^0_2. □

The Σ^b_0-comprehension scheme is the scheme of axioms

$$\exists y < 2^{|a|}\ \forall i < |a|\ \ (Bit(y, i) = 1\ \leftrightarrow\ A(i))$$

for every Σ^b_0-formula $A(i)$.

Corollary 21 *The Σ_0^b-comprehension scheme is not provable in R_2^0.*

To see this, just observe that the function g above can be easily defined using the comprehension axiom for the formula $A(i) :\equiv i \bmod 2 = |a| \bmod 2$. This shows that R_2^0 cannot even prove the comprehension scheme for equations, since $x \bmod 2$ can be expressed as a term in the language of R_2^0.

Acknowledgements: I would like to thank Stephen Bloch, Peter Clote and Wilfried Sieg for some questions and remarks that led to improvements of the paper.

References

[1] B. Allen. Arithmetizing uniform *NC*. *Annals of Pure and Applied Logic*, 53:1–50, 1991.

[2] S. R. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.

[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] P. Clote. A first order theory for the parallel complexity class NC. Technical Report BCCS-89-01, Boston College, January 1989.

[5] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic*. Springer Verlag, Berlin, 1993.

[6] J. Johannsen. On the weakness of sharply bounded polynomial induction. In G. Gottlob, A. Leitsch, and D. Mundici, editors, *Computational Logic and Proof Theory*, volume 713 of *Lecture Notes in Computer Science*, pages 223–230. Springer Verlag, 1993.

[7] J. Johannsen. On sharply bounded length induction. In H. Kleine Büning, editor, *Computer Science Logic*, volume 1092 of *Lecture Notes in Computer Science*, pages 362–367. Springer, 1996.

[8] J. Johannsen. *Schwache Fragmente der Arithmetik und Schwellwertschaltkreise beschränkter Tiefe*. Dissertation, Universität Erlangen-Nürnberg, 1996.

[9] D. S. Johnson. A catalog of complexity classes. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science Vol. A*, chapter 2, pages 67–161. Elsevier, Amsterdam, 1990.

[10] 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.

[11] G. Takeuti. *RSUV* isomorphisms. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, volume 23 of *Oxford Logic Guides*, pages 364–386. Clarendon Press, Oxford, 1993.