数理解析研究所講究録 1217 巻 2001 年 45-60

MODELS OF BOUNDED ARITHMETIC

SATORU KURODA
GUNMA PREFECTURAL WOMEN'S UNIVERSITY
黒田覚
群馬県立女子大学

1. Introduction

In the last two decades, much progress has been made in the study of weak fragments of arithmetic. Generally speaking, the term "weak fragments" or "bounded arithmetic" represents those theories which cannot define the totality of the exponential function. These terminologies are justified by the result of R. Parikh [20] dated back in 1975 which states that Δ_0 induction cannot Δ_0 define functions of superpolynomial growth. As the exponential relation has Δ_0 presentation, it follows that the well-known theory $I\Delta_0$ cannot define exponentiation.

The second leap was made by J. Paris and A. Wilkie [21]. They investigated properties of the theories $I\Delta_0$ and $I\Delta_0+\Omega_1$, both proof theoretical and model theoretical. Among them are the problem posed by Macintyre whether the pigeonhole principle is provable in these theories and the provability of Matijasevič theorem in $I\Delta_0$. Especially the first problem was given a partial answer for the relativised case by M. Ajtai [2] for which he used the forcing method and this later became one of the main topic in the 1990s.

The third great progress is closely connected to the theory of computational complexity, notably to the famous $P = NP$ problem. In [8], S. Cook presented an equational theory PV which has defining axioms for all polynomial time computable functions. There he showed that reasonings in PV is translated into polynomial size extended Frege proofs and vice versa. Inspired by this result and the traditional Gentzen-style proof theory, S. Buss [5] introduced a hierarchy of bounded arithmetic theories S^i_2 and T^i_2 whose provably total functions corresponds to the i-th level of the polynomial hierarchy.

In this exposition, we will survey model-theoretical aspects of various theories of bounded arithmetic. The first of such studies is credited to R. Parikh, who proved his own famous Parikh's theorem model theoretically. Also, after the Buss' cerebrating results, A. Wilkie showed the witnessing theorem using a model theoretical method (unpublished) and P. Hájek and P. Pudlák [10] generalized Wilkie's proof to other theories of bounded arithmetic. At first these results seemed only subsidiary ones and proof theoretical analysis were considered more essential for bounded arithmetic. However recent analysis of witnessing using Herbrand type argument revealed its deeper structure. Especially J. Avigad [3] introduced the notion of Herbrand saturation which enabled the use of essentially the same method to show witnessing and conservation for various theories.

Finally one more progress is worth mentioning here in the model theory of weak fragments. The problem of initial segments and end extensions was one of the fundamental problems in stronger fragments of arithmetic. (See Kaye [16]). In the case of bounded arithmetic sharper notions are defined to investigate the structure of models of arithmetic.

One of such is the notion of length initial substructure defined by J. Johannsen [14]. He used it to show several independence results for sharply bounded arithmetic. For example, he showed model theoretically the theorem by G. Takeuti [23] stating that the theory S_2^0 cannot define the predecessor function.

On the other hand, A. Beckmann [4] considered other variations of initial segment and he showed that end extension problems accroding to these variations are closely related to separations of complexity classes.

This paper is organized as follows: in section 2 we will prepare basic notions of first and second order theories of bounded arithmetic and present some properties which wiil be used in later sections. In section 3 we will analyse proof of witnessing. In section 4 we give model theoretical arguments for connecting first and second order theories. Finally in section 5 some modifications of initial segments and end extensions are presented and discuss about their applications.

2. Preliminaries

First we will give some basic notions of bounded arithmetic.

2.1. Language. We will use several different languages according to the theory in concern. The language L_0 contains a constant 0, function symbols $S(x) = x+1$, $x+y$, $x \cdot y$ and a relation symbol $\leq$. The language L_1 contains all symbols in L_0 together with additional function symbols $|x| = \lfloor \log_2(x+1) \rfloor$, $\lfloor \cdot/2 \rfloor$ and $x \# y = 2^{|x| \cdot |y|}$.

2.2. Complexity of formulae. Let L be a fixed language of arithmetic. For a term t in L, quantifiers of the form $\forall x \leq t$ and $\exists x \leq t$ are called bounded. Let $|t|$ denote the length of the binary expression of t. Then we call quantifiers of the form $\forall x \leq |t|$ and $\exists x \leq |t|$ sharply bounded. (Notice that when we refer to sharply bounded quantifiers, we assume that the function $| \cdot |$ is in the language L. A formula is called bounded if all quantifiers in it are bounded and sharply bounded if all quantifiers are sharply bounded.

Definition 1. *The sets of L_1 formulae Σ_i^b and Π_i^b ($i \geq 0$) are defined inductively as follows:*

1. $\Sigma_0^b = \Pi_0^b$ *is the set of sharply bounded formulae;*
2. Σ_{i+1}^b *and* Π_{i+1}^b *are the smallest sets satisfying*
   (a) $\Sigma_i^b, \Pi_i^b \subseteq \Sigma_{i+1}^b$ *and* $\Sigma_i^b, \Pi_i^b \subseteq \Pi_{i+1}^b$,
   (b) Σ_{i+1}^b *and* Π_{i+1}^b *are closed under connectives* $\wedge$, $\vee$ *and sharply bounded quantifications,*
   (c) Σ_{i+1}^b *is closed under bounded existential quantifications and* Π_{i+1}^b *is closed under bounded universal quantifications,*
   (d) *if* $\varphi \in \Sigma_{i+1}^b$ *or* $\varphi \in \Pi_{i+1}^b$ *then* $\neg\varphi \in \Pi_{i+1}^b$ *and* $\neg\varphi \in \Sigma_{i+1}^b$ *respectively,*
   (e) *if* $\varphi \in \Pi_{i+1}^b$ *and* $\psi \in \Sigma_{i+1}^b$ *then* $\varphi \supset \psi \in \Sigma_{i+1}^b$, *the same statement holds if we exchange* Σ_{i+1}^b *and* Π_{i+1}^b.

$\Sigma_\infty^b = \bigcup_{i \in \omega} \Sigma_i^b$.

Definition 2. *The set of bounded formulae in the language L_0 is denoted by Δ_0.*

2.3. Axioms. We use the following axioms to define our weak theories. P^- is the set of finite number of sentences which define symbols in L_0. BASIC is the same as P^- for the language L_1. Examples of P^- and BASIC can be found in Hájek and Pudlák [ ].

Definition 3. *Let Φ be a set of foumulae. Then*

1. *Φ-IND:*
   $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(x)$,
2. *Φ-PIND:*
   $\varphi(0) \wedge \forall x(\varphi(\lfloor x/2 \rfloor) \rightarrow \varphi(x)) \rightarrow \forall x \varphi(x)$,
3. *Φ-LIND:*
   $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(|x|)$,

where $\varphi \in \Phi$.

Definition 4. *For $i \geq 1$ the function $x \#_i y$ is defined inductively as follows:*

$$\begin{aligned} x \#_1 y &= |x| \cdot |y|, \\ x \#_{i+1} y &= 2^{x \#_i y}. \end{aligned}$$

The axiom Ω_i states that the function $\#_{i+1}$ is total.

2.4. Definition of theories. Now we can define various theories of bounded arithmetic which we will treat in this exposition.

Definition 5. *$I\Delta_0$ is the L_0 theory with axioms*

- *P^-*
- *Δ_0-IND*

Definition 6.
1. *For $i \geq 0$, S_2^i is the L_1 theory with axioms*
   - *BASIC*
   - *Σ_i^b-PIND*
2. *For $i \geq 0$, T_2^i is the L_1 theory with axioms*
   - *BASIC*
   - *Σ_i^b-IND*

2.5. Function Algebra and the theory PV. We also treat slightly different type of theories which is based on recursion theoretic characterizations of complexity classes.

Definition 7. *A function f is defined by bounded recursion on notation from g, h_0, h_1 and k if*

$$\begin{aligned} f(0, \vec{x}) &= g(\vec{x}), \\ f(2n, \vec{x}) &= h_0(n, \vec{x}, f(n, \vec{x})), \ \text{if } n \neq 0, \\ f(2n+1, \vec{x}) &= h_1(n, \vec{x}, f(n, \vec{x})), \end{aligned}$$

provided that $f(n, \vec{x}) \leq k(n, \vec{x})$ for all n and $\vec{x}$.

Proposition 1. *A function f is polynomial time computable if it is in the smallest class containing $Z(x) = 0$, $S(x) = x + 1$, $P_n^k(x_1, \cdots, x_n) = x_k$, $x \# y$ and closed under composition and bounded recursion on notation*

Definition 8. *Let L_{PV} be the language with function symbols for each polynomial time computable functions together with a relation symbol $\leq$. PV is the L_{PV} theory with defining axioms for each polynomial time computable functions characterized by the previous proposition plus PIND for open L_{PV} formulae.*

2.6. Second Order Systems. We will also consider second order systems. The essence of considering second order systems is that second order objects (sets) are regarded as short sequences in the sense that

$$\forall i \leq |a|(i \in X \Leftrightarrow Bit(x,i) = 1),$$

where $Bit(x,i)$ is the i-th bit of the binary expression of x. Thus any set must contain only a finite number of elements. Furthermore, in the second order case, there are two types of theories according to whether we include the smash function in our second order language.

Definition 9. *Let L_2 be the second order language with the following symbols:*

- *functions of L_2 are the functions of L_1 minus $x\#y$,*
- *L_2 has second order variables of the form $X^{p(|t|)}$ where p is a monotone polynomial and t is a term,*
- *predicates of L_2 are $\leq$ and $x \in X^{p(|t|)}$.*

The intended meaning of $X^{p(|t|)}$ is that all elements of X are bounded by $p(|t|)$.

Definition 10. *The sets of L_2 formulae $\Sigma_i^{1,b}$ and $\Pi_i^{1,b}$ $(i \geq 0)$ are defined inductively as follows:*

1. *$\Sigma_0^{1,b} = \Pi_0^{1,b}$ is the set of bounded formulae;*
2. *$\Sigma_{i+1}^{1,b}$ and $\Pi_{i+1}^{1,b}$ are the smallest sets satisfying*
   (a) *$\Sigma_i^{1,b}, \Pi_i^{1,b} \subseteq \Sigma_{i+1}^{1,b}$ and $\Sigma_i^{1,b}, \Pi_i^{1,b} \subseteq \Pi_{i+1}^{b}$,*
   (b) *$\Sigma_{i+1}^{1,b}$ and $\Pi_{i+1}^{1,b}$ are closed under connectives $\wedge$, $\vee$ and first order bounded quantifications,*
   (c) *$\Sigma_{i+1}^{1,b}$ is closed under second order existential quantifications and $\Pi_{i+1}^{1,b}$ is closed under second order universal quantifications,*
   (d) *if $\varphi \in \Sigma_{i+1}^{1,b}$ or $\varphi \in \Pi_{i+1}^{1,b}$ then $\neg\varphi \in \Pi_{i+1}^{1,b}$ and $\neg\varphi \in \Sigma_{i+1}^{1,b}$ respectively,*
   (e) *if $\varphi \in \Pi_{i+1}^{1,b}$ and $\psi \in \Sigma_{i+1}^{1,b}$ then $\varphi \supset \psi \in \Sigma_{i+1}^{1,b}$, the same statement holds if we exchange $\Sigma_{i+1}^{1,b}$ and $\Pi_{i+1}^{1,b}$.*

Definition 11. *Let $BASIC_2$ be a finite set of axioms which defines symbols in L_2.*

Definition 12 (Buss). *For $i \geq 0$, U_1^i is the theory with the following axioms:*

- *$BASIC_2$ axioms*
- *axiom stating that all sets are bounded:*

$$\forall X^{p(|t|)} \forall x(x \in X^{p(|t|)} \rightarrow x < p(|t|))$$

- *$\Sigma_i^{1,b}$-PIND*
- *$\Sigma_0^{1,b}$-CA:*

$$\forall x \exists X^x \forall y < x(y \in X^x \leftrightarrow \varphi(y)),$$

where $\varphi \in \Sigma_0^{1,b}$.

V_1^i is obtained from U_1^i by replacing $\Sigma_i^{1,b}$-PIND with $\Sigma_i^{1,b}$-IND. U_2^i and V_2^i are obtained by adding the smash function $x\#y$ and its defining axioms to U_1^i and V_1^i respectively.

2.7. **Some Properties of Bounded Arithmetic.**

Definition 13. *A function f is Σ_i^b definable in a theory T if for some $\varphi \in \Sigma_i^b$*

- $T \vdash \forall x \exists ! y \varphi(x, y)$,
- $\mathbb{N} \models \forall x \varphi(x, f(x))$.

We denote by $\Sigma_i^b(f)$ the set of Σ_i^b formulae in the lanugage $L_1 \cup \{f\}$. For a theory T we denote by $T(f)$ the theory T in the language $L_1 \cup \{f\}$. Also for a set of functions F, $T(F)$ is the theory in the languages $L_1 \cup \{f : f \in F\}$ together with defining axioms for all $f \in F$.

Proposition 2. *Let f be a Σ_1^b definable function in S_2^1 then $S_2^1(f)$ is a conservative extension of S_2^1.*

Proposition 3. *For $i \geq 1$, $S_2^1 \vdash \Sigma_i^b - LIND \leftrightarrow \Sigma_i^b - PIND$.*

Proposition 4. *For $i \geq 1$, $S_2^i \subseteq T_2^i \subseteq S_2^{i+1}$ and $U_2^i \subseteq V_2^i \subseteq U_2^{i+1}$*

2.8. **Models of Arithmetic.** Finally we state some basic notions and properties of models of arithmetic.

Definition 14. *Let M and N be models of arithmetic in the same languages and Φ be a set of formulae. We say M and N are Φ elementary if for all $\varphi \in \Phi$ $M \models \varphi$ if and only if $N \models \varphi$. M and N are elementary if for any formula truth values coincides.*

Definition 15. *Let M be a model of arithmetic and N be a substructure of M. We say N is a initial segment of M (denoted by $N \subseteq_e M$) if for all $x \in M$ if there exists $y \in N$ such that $x < y$ then $x \in N$.*

Proposition 5. *Let M and N be models of arithmetic with $N \subseteq_e M$ and suppose $\varphi(\vec{x}) \in \Delta_0$ (or Σ_∞^b) with parameters among $\vec{x}$. Then for any $\vec{c} \in N$, $M \models \varphi(\vec{c})$ if and only if $N \models \varphi(\vec{c})$. In words, bounded formulae are absolute between M and N.*

3. Witnessing in Models of Arithmetic

3.1. **Parikh's Theorem.** Before we discuss about witnessing proofs, we first give a model theoretic proof of Parikh's theorem, which might help understanding the details of witnessing. Parikh's theorem was first proved in a proof theoretical manner and soon after that, much simpler model theoretic proof was established. The theorem holds for any bounded theories while we state the case for $I\Delta_0$.

Theorem 1 (Parikh [20]). *Let $\varphi \in \Delta_0$ and suppose $I\Delta_0 \vdash \forall x \exists y \varphi(x, y)$. Then there exists a term $t(x)$ such that $I\Delta_0 \vdash \forall x \exists y \leq t(x) \varphi(x, y)$.*

Proof. For the sake of contradiction suppose for any term $t(x)$,

$$I\Delta_0 \not\vdash \forall x \exists y \leq t(x) \varphi(x, y).$$

Let $t_1(x), t_2(x), \ldots$ be an enumeration of all terms whose only free variable is x. Then for any $n \in \omega$,

$$I\Delta_0 + \neg \exists y \leq t_1(c) \varphi(c, y) + \cdots + \neg \exists y \leq t_n(c) \varphi(c, y)$$

is consistent where c is a new constant symbol. So by compactness

$$I\Delta_0 + \{\neg \exists y \leq t_n(c) \varphi(c, y)\}_{n \in \omega}$$

is also consistent. Let M be a model of this theory and define

$$N = \{a \in M \ : \ M \models a \leq t_n(c) \text{ for some } n \in \omega\}.$$

Then as $N \subseteq_e M$, $N \models I\Delta_0$ and by the definition of N, $N \models \neg\exists y\varphi(c, y)$. □

3.2. **Witnessing proof I.** Now we shall give the first proof of witnessing theorem which can be applied to any Π_1^0 axiomatized theory as the argument utilizes Herbrand's theorem for Π_1^0 axiomatized theories.

Theorem 2 (Herbrand [11]). *Let T be a Π_1^0 axiomatized theories and suppose $T \vdash \forall x\exists y\varphi(x, y)$ where φ is a quantifier free formula. Then there exists a finite number of terms $t_1, \ldots, t_n$ such that*

$$T \vdash \forall x\,[\varphi(x, t_1(x)) \vee \cdots \vee \varphi(x, t_n(x))].$$

Before proving Herbrand's theorem we need the following model theoretic property of Π_1^0 axiomatized theory.

Lemma 1 (Łos and Tarski). *A theory T is Π_1^0 axiomatized if and only if it is closed under substructures, that is, if $M \models T$ and N is a substructure of M then $N \models T$.*

Proof of Herbrand's theorem. The proof proceeds almost parallel to that of Parikh's theorem. For the sake of contradiction suppose

$$T \nvdash \forall x\,[\varphi(x, t_1(x)) \vee \cdots \vee \varphi(x, t_n(x))]$$

for any finite set of terms $t_1, \ldots, t_n$. Then

$$T + \exists x\,[\neg\varphi(x, t_1(x)) \wedge \cdots \wedge \neg\varphi(x, t_n(x))]$$

is consistent. Thus by compactness

$$T + \neg\varphi(c, t_1(c)) + \neg\varphi(c, t_2(c)) + \cdots$$

is consistent where c is a new constant symbol. Let M be a model of this theory and define $N = \{t(c) \ : \ t \text{ is a term}\}$. Then N is a substructure of M. As T is Π_1^0 axiomatized, $N \models T$ by Lemma 1 and by construction $T \models \neg\exists y\varphi(c, y)$. □

Lemma 2. *PV is a Π_1^0 axiomatized theory.*

Proof. It suffices to show that the witness of PIND axiom for quantifier free formulae can be computed by a polynomial time function. This can be done using binary search. That is, suppose $\varphi(0) \wedge \neg\varphi(a)$ holds for a quantifier free formula φ, then using binary search we can compute $x < a$ such that $\varphi(\lfloor a/2 \rfloor) \wedge \neg\varphi(a)$ holds. □

Theorem 3 (Witnessing theorem for PV). *Let $\varphi(x, y) \in \Sigma_1^b$ and suppose $PV \vdash \forall x\exists y\varphi(x, y)$. Then there exists a polynomial time computable function $f \in L_{PV}$ such that $PV \vdash \forall x\varphi(x, f(x))$.*

Proof. First notice that for $\varphi(x, y) \in \Sigma_1^b$ there exists a quantifier free formula $\psi(x, y, z) \in$ such that

$$PV \vdash \forall x, y[\varphi(x, y) \leftrightarrow \exists z\psi(x, y, z)].$$

Suppose $PV \vdash \forall x\exists y\varphi(x, y)$. By the above remark $PV \vdash \forall x\exists y\exists z\psi(x, y, z)$. Let $w = (y, z)$. Then $PV \vdash \forall x\exists w\psi(x, (w)_0, (w)_1)$. Now by Theorem 2, there exists a finite number of functions $f_1, \ldots, f_n \in L_{PV}$ which witnesses w. Since definition by cases can be realized by a polynomial time algorithm, these functions can be combined into a single polynomial time computable function. □

3.3. **Witnessing Proof II.** Next we extend Theorem 3 to the case for S_2^1 as follows:

Theorem 4 (Buss [5]). *Let $\varphi \in \Sigma_1^b$ and assume that $S_2^1 \vdash \forall x \exists y \varphi(x, y)$. Then there exists a polynomial time computable function f such that $PV \vdash \forall x \varphi(x, f(x))$.*

This time a simple application of Herbrand's theorem fails. To see this suppose $PV \not\vdash \varphi(a, f(a))$ for any $f \in L_{PV}$. Then by compactness there exists a model

$$M \models PV + \{\neg\varphi(a, f(a)) \ : \ f \in PTIME\}.$$

Define $M^* = \{f(a) \ : \ f \in PTIME\}$. Unfortunately, we cannot prove that $M^* \models S_2^1$ since S_2^1 is not Π_1^0 axiomatized.

So we need a more complicated construction of a model. This can be achieved by the following chain construction. We will present a method developed by Zambella:

Theorem 5 (Zambella [26]). *Let $M \models PV$ be a countable model. Then there exists another model $M' \models S_2^1(PV)$ such that*

1. *M' is a Σ_1^b elementary extension of M,*
2. *for any open PV formula $\varphi(x, y)$ there exists a PV-term $f(x)$ with only free variable x such that*

$$M' \models \forall x \exists y \varphi(x, y) \rightarrow \forall x \varphi(x, f(x)).$$

Proof Sketch. Let $\varphi_1, \varphi_2, \ldots$ be an enumeration of Σ_1^b formulae. We shall construct a chain of models $M_0, M_1, \ldots$ as follows:

1. $M_0 = M$.
2. To construct M_{k+1} add a witness for φ_k and take the closure under all polynomial time computable functions.

Finally, let

$$M' = \bigcup_{k \in \omega} M_k.$$

Now we claim that $M' \models S_2^1(PV)$. Suppose

$$M' \models \varphi(0) \wedge \forall x < |a|(\varphi(x) \rightarrow \varphi(x+1)).$$

Then we can compute a witness of $\varphi(x+1)$ using a witness of $\varphi(x)$ in M'. Iterating this for $|a|$ times and we have $M' \models \varphi(|a|)$. Thus $M' \models LIND(\varphi)$ for any Σ_1^b formula in the language L_{PV}. Also the second step in the construction of M' can be done so that M_{k+1} is Σ_i^b elementary over M_k for each k. So condition 1 is satisfied. Furthermore, condition 2 is guaranteed since we added witnesses for all $\varphi \in \Sigma_1^b$ in M'. □

Now Theorem 5 implies that S_2^1 is Σ_1^b conservative over PV. So S_2^1 and PV have the same Σ_1^b definable functions.

3.4. **Herbrand Saturated Models.** The above witnessing arguments are simplified by using Herbrand saturated models, a new method developed by J. Avigad [3]. Here we will illustrate how the $\forall\exists\Sigma_1^b$ conservation of S_2^1 over PV is proved.

Definition 16. *Let L be a language of arithmetic and M a L-structure. Then define*

$$L(M) = L \cup \{c \ : \ \textit{constant for each element in } M\}.$$

A type with parametes from M is a set of sentences in and extension of $L(M)$ by finitely many constants. Let Γ be a type with parameters from M. Then Γ is realized in M if there is an interpretation of additional constants in M making every sentence in Γ true. Γ is universal if every sentence in Γ is universal. Furthermore, Γ is principal if Γ consists of a single sentence.

Definition 17. *Let M be a L-structure. M is Herbrand saturated if for any principal universal type if Γ is consistent with the universal diagram of M,that is all true universal sentences in M, then Γ is realized in M.*

Theorem 6. *Every consistent unversal theory T has an Herbrand saturated model.*

Proof Sketch. Let $L_\omega = L \cup \{c_1, c_2, \dots\}$ and $\theta_1(\vec{x_1}, \vec{y_1}), \theta_2(\vec{x_2}, \vec{y_2}), \dots$ be an enumeration of all quantifier free L_ω formulae. Define

$$\begin{aligned} S_0 &= \text{universal axioms of } T, \\ S_{i+1} &= \begin{cases} S_i \cup \{\forall \vec{y_{i+1}} \theta_{i+1}(\vec{c}, \vec{y_{i+1}})\}, & \text{if it is consistent,} \\ S_i, & \text{otherwise.} \end{cases} \end{aligned}$$

Then $S_\omega = \bigcup_{i\in\omega} S_i$ is consistent. Let N be a model of S_ω and define

$$M = \{t^N \ : \ t \in L_\omega\}.$$

Then M is Herbrand saturated and $M \models T$. □

Theorem 7. *Let M be an Herbrand saturated L structure and suppose that $M \models \forall\vec{x}\exists\vec{y}\varphi(\vec{x}, \vec{y}, \vec{a})$ where φ is a quantifier formula and $\vec{a} \in M$. Then there exists an universal formula $\psi(\vec{z}, \vec{w})$ and terms $\vec{t_1}(\vec{z}, \vec{w}), \dots, \vec{t_k}(\vec{z}, \vec{w})$ such that*

$$M \models \exists\vec{w}\psi(\vec{a}, \vec{w})$$

and

$$\models \psi(\vec{z}, \vec{w}) \to \varphi(\vec{x}, \vec{t_1}(\vec{x}, \vec{z}, \vec{w}, \vec{z})) \vee \dots \vee \varphi(\vec{x}, \vec{t_k}(\vec{x}, \vec{z}, \vec{w}, \vec{z})).$$

Proof. Direct application of Herbrand's theorem. □

Theorem 8. *Let T_2 be a universal theory and T_1 be a theory in the language of T_2. Suppose every Herbrand saturated model of T_2 is also a model of T_1. Then every $\forall\exists$ sentence provable in T_1 is also provable in T_2.*

Proof. Suppose every Herbrand saturated model of T_2 is a model of T_1. Let $\varphi(\vec{x}, \vec{y})$ be a quantifier free formula in the language of T_2 such that $T_2 \nvdash \forall\vec{x}\exists\vec{y}\varphi(\vec{x}, \vec{y})$. We claim that $T_1 \nvdash \forall\vec{x}\exists\vec{y}\varphi(\vec{x}, \vec{y})$. Assume that $T_2 \cup \{\forall\vec{y}\neg\varphi(\vec{d}, \vec{y})\}$ is consistent where $\vec{d}$ is new constants. By Theorem 6, there is an Herbrand saturated model M of this theory. So the reduct of M to the language of T_2 is a model of $T_1 \cup \{\forall\vec{y}\neg\varphi(\vec{d}, \vec{y})\}$. Bu assumption this is also a model of T_1. □

Now we will prove our conservation result

Theorem 9. *S^1_2 is conservative over PV for $\forall\exists\Sigma^b_1$ sentences.*

Proof. Let $M \models PV$ be an Herbrand saturated model. Note that such a model exists since PV is an universal theory. By Theorem 8 it suffices to show that $M \models \Sigma^b_1$-LIND. First note that for any Σ^b_1 formula $\psi(x, \vec{z})$ there is a quantifier formula $\varphi(x, y, \vec{z})$ such that

$$PV \vdash \psi(\vec{x}, \vec{z}) \leftrightarrow \exists y\varphi(x, y, \vec{z}).$$

Suppose M satisfies

- $\exists y\varphi(0, y, \vec{a})$ and
- $\forall x(\exists y\varphi(x, y, \vec{a}) \rightarrow \exists y\varphi(x+1, y, \vec{a}))$.

As the second formula is equivalent to

$$\forall x, y\exists y'(\varphi(x, y, \vec{a}) \rightarrow \varphi(x+1, y', \vec{a})),$$

by Theorem 7 we have PV functions f and g such that

- $\exists y\varphi(0, f(\vec{a}, \vec{b_1}, \vec{a}))$ and
- $\forall x\forall y[\varphi(x, y, \vec{a}) \rightarrow \varphi(x+1, g(x, y, \vec{a}, \vec{b_2}), \vec{a})]$.

Now using bounded recursion on notation from f and g yields a function which computes the witness of $\forall x\exists y\varphi(x, y, \vec{a})$. □

4. Translations between First and Second Order Theories

4.1. **RSUV isomorphism.** The RSUV isomorphism clarifies the relation between first order theories and second order theories without the smash function. Intuitively, large numbers of first order world is translated by a finite set and vice versa. More formally, the theorem is stated as follows:

Theorem 10 (Takeuti [25]). *There are translations between first order bounded formulae and second order bounded formulae*

$$A \in \Sigma_{\infty}^{1,b} \mapsto A^1 \in \Sigma_{\infty}^{b} \text{ and } B \in \Sigma_{\infty}^{b} \mapsto B^2 \in \Sigma_{\infty}^{1,b}$$

such that

1. *if* $S_2^i \vdash B$ *then* $V_1^i \vdash B^2$,
2. *if* $V_1^i \vdash A$ *then* $S_2^i \vdash A^1$,
3. $S_2^i \vdash B \equiv (B^2)^1$, *and*
4. $V_1^i \vdash A \equiv (A^1)^2$.

Rather than giving a formal proof of RSUV isomorphism, we shall illustrate how a first order model of S_2^i is translated to a second order model of V_1^i and vice versa. This method is due to Krajíček [17].

First let $M \models S_2^i$. The first order part of our second order model is

$$Log(M) = \{|x| \ : \ x \in M\}.$$

For the second order part, consider pairs of elements of M, $(\alpha, |a|)$. We will regard this as a second order object A by the following correspondence;

$$\forall x < |a|(x \in A \Leftrightarrow Bit(a, x) = 1).$$

To avoid duplication, define

$$(\alpha, |a|) \sim (\beta, |b|) \Leftrightarrow |a| = |b| \wedge \forall x < |a|(Bit(a, x) = Bit(b, x)).$$

Now define $S = \{(\alpha, |a|) \ : \ \alpha, a \in M\}$ and $S^* = S/\sim$. Then

$$(Log(M), S^*) \models V_1^i.$$

Conversely, take $(M, S) \models V_1^i$. This time consider $M = \{(a, \alpha) \ : \ a \in M, \alpha \in S\}$. By a similar argument as above, we obtain a model of V_1^i. □

We also have similar correspondences between other first and second order theories. For example, F. Ferreira defined a string language theory $Th - FO$. This theory have all AC^0 computable functions together with their defining axioms that utilizes a decriptive complexity characterization developed by N. Immerman [12]. Then he showed that

Theorem 11 (Ferreira [9]). *$I\Delta_0$ and $Th - FO$ are isomorphic via RSUV isomorphism.*

4.2. **Restricted Exponentiation.** Now we talk about an isomorphism between first order bounded arithmetic and second order theories with the smash function. So the question is: which theory of first order bounded arithmetic can translate reasonings in second order thories like U_2^i or V_2^i? We shall answer this question by allowing restricted use of exponentiation function in certain first order theories.

Definition 18. *For a bounded arithmetic theory T, the set $T+1$-Exp consists of all Σ_∞^b formulae $\varphi(a)$ such that there is a term $t(a)$ for which T proves the implication*

$$t(a) < |c| \rightarrow \varphi(a)$$

where c is a free variable not occurring in $t(a)$ or φ.

Theorem 12 (Krajíček [17]). *Let $\varphi(a) \in \Sigma_\infty^b$. Then*

$$\varphi(a) \in S_2^i + 1\text{-}Exp \text{ iff } V_2^i \vdash \varphi(a).$$

The same relation holds for R_2^i and U_2^i in place of S_2^i and V_2^i respectively.

Proof. Assume that $V_2^i \nvdash \varphi(a)$. Then there is a model

$$(K, S) \models V_2^i + \neg\varphi(a).$$

The same construction as in the proof of Theorem 10 yields a model $M \models S_2^i$ with $Log(M) = K$. Assume

$$S_2^i \vdash t(a) < c \rightarrow \varphi(a).$$

Since $(K, S) \models V_2^i$, $t(m) \in K$, so $2^{t(m)} \in M$. Hence $\varphi(m)$ holds in M. As K is an initial segment of M and φ is a bounded formula, it must be that $K \models \varphi(m)$, which is a contradiction.

For the converse implication, assume that $\varphi(a) \notin S_2^i + 1$-$Exp$. By compactness we have a model $M \models S_2^i$ with a cut $I \subseteq_e M$ such that

1. $I \models S_2^i$,
2. $\exists c \in M \setminus I \forall b \in I, M \models 2^b < c$.

Let

$$S = \{\alpha \subseteq I \ : \ \alpha \text{ is coded by some } a \in M, M \models a \leq c\}.$$

Now it is readily proved that $(I, S) \models V_2^i$. □

Problem 1. *Which second order bounded arithmetic is equivalent to the theory $AC^0CA + 1$-Exp in the sense of previous theorem, where AC^0CA is the theory with axioms for all AC^0 definable functions together with polynomial induction for Σ_0^b formulae?*

In the next section we will use a similar translation of models to show that certain initial segment of a model of S_2^1 can be used to constract a second order

5. Substructures of Models of Bounded Arithmetic

Now we will consider much deeper analysis of models of bounded arithmetic. One of fundamental problems in "classical" theories of models of arithmetic like Peano arithmetic concerned about a model and its initial segment. For example there are problems like

1. for a model $M \models PA$ does there exist $N \subset_e M$ such that $N \models PA$?
2. for a model $M \models PA$ does there exist $M \subset_e N$ such that $N \models PA$?

In the context of bounded arithmetic, these questions are almost nonsense since we talk only about bounded formulae in our theories while bounded formulae are absolute between a model and its initial segment. Thus we need a sharper notion of initial segment to argue in the case for bounded arithmetic.

In this section we introduce two attempts for defining such notions of substructures.

5.1. Length Initial Substructures.

The first notion, length initial substructure, is introduced by J. Johannsen in order to give a model theoretical proof of the following theorem:

Theorem 13 (Takeuti [23]). $S_2^0 \not\vdash \forall x(x = 0 \vee \exists y(y = Sx))$.

He also proved similar independence results concerning systems S_2^0 and the following theories:

Definition 19. *R_2^0 is the theory obtained from S_2^0 by adding subtraction and MSP function defined by*

$$\begin{aligned} MSP(x,0) &= x, \\ MSP(x,i+1) &= \lfloor MSP(x,i)/2 \rfloor. \end{aligned}$$

L_2^0 is obtained from S_2^0 by replacing Σ_0^b-PIND by Σ_0^b-LIND.

Theorem 14 (Johannsen [14],Tada and Tatsuta [22]). *For $k \in \omega$, R_2^0 proves*

$$\forall x \exists y (y = \lfloor x/k \rfloor)$$

if and only if k is a power of 2.

Theorem 15 (Johannsen [13]). $L_2^0 \not\vdash \Sigma_0^b$*-PIND.*

We first introduce the key notion to prove above three theorems in a single method.

Definition 20 (Johannsen [13]). *Let M be a model of bounded arithmetic and N a substructure of M. N is called a length initial substructure of M, denoted by $N \subseteq_l M$, if*

$$\forall x \in M \exists y \in N (x \leq |y| \to x \in N).$$

There is a close similarity between length initial substructures and initial segments.

Proposition 6. *Let $N \subseteq_l M$ and $\varphi \in \Sigma_0^b$. Then for all $\vec{a} \in N$,*

$$N \models \varphi(\vec{a}) \text{ if and only if } M \models \varphi(\vec{a}).$$

Proof. By induction on the complexity of φ. □

Note that L_2^0 is a $\forall\Sigma_0^b$ axiomatized theory and also

Proposition 7. *R_2^0 is $\forall\Sigma_0^b$ axiomatized.*

Proof. R_2^0 we can be axiomatized by Σ_0^b-LIND since we have subtraction and MSP function. □

Thus if for example $M \models S_2^1$ and $N \subseteq_l M$ then it must be that $N \models R_2^0$. So to show that these theories it suffices to construct a length initial substructure in which the predecessor or division cannot be defined:

Lemma 3. *For some $M \models S_2^1$ there exist length initial substructure N_1 and N_2 of M such that*

1. $N_1 \models \forall x \exists y(x = y + 1)$,
2. $N_2 \models \forall x \exists y(y = \lfloor x/k \rfloor)$.

Proof. Take $M \models S_2^1$ to be such that $\log(M) \neq M$ and $\log(M)$ is closed under $\#$. Define

$$\begin{aligned} N_1 &= \{a \in M \ : \ count(a) \leq ||b|| \text{ for some } b \in M\}, \\ N_2 &= \{a \in M \ : \ blk(a) \leq ||b|| \text{ for some } b \in M\}, \end{aligned}$$

where

$$\begin{aligned} count(a) &= \#i < |a|(Bit(a,i) = 1), \\ blk(a) &= \#i < |a|(Bit(a,i) \neq Bit(a,i+1)). \end{aligned}$$

Furthermore, N_1 satisfies S_2^0. □

On the other hand,

Lemma 4. *Let $M \models S_2^1 + \Omega_2 + \neg Exp$. Then there is a length initial substructure N of M which does not satisfy S_2^0.*

Proof. For $x \in M$ and $n \in \mathbb{N}$ define

$$\begin{aligned} x^{\#0} &= 1, \\ x^{\#1} &= x, \\ x^{\#(n+1)} &= x^{\#n}\#x. \end{aligned}$$

Choose a large $a \in M$ and define

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

□

Problem 2. *Let $p, q \in \omega$ be relatively prime. Show that*

$$R_2^0 + \forall x \exists y(y = \lfloor x/p \rfloor) \nvdash \forall x \exists y(y = \lfloor x/q \rfloor).$$

Theorem 14 can be extended to a independence for second order theory T^{pol}.

Definition 21. *$\Sigma_i^{1,w}$ and $\Pi_i^{1,w}$ are defined inductively as follows:*

1. *$\Sigma_0^{1,w} = \Pi_0^{1,w}$ is the set of sharply bounded formula with possibly second order free variables.*
2. *$\Sigma_i^{1,w} \subseteq \Pi_{i+1}^{1,w}$ and $\Pi_i^{1,w} \subseteq \Sigma_{i+1}^{1,w}$.*
3. *$\Sigma_i^{1,w}$ and $\Pi_i^{1,w}$ are closed under conjunction disjunction and first order sharply bounded quantification.*
4. *$\Sigma_{i+1}^{1,w}$ is closed under second order existential quantification $\exists X^{p(|t|)}$ and $\Pi_{i+1}^{1,w}$ is closed under second order universal quantification $\forall X^{p(|t|)}$.*

Let $\Sigma_\infty^{1,w} = \bigcup_{i \in \omega} \Sigma_i^{1,w}$.

Definition 22 (Clote and Takeuti [7]). *T^{pol} is the theory in the language of R_2^0 extended by second order variables which consists of the following axioms:*

- *BASIC axioms*
- *bounding sets axiom: $\forall X^{p(|t|)}(x \in X \to x \le p(|t|))$*
- *$\Sigma_1^{1,w}$-LIND*

T^{pol+} is the theory T^{pol} extended by the binary counting function

$$count(x) = \#\{i < |x| \ : \ Bit(x,i) = 1\}.$$

Lemma 5 (Kuroda [19]). *Let $M \models S_2^1$ and $N \subseteq_I M$. Then there exists $S \subseteq P(N)$ such that $(M,S) \models T^{pol+}$.*

To prove the lemma, we use a similar translation as used in the previous section.

Definition 23. *The TS-translation is the mapping of a $\Sigma_\infty^{1,w}$ formula φ into a Σ_∞^b formula φ^{TS} defined inductively as follows:*

- *if φ is a first order atomic formula then $\varphi^{TS} \equiv \varphi$.*
- *if $\varphi \equiv x \in X^{p(|t|)}$ then $\varphi^{TS} \equiv (x \le p(|t|) \wedge Bit(a_X, x) = 1)$.*
- *if $\varphi \equiv \varphi_0 \wedge \varphi_1, \varphi_0 \vee \varphi_1$ or $\neg\varphi_0$, then $\varphi^{TS} \equiv {\varphi_0}^{TS} \wedge {\varphi_1}^{TS}, {\varphi_0}^{TS} \vee {\varphi_1}^{TS}$ or $\neg{\varphi_0}^{TS}$ respectively.*
- *if $\varphi \equiv \forall x \le |t|\varphi_0(x)$ or $\exists x \le |t|\varphi_0(x)$ then $\varphi^{TS} \equiv \forall x \le |t|\varphi_0(x)^{TS}$ or $\exists x \le |t|\varphi_0(x)^{TS}$ respectively.*
- *if $\varphi \equiv \forall X^{p(|t|)}\varphi_0(X)$ or $\exists X^{p(|t|)}\varphi_0(X)$ then $\varphi^{TS} \equiv \forall x \le 2^{p(|t|)}\varphi_0(x)^{TS}$ or $\exists x \le 2^{p(|t|)}\varphi_0(x)^{TS}$ respectively.*

Proof of Lemma 5. Let M and N be as above. We say that $a \in M$ is an N-code if there exists $X \subseteq N$ such that

$$\forall i < |a|(Bit(a,i) = 1 \leftrightarrow i \in X).$$

Let

$$S_N := \left\{ \langle p(|b|), a\rangle \ : \ \begin{array}{l} p \text{ is a polynomial, } b \in N \text{ and} \\ a \text{ is an } N\text{-code} \end{array} \right\}.$$

Define the equivalence relation on S_N by

$$\begin{array}{l} \langle p(|b_1|), a_1\rangle =_2 \langle p(|b_2|), a_2\rangle \\ \Leftrightarrow p(|b_1|) = p(|b_2|) \wedge \forall i < p(|b_1|)(Bit(a_1,i) = Bit(a_2,i)). \end{array}$$

Finally let $S_N^* := S_N / =_2$. Note that each element in S_N^* can be identified with a finite subset of N in the sense of M in a natural way. Thus we may consider S_N^* as a subset of $P(N)$.

By induction on the complexity of $\varphi \in \Sigma_\infty^{1,w}$ we shall show that $(N, S_N^*) \models \varphi(A^{p(|t|)})$ if and only if $M \models \varphi^{TS}(a_A)$, with a suitable assignment $A \mapsto a_A$ from S_N^* into M. For the base case, it suffices to consider the case where $\varphi(A^{p(|t|)}) \equiv c \in A^{p(|t|)}$. Let $\langle p(|t|), a\rangle$ represent $A^{p(|t|)} \in S_N^*$. By putting $a_A = a$ we have

$$(N, S_N^*) \models c \in A^{p(|t|)} \text{ iff } M \models (c \le p(|t|) \wedge Bit(a_A, c) = 1).$$

For the induction step, the case where the outermost connective is either a logical connective or a first order sharply bounded quantifier is trivial. Let $(N, S_N^*) \models \exists X^{p(|t|)}\varphi(X^{p(|t|)})$. Then $(N, S_N^*) \models \varphi(A^{p(|t|)})$ for some $A^{p(|t|)} \in S_N^*$. By the inductive hypothesis, we have $M \models \left(\varphi^{TS}(a_A) \wedge a_A \le 2^{p(|t|)}\right)$ for the same a_A as above. Thus $M \models \exists x \le 2^{p(|t|)}\varphi^{TS}(x)$. The case for second order universal quantifier is treated similarly, thus we have proved the claim.

Now we claim that $(N, S_N^*) \models T^{pol+}$. First note that $N \models BASIC^+$. So $(N, S_N^*) \models BASIC^+$. By definition of S_N^* it is also straightforward to see that

$$(N, S_N^*) \models \forall X^{p(|t|)} \forall x (x \in X^{p(|t|)} \to x \leq p(|t|)).$$

For $\Sigma_1^{1,w}$-LIND we consider the equivalent scheme

$$LIND_a(\varphi) \equiv \varphi(0) \wedge \forall x < |a| (\varphi(x) \to \varphi(x+1)) \to \varphi(|a|).$$

Assume $(N, S_N^*) \models \neg LIND_a(\varphi)$ for some $\varphi \in \Sigma_1^{1,w}$. Note that $\neg LIND_a(\varphi) \in \Sigma_\infty^{1,w}$. So applying TS-translation yields $(\neg LIND_a(\varphi))^{TS}$ with $M \models (\neg LIND_a(\varphi))^{TS}$. It is easy to see that $(\neg LIND_a(\varphi))^{TS} \equiv \neg LIND_a(\varphi^{TS})$. Thus $M \models \neg LIND_a(\varphi^{TS})$ and as $\varphi^{TS} \in \Sigma_1^b$, this contradicts to the assumption that $M \models S_2^1$. □

Thus we have

Theorem 16 (Kuroda [18]). *T^{pol+} cannot define the function $\lfloor x/k \rfloor$ for k not a power of 2.*

This improves the result by Takeuti [24].

Concerning length initial substructures, following questions are of interest:

Problem 3. *Find necessary and sufficient conditions for*

1. *for all $M \models R_2^0$ there is $N \models S_2^1$ such that $M \subseteq_l N$,*
2. *for all $M \models S_2^1$ there is $N \models S_2^1$ such that $M \subseteq_l N$,*
3. *for all $M \models R_2^0$ there is $N \models T_2^1$ such that $M \subseteq_l N$,*

Note that the unconditional positive solution to the first problem implies the first order conservation of T^{pol} over R_2^0.

5.2. **Weak end extension.** The second variation is motivated by so-called end extension problem. An example of bounded arithmetic version is the following:

Problem 4. *Are there models of $I\Delta_0 + B\Sigma_1$ without proper end-extension to models of $I\Delta_0$?*

Z. Adamowicz found a partial solution to this problem.

Theorem 17 (Adamowicz [1]). *There exists a Π_1 sentence τ such that there is a model of $I\Delta_0 + \Omega_1 + \tau + B\Sigma_1$ without proper end-extensions to models of $I\Delta_0 + \Omega_1 + \tau$.*

Turning our attension to the model of Buss-like systems, Beckmann defined the following weaker notions of end extensions.

Definition 24 (Beckmann [4]). *Let M be a model of bounded arithmetic.*

1. *A model M is 0^b-unincreasable with respect to T if there are no Σ_0^b elementary extension to models of T.*
2. *Let M be a substructure of N. Then M is log-proper if* $\log(M) \neq \log(N)$.
3. *M is a weak end extension of N, denoted by $M \subseteq_e^w N$ if $M \subseteq_e N$ and* $\log(M) \subseteq_e \log(N)$.
4. *M is 1^b-closed with respect to T if for all $N \models T$ whenever N is an Σ_0^b elementary extension of M then N is Σ_1^b elementary.*

The following implication is an direct consequence from the definition.

Proposition 8. *If M is 0^b-unincreasable with respect to T then M is 1^b-closed with respect to T and also M does not have weak end extension to models of T.*

More interesting is the following:

Definition 25. *Let $BL\Sigma_1^b$ denote the following bounded collection schema:*

$$\forall x \leq |t| \exists y \varphi(x,y) \rightarrow \exists z \forall x \leq |t| \exists y \leq z \varphi(x,y),$$

where $\varphi \in \Sigma_1^b$.

Theorem 18 (Buss [6]). *For $i \geq 1$, $S_2^i + BL\Sigma_1^b$ is $\forall\Pi_1^b$ conservative over S_2^i.*

Theorem 19 (Beckmann [4]). *Let $1 \leq i \leq j$. Then the following conditions are equivalent:*

1. *T_2^j is not $\forall\Pi_1^b$ conservative over S_2^i,*
2. *there is a model M of S_2^i which is log-proper and 0^b-unincreasable with respect to T_2^j,*
3. *there is a model M of $S_2^i + \Omega_1^{nst}$ which is 1^b-closed with respect to T_2^j, where*

$$\Omega_1^{nst} \equiv \exists c \left[\bigwedge_{k \in \omega} (k < c) \wedge \forall x \exists y (||x|| \cdot c = ||y||) \right],$$

4. *there is a countable model M of $S_2^i + BL\Sigma_1^b$ without weak end extensions to models of T_2^j.*

References

[1] Z. Adamowicz. *A Contribution to the End-extension Problem and the Π_1 Conservativeness Problem.* Annals of Pure and Applied Logic 61 (1993) 3–48.

[2] M. Ajtai. *The Complexity of the Pigeonhole Principle.* In Proc. of the IEEE 29th Annual Symposium on Foundations of Computer Science. (1988) 346–355.

[3] J. Avigad. *Saturated Models of Universal Theories.* Preprint. (2000).

[4] A. Beckmann. *Modeltheoretic Characterizations of $\forall\Pi_1^b$-Separations in Bounded Arithmetic.* Preprint. (2000).

[5] S. R. Buss. *Bounded Arithmetic.* Bibliopolis. (1986).

[6] S. R. Buss. *A Conservation Result Concerning Bounded Theories and the Collection Axiom.* Proceedings of American Mathematical Society. 100 (1987) 709–715.

[7] P. Clote and G. Takeuti. *Bounded arithmetic for NC, AlogTIME, L and NL.* Annals of Pure and Applied Logic. 56 (1992) 73–117.

[8] S.A. Cook. *Feasibly Constructive Proofs and the Propositional Calculus.* In Proc. of the 7th Annual ACM Symposium on Theory of Computing. (1975) 83–97.

[9] F. Ferreira. *On end-extensions of models of* $\neg$exp, Math. Log. Quart., 42, 1996, 1–18.

[10] P. Hájek and P. Pudlák. *Metamathematics of First Order Arithmetic.* Springer-Verlag. (1991).

[11] J. Herbrand. *Recherches sur la théorie de la démonstartion.* Prace Towarzystwa Naukowego Warszawskiego vol. III no. 33 (1930).

[12] N. Immerman. *Expressibility and parallel complexity,*SIAM J. Comput. (1989) 625–638.

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

[14] J. Johannsen. *A model-theoretic property of sharply bounded formulae, with some applications.* Mathematical Logic Quarterly. 44 (1998) 205–215.

[15] J. Johannsen. *A remark on independence results for sharply bounded arithmetic.* Mathematical Logic Quarterly. 44 (1998) 569–571.

[16] R. Kaye *Models of Peano Arithmetic.* Oxford University Press. (1991).

[17] J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Computational Complexity.* Cambridge University Press. (1995).

[18] S. Kuroda. *On a theory for AC^0 and the Strength of the Induction Scheme.* Mathematical Logic Quarterly. 44 (1998) 417–426.

[19] S. Kuroda. *An Independence Result on Weak Second Order Bounded Arithmetic.* To appear in Mathematical Logic Quarterly. (2001)

[20] R. Parikh *Existence and Feasibility in Arithmetic.* Journal of Symbolic Logic. 36 (1971) 494–508.

[21] J. Paris and A. Wilkie. *On the Scheme of Induction for Bounded Arithmetic Formulas.* Annals of Pure and Applied Logic. 35 (1987) 261-302.

[22] M. Tada and M. Tatsuta. *The Function $\lfloor a/m \rfloor$ in Sharply Bounded Arithmetic.* Archive for Mathematical Logic. 37 (1997) 51–57.

[23] G. Takeuti. *Sharply Bounded Arithmetic and the Function $a-1$.* In: Logic and Computation, Contemporary Mathematics. 106 (1990) 281–288.

[24] G. Takeuti. *A second order version of S_2^i and U_2^1.* Journal of Symbolic Logic. 56 (1991) 1038–1063.

[25] G. Takeuti. *RSUV Isomorphism.* In Arithmetic, Proof Theory and Computational Complexity. Clarendon Press. (1993) 364–386.

[26] D. Zambella. *Notes on Polynomially Bounded Arithmetic.* Journal of Symbolic Logic. 61 (1996) 942–966.