

## 6.2. Effectivity.

We begin with a straightforward effectivity result concerning Propositions A-H. Specifically, we show that Propositions A-H hold in the arithmetic sets. Later we will show that Propositions C,E-H hold in the recursive sets.

We don't know if any or all of Propositions A,B,D hold in the recursive sets. We conjecture that

- i. None of Propositions A,B,D hold in the recursive sets.
- ii. This fact can be proved in  $ACA'$ .

DEFINITION 6.2.1. Let  $ACA^+$  be the formal system consisting of  $ACA_0$  and "for all  $x \subseteq \omega$ , the  $\omega$ -th Turing jump of  $x$  exists".

See [Si99,09], p. 404, where  $ACA^+$  is written as  $ACA_0^+$ .  $ACA^+$  is a proper extension of  $ACA'$  that allows us to handle  $\omega$  models of  $ACA_0$ .

Note that the countable  $\omega$  models of  $ACA_0$ ,  $ACA'$ ,  $ACA$  are the same as the countable families of subsets of  $\mathbb{N}$  that are closed under relative arithmeticity, as induction is automatic in  $\omega$  models. (Here  $ACA$  is  $ACA_0$  with induction for all formulas, and is a proper extension of  $ACA'$ ).

THEOREM 6.2.1. Let  $X$  be any of Propositions A-H. The following are provably equivalent in  $ACA^+$ .

- i.  $X$  is true.
- ii.  $X$  is true in the arithmetic sets.
- iii.  $X$  is true in every countable  $\omega$  model of  $ACA_0$ .
- iv.  $X$  is true in some countable  $\omega$  model of  $ACA_0$ .
- v.  $1-Con(MAH)$ .
- vi.  $1-Con(SMAH)$ .

Proof: Let  $X$  be as given. We argue in  $ACA^+$ . By Theorems 5.9.11, 6.1.2, and 6.1.10,  $X$  is equivalent to  $1-Con(MAH)$ ,  $1-Con(SMAH)$ . Hence i,v,vi are equivalent. It suffices to prove  $vi \rightarrow iii \rightarrow ii \rightarrow iv \rightarrow vi$ .

Since  $ACA'$  proves  $X$  is equivalent to  $1-Con(SMAH)$ , we see that in any  $\omega$  model of  $ACA_0$ ,  $X$  is equivalent to  $1-Con(SMAH)$ .

For  $vi \rightarrow iii$ , suppose  $1-Con(SMAH)$ . Then  $1-Con(SMAH)$  is true in any  $\omega$  model of  $ACA_0$ . Hence  $X$  is true in every  $\omega$  model of  $ACA_0$ , and therefore  $iii,ii,iv$ .

iii  $\rightarrow$  ii  $\rightarrow$  iv is trivial.

For iv  $\rightarrow$  vi, suppose  $X$  is true in some countable  $\omega$  model of  $ACA_0$ . Then  $1\text{-Con}(\text{SMAH})$  is true in some  $\omega$  model of  $ACA_0$ . Hence  $1\text{-Con}(\text{SMAH})$ . QED

We are now going to show that Propositions C,E-H hold in the recursive subsets of  $N$ . Propositions C,E-H, when stated in the recursive sets, become  $\Pi_4^0$  statements.

We shall see that Propositions C,E-H hold in the smaller family of infinite sets with primitive recursive enumeration functions.

We also show that all of these variants of C,E-H are provably equivalent to  $1\text{-Con}(\text{SMAH})$  in  $ACA'$ .

We conjecture that a more careful argument will show that Propositions C,E-H hold in the yet smaller family of infinite superexponentially Presburger sets. In light of the primitive recursive decision procedure for superexponential Presburger arithmetic, Propositions C,E-H, when stated in the superexponentially Presburger sets, become  $\Pi_2^0$  statements. This topic will be discussed at the end of this section.

Recall  $\text{TM}(0,1,+,-,\cdot,\uparrow,\log)$ ,  $\text{ETM}(0,1,+,-,\cdot,\uparrow,\log)$ ,  $\text{BAF}$ ,  $\text{EBAF}$ , from Definitions 5.1.1 - 5.1.7. According to Theorem 5.1.4,  $\text{BAF} = \text{EBAF}$ .

DEFINITION 6.2.2. Sometimes we will omit some items among  $0,1,+,-,\cdot,\uparrow,\log$  when using this notation. E.g., terms in  $\text{TM}(0,1,+,-)$  use only  $0,1,+,-$ , and not  $\cdot,\uparrow,\log$ . E.g., terms and formulas in  $\text{ETM}(0,1,+)$  use only  $0,1,+$ . In  $\text{ETM}(\underline{\quad})$  we always use  $<,=$  as the relations for the quantifier free formulas.

We will develop explicit infinite sets of indiscernibles for functions in  $\text{BAF}$ , in the appropriate sense, using iterated base 2 exponentials. It is particularly convenient to use the following definition for our purposes.

DEFINITION 6.2.3. Let  $f:N^k \rightarrow N$ . An SOI for  $f$  is a set  $A \subseteq N$  such that for all  $x,y \in A^k$ ,

if  $x,y \in A^k$  are order equivalent

(i.e., have the same order type)  
 then  $f(x)$  and  $f(y)$  have the same sign  
 (i.e., either  $> 0$  or  $= 0$ ).

We first define the set of functions  $\Gamma(\mathfrak{R})$ . For this purpose, we take  $+', -, \uparrow'$  to be the ordinary addition, subtraction, and base 2 exponentiation functions from  $\mathfrak{R}^2$  into  $\mathfrak{R}$  ( $\uparrow'$  maps  $\mathfrak{R}$  into  $\mathfrak{R}$ ).

It will be important to recall that, according to section 5, we use  $+, -, \cdot, \uparrow, \log$  for functions from and into  $N$ , where  $-, \log$  are modified so that they are  $N$  valued. We call this  $N$  arithmetic.

On the other hand,  $+', -, \uparrow'$  take arguments and values from  $\mathfrak{R}$ , and we call this  $Z$  arithmetic.

In this section, we will not use real numbers after we have proved Lemma 6.2.6.

DEFINITION 6.2.4.  $\Gamma(\mathfrak{R})$  is the set of all functions from  $\mathfrak{R}$  into  $\mathfrak{R}$  that are given by terms in  $0, 1, +', -, \uparrow'$  in only the variable  $x$ .

DEFINITION 6.2.5. By positive, we will always mean  $> 0$ . By negative, we will always mean  $< 0$ .

LEMMA 6.2.2. Every function in  $\Gamma(\mathfrak{R})$  is eventually positive, eventually negative, or eventually zero.

Proof:  $\Gamma(\mathfrak{R})$  is a small fragment of what are called the exp-log functions. Thus the statement is a special case of a well known theorem of Hardy from [Ha10]. QED

LEMMA 6.2.3. Let  $f: N \rightarrow N$  be given by a term in  $TM(0, 1, +, -, \uparrow)$ . There exists  $f^* \in \Gamma(\mathfrak{R})$  such that for sufficiently large  $x \in N$ ,  $f(x) = f^*(x)$ .  $f$  is eventually positive or eventually zero.

Proof: By induction on  $t \in TM(0, 1, +, -, \uparrow)$ . Suppose that we have defined  $r^*$  with the required property, for all terms  $r$  in  $TM(0, 1, +, -, \uparrow)$  with less symbols than  $t$  has.

case 1.  $t$  is  $0, 1, v$ . Set  $t^* = t$ .

case 2.  $t$  is  $s \uparrow$ . Set  $t^* = s^* \uparrow$ .

case 3.  $t$  is  $r$ - $s$ . By the induction hypothesis, for sufficiently large  $x \in \mathbb{N}$ ,  $t(x) = r^*(x) - s^*(x)$ . By Lemma 6.2.2,  $r^*(x) - s^*(x)$  is either eventually  $\geq 0$  or eventually  $< 0$ . In the former case, set  $t^* = r^* - s^*$ . In the latter case, set  $t^* = 0$ .

The final claim follows from the first claim and Lemma 6.2.2. QED

LEMMA 6.2.4. Let  $f: \mathbb{N} \rightarrow \mathbb{N}$  be given by a term in  $\text{ETM}(0, 1, +, -, \uparrow)$ . There exists  $f^* \in \Gamma(\mathfrak{R})$  such that for sufficiently large  $x \in \mathbb{N}$ ,  $f(x) = f^*(x)$ .  $f$  is eventually positive or eventually zero.

Proof: We first claim the following. Let  $\varphi(v)$  be a quantifier free formula in  $0, 1, +, -, \uparrow, <$ . Then either  $\varphi(x)$  is true for all sufficiently large  $x \in \mathbb{N}$ , or  $\varphi(x)$  is false for all sufficiently large  $x \in \mathbb{N}$ . The claim is proved by induction on  $\varphi$ .

The atomic cases are  $s(x) < t(x)$ ,  $s(x) = t(x)$ . In either case, apply Lemma 6.2.3 to  $s(x) - t(x)$  and  $t(x) - s(x)$ . Then

$s(x) - t(x)$  is eventually positive or eventually zero.  
 $t(x) - s(x)$  is eventually positive or eventually zero.

If  $s(x) - t(x)$  is eventually positive then  $s(x) < t(x)$  and  $s(x) = t(x)$  are eventually false. If  $t(x) - s(x)$  is eventually positive then  $s(x) < t(x)$  is eventually true and  $s(x) = t(x)$  is eventually false.

Suppose  $s(x) - t(x)$  is not eventually positive and  $t(x) - s(x)$  is not eventually positive. Then  $s(x) - t(x)$  and  $t(x) - s(x)$  are both eventually zero. Hence  $s(x) = t(x)$  eventually holds. This establishes the claim.

Now write  $f$  as an extended term  $t$  from  $\text{ETM}(0, 1, +, -, \uparrow)$ , according to Definition 5.1.5. We can assume that  $t$  has at most the variable  $v$  and does not use  $\cdot, \log$ . Apply the claim to each of the finitely many cases in  $t$ . Then only one case applies for all sufficiently large  $x \in \mathbb{N}$ . Let this be the  $j$ -th case,  $1 \leq j \leq n+1$ . Then  $t = t_j$  holds eventually. Apply Lemma 6.2.3 to  $t_j$ . QED

The structure  $(\mathbb{N}, +)$  has been extensively studied, and its first order theory is called Presburger arithmetic. It has a well known decision procedure, conducted well within PRA.

This is proved using quantifier elimination in an expanded language. See [Pr29], [En72].

The structure  $(\mathbb{N}, +, \uparrow)$  has also been studied, and its first order theory is called (base 2) exponential Presburger arithmetic. It also has a decision procedure, conducted well within PRA. Again this is proved using quantifier elimination in an expanded language. See [Se80], [Se83], [CP85]. Appendix B provides a self contained exposition of this result by F. Point.

DEFINITION 6.2.6. Recall from Definition 5.3.6 that  $\uparrow p$  is  $0 \uparrow \dots \uparrow$ , and  $\uparrow p(n) = n \uparrow \dots \uparrow$ , where there are  $p$   $\uparrow$ 's,  $p \geq 0$ .  $\uparrow 0 = 0$ . For  $E \subseteq \mathbb{N}$ , define

$$\begin{aligned} \uparrow E &= \{\uparrow p : p \in E\}, \text{ for } E \subseteq \mathbb{N}. \\ \text{mesh}(E) &= \min(E \cup \{x-y > 0 : x, y \in E\}). \end{aligned}$$

THEOREM 6.2.5. The first order theory of the structure  $(\mathbb{N}, +, \uparrow)$  is primitive recursive. Suppose the sentence  $(\forall n_1, \dots, n_k) (\exists m) (\varphi(n, m))$  holds in  $(\mathbb{N}, +, \uparrow)$ . There exists  $p \geq 1$  such that  $(\forall n_1, \dots, n_k) (\exists m \leq \uparrow p(|n_1, \dots, n_k|)) (\varphi(n, m))$  holds in  $(\mathbb{N}, +, \uparrow)$ .

Proof: This result first appeared in [Se80] and [Se83]. It is implicit in [CP86]. For a clearer, self contained exposition, see Theorem 3.3 in Appendix B by F. Point. QED

Recall the definition of an SOI for  $f: \mathbb{N}^k \rightarrow \mathbb{N}$ . It is convenient to use the following weaker notion.

DEFINITION 6.2.7. Let  $f: \mathbb{N}^k \rightarrow \mathbb{N}$ . A restricted SOI for  $f$  is a set  $A \subseteq \mathbb{N}$  such that for all  $x, y \in A^k$ ,

$$\begin{aligned} &\text{if } x, y \in A^k \text{ are each strictly increasing} \\ &\text{then } f(x) \text{ and } f(y) \text{ have the same sign} \\ &\text{(either } > \text{ or } = \text{)}. \end{aligned}$$

LEMMA 6.2.6. Let  $f: \mathbb{N}^k \rightarrow \mathbb{N}$  be given by a term in  $\text{TM}(0, 1, +, -, \uparrow)$ . If  $\text{mesh}(A)$  is sufficiently large then  $\uparrow A$  is a restricted infinite SOI for  $f$ .

Proof: We prove by induction on  $k \geq 1$  that this is true for all such  $f: \mathbb{N}^k \rightarrow \mathbb{N}$ . For  $k = 1$ , let  $f: \mathbb{N} \rightarrow \mathbb{N}$  be as given. By Lemma 6.2.4, let  $t$  be such that  $f$  has constant sign on  $[t, \infty)$ . Then for  $\text{mesh}(A) \geq t$ ,  $\uparrow A$  is a restricted infinite SOI for  $f$ .

Now fix  $k \geq 1$ , and let  $f: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  be as given. By Lemma 6.2.4,

$$(\forall x \in \mathbb{N}^k) (\exists t \in \mathbb{N}) \\ (f(x, m) \text{ has constant sign for } m \geq t).$$

By Lemma 6.2.5, let  $p \in \mathbb{N}$  be such that

$$(\forall x \in \mathbb{N}^k) \\ (f(x, m) \text{ has constant sign for } m \geq \uparrow p(|x|)).$$

$$1) (\forall x \in \mathbb{N}^k) \text{ (the eventual sign of } f(x, \_) \\ \text{is the sign of } f(x, \uparrow p(|x|)).$$

We now apply the induction hypothesis to the  $k$ -ary function  $f(x, \uparrow p(|x|))$  to obtain the following.

$$2) (\forall A \subseteq \mathbb{N}) \text{ (mesh}(A) \text{ sufficiently large} \rightarrow \\ (\forall x, y \in (\uparrow A)^k) \text{ (} x, y \text{ strictly increasing} \rightarrow \\ f(x, \uparrow p(|x|), g(y, \uparrow p(|y|)) \text{ have the same sign)).}$$

By 1), 2),

$$3) (\forall A \subseteq \mathbb{N}) \text{ (mesh}(A) \text{ sufficiently large} \rightarrow \\ (\forall x, y \in (\uparrow A)^k) \text{ (} x, y \text{ strictly increasing} \rightarrow \\ f(x, x'), f(y, y') \text{ have the same sign} \\ \text{provided } x' \geq \uparrow p(|x|), y' \geq \uparrow p(|y|)).$$

We now claim that

$$(\forall A \subseteq \mathbb{N}) \text{ (mesh}(A) \text{ sufficiently large} \rightarrow \\ A \text{ is a restricted SOI for } f).$$

To see this, let  $\text{mesh}(A)$  be sufficiently large, and  $x, y \in (\uparrow A)^{k+1}$  be strictly increasing. Then

$$4) x_1 < \dots < x_k, \text{ and } x_{k+1} > \uparrow p(|x_1, \dots, x_k|). \\ y_1 < \dots < y_k, \text{ and } y_{k+1} > \uparrow p(|y_1, \dots, y_k|).$$

This is because we can write

$$|x_1, \dots, x_k| = \uparrow u, x_{k+1} = \uparrow v, u, v \in A, \\ \text{where } v-u \text{ is sufficiently large.} \\ v-u > p. \\ \uparrow p(|x_1, \dots, x_k|) = \uparrow p(\uparrow u) = \uparrow(p+u) \\ < \uparrow v = \uparrow p(|x_1, \dots, x_k|).$$

By 3), 4),

$$f(x_1, \dots, x_k, x_{k+1}), f(y_1, \dots, y_k, y_{k+1})$$

have the same sign.

This verifies the claim. QED

LEMMA 6.2.7. Let  $f: N^k \rightarrow N$  be given by a term in  $ETM(0, 1, +, -, \uparrow)$ . There are finitely many functions  $g_1, \dots, g_n$  whose domains are various  $N^{k'}$ ,  $k' < k$ , and whose range is a subset of  $N$ , given by terms in  $TM(0, 1, +, -, \uparrow)$ , such that any common restricted infinite SOI for  $g_1, \dots, g_n$  is an infinite SOI for  $f$ .

Proof: Let  $f$  be as given. Enumerate the order types of  $k$ -tuples from  $N$ , by  $\alpha_1, \dots, \alpha_n$ . Pick the unique representatives  $\beta_1, \dots, \beta_n$  which are  $k$ -tuples whose range is an interval  $[1, p]$ ,  $1 \leq p \leq n$ . Set  $g_i(x_1, \dots, x_k) = f(x[\beta_i[1]], \dots, x[\beta_i[k]])$ . Each  $g_i$  handles the order type  $\alpha_i$  in the definition of SOI. QED

LEMMA 6.2.8. Let  $f: N^k \rightarrow N$  be given by a term in  $ETM(0, 1, +, -, \uparrow)$ . If  $\text{mesh}(A)$  is sufficiently large, then  $\uparrow A$  is an infinite SOI for  $f$ .

Proof: Let  $f$  be as given, and let  $g_1, \dots, g_n$  be as given by Lemma 6.2.7. By Lemma 6.2.6, for all  $1 \leq i \leq n$ , if  $\text{mesh}(A)$  is sufficiently large then  $\uparrow A$  is a restricted SOI for  $g_i$ . Hence if  $\text{mesh}(A)$  is sufficiently large then  $\uparrow A$  is a common restricted SOI for  $g_1, \dots, g_n$ . Now apply Lemma 6.2.7. QED

We now wish to establish Lemma 6.2.8 for  $ETM(0, 1, +, -, \cdot, \uparrow, \log)$ . We do this by showing that  $\cdot$  and  $\log$  can be eliminated in these terms, when restricting to  $\uparrow([r, \infty))$ , provided  $r$  is sufficiently large.

DEFINITION 6.2.8. Let  $n, k \geq 1$ . The  $n, k$ -terms are the terms  $v_1, \dots, v_n$ , and  $v_{i+j}$ , where  $1 \leq i \leq n$ ,  $1 \leq j \leq k$ .

DEFINITION 6.2.9. An  $n, k$ -ordering consists of an ordering of the  $n, k$ -terms. I.e., a listing

$$\alpha_1 \text{ rel } \alpha_2 \text{ rel } \dots \text{ rel } \alpha_{n(k+1)}$$

where each  $\text{rel}$  is either  $<$  or  $=$ , and  $\alpha_1, \dots, \alpha_{n(k+1)}$  is an enumeration without repetition of the  $n, k$ -terms.

An  $n, k$ -ordering may or may not hold, given an assignment of elements of  $N$  to the variables  $v_1, \dots, v_n$ .

Example 1.  $v_1 < v_1+1 < v_1+2 < v_2 = v_3 < v_2+1 = v_3+1 < v_2+2 = v_3+2$  is a  $3, 2$ -ordering which holds for some  $v_1, v_2, v_3 \in N$ .  
E.g.,  $v_1 = 0, v_2 = v_3 = 3$ .

Example 2.  $v_1 < v_2 < v_3 < v_1+1 < v_2+1 < v_3+1 < v_1+2 < v_2+2 < v_3+2$  is a  $3, 2$ -ordering which does not hold for any  $v_1, v_2, v_3 \in N$ . From  $v_3 < v_1+1$ , we obtain  $v_3 \leq v_1$ , contradicting  $v_1 < v_3$ .

We can obviously view every  $n, k$ -ordering as a conjunction of comparisons between all pairs of the  $n$ -terms. Only some of these conjunctions of comparisons hold for some choice of  $v_1, \dots, v_n \in N$ .

DEFINITION 6.2.10. Let  $X$  be an  $n, k$ -ordering. We write  $\alpha <_X \beta$ ,  $\alpha =_X \beta$ , for  $n, k$ -terms  $\alpha, \beta$ , according to the relevant position of  $\alpha, \beta$  in  $X$ . Here  $<_X$  and  $=_X$  are transitive. Define  $\alpha >_X \beta \Leftrightarrow \alpha <_X \beta$ ,  $\alpha \geq_X \beta \Leftrightarrow \beta \leq_X \alpha$ .

DEFINITION 6.2.11. The signed  $X$  sums are of the form

$$\beta_1 \uparrow \pm \beta_2 \uparrow \pm \dots \pm \beta_m \uparrow.$$

0.

where

- i.  $m \geq 1$ .
- ii.  $\beta_1, \dots, \beta_m$  are  $n, k$ -terms.
- iii.  $\beta_1 >_X \beta_2 >_X \dots >_X \beta_m$  holds in the  $n, k$ -ordering  $X$ .
- iv. There is no consecutive pair  $+\beta_i \uparrow, -\beta_{i+1} \uparrow$  for which  $\beta_i =_X \beta_{i+1}+1$ . For this purpose,  $\beta_1 \uparrow$  is considered to be  $+\beta_1 \uparrow$ .
- v. There is no consecutive pair  $-\beta_i \uparrow, +\beta_{i+1} \uparrow$  for which  $\beta_i =_X \beta_{i+1}+1$  in  $X$ .

We evaluate signed  $X$  sums at elements of  $N$  only, and we always associate to the left

$$(\dots (\beta_1 \uparrow \pm \beta_2 \uparrow) \pm \dots \pm \beta_m \uparrow).$$

where each  $\pm$  is  $+$  or  $-$ , both interpreted in the usual way using  $N$  arithmetic; i.e.,  $-$  indicates cutoff subtraction. Also note that the first summand,  $\beta_1 \uparrow$ , is not signed, which has the same effect as  $+\beta_1 \uparrow$ .



It is clear that the evaluation of a signed X sum is the same as the evaluation in Z arithmetic, since cutoff subtraction never gets triggered.

Conditions iv,v in Definition 6.2.10 rule out the possibility of an obvious simplification in signed X sums, corresponding to the ordinary algebraic laws  $2^{p+1}-2^p = 2^p$ , and  $-2^{p+1}+2^p = -2^p$ .

DEFINITION 6.2.12. Let X be an n,k-ordering. For X sums  $\lambda$ , we write  $\text{lth}(\lambda)$  for the number of summands in  $\lambda$ , and  $\#(\lambda)$  for the largest j such that some  $v_i+j$  is a summand. We take  $\text{lth}(0) = \#(0) = 0$ . Also, if  $\lambda$  has no  $v_i+j$  (i.e.,  $\lambda$  consists entirely of variables), then  $\#(\lambda) = 0$ . Obviously  $\#(\lambda) \leq k$ .

LEMMA 6.2.9. Let  $n \geq 3$  and X be an  $n, n^2$ -ordering. Let  $t = y_1 \uparrow \pm y_2 \uparrow \pm \dots \pm y_m \uparrow$  be parenthesized in any way, where  $\{y_1, \dots, y_m\} \subseteq \{v_1, \dots, v_n\}$ , and the y's are distinct,  $m \geq 1$ . There exists a signed X sum  $t^*$ , with  $\text{lth}(t^*) \leq m$  and  $\#(t^*) \leq m^2$ , which agrees with t at all  $v_1, \dots, v_n \in \mathbb{N}$  for which X is true. Here t (and of course  $t^*$ ) are evaluated using N arithmetic.

Proof: Fix n,X as given. We prove the claim by induction on  $1 \leq m \leq n$ .

The basis case  $m = 1$  is trivial. Now fix  $1 \leq m \leq n$ , and assume that the claim is true for all  $1 \leq m' < m$ . We now prove the claim for m.

Let  $t = y_1 \uparrow \pm y_2 \uparrow \pm \dots \pm y_m \uparrow$  be parenthesized in any way, where  $\{y_1, \dots, y_m\} \subseteq \{v_1, \dots, v_n\}$ , and the y's are distinct.

First suppose t is  $(r)+(s)$ ,  $\text{lth}(r)+\text{lth}(s) = m$ . By the induction hypothesis, let  $r^*, s^*$  be signed X sums,  $\text{lth}(r^*), \text{lth}(s^*) < m$ ,  $\#(r^*), \#(s^*) \leq (m-1)^2$ , where r agrees with  $r^*$  provided X holds, and s agrees with  $s^*$  provided X holds. Then t agrees with  $(r^*)+(s^*)$  provided X holds. Write  $t = (r^*)+(s^*)$  as

$$1) \quad t = (\beta_1 \uparrow \pm \dots \pm \beta_p \uparrow) + (\gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow)$$

with N arithmetic for t, and Z arithmetic for the  
two summands on the right,  
provided X holds.

Since we are using Z arithmetic on the right, we can rearrange the terms on the right. Place  $\gamma_1$  and the  $\pm \gamma$ 's in

their appropriate positions amongst the  $\beta$ 's, in  $X$ , resulting in

2)  $t = \delta_1 \uparrow \pm \dots \pm \delta_{p+q} \uparrow$   
 with  $N$  arithmetic on the left and  $Z$  arithmetic on the  
 right,  
 provided  $X$  holds.

so that we have  $\delta_1 \geq_x \dots \geq_x \delta_{p+q}$ . Note that conditions iii-v in Definition 6.2.11, may fail for the right side of 3).

We continue to work in  $Z$  arithmetic. We iterate a process, which, at each stage, shortens the right side of 2). Recall that  $p+q \leq m$ . So the process will continue for at most  $m$  steps. The process runs as follows. Choose any  $i$  such that the consecutive pair  $\pm \delta_i \uparrow, \pm \delta_{i+1} \uparrow$  violates any of conditions iii-v. Remove or replace  $\pm \delta_i \uparrow \pm \delta_{i+1} \uparrow$  as follows.

case 1.  $\delta_i = \delta_{i+1}$  in  $X$ .

Replace  $+ \delta_i \uparrow + \delta_{i+1} \uparrow$  by  $(\delta_i+1) \uparrow$ .  
 Replace  $- \delta_i \uparrow - \delta_{i+1} \uparrow$  by  $- (\delta_i+1) \uparrow$ .  
 Remove  $+ \delta_i \uparrow - \delta_{i+1} \uparrow$ .  
 Remove  $- \delta_i \uparrow + \delta_{i+1} \uparrow$ .

case 2.  $\delta_i = \delta_{i+1}+1$  in  $X$ .

Replace  $+ \delta_i \uparrow - \delta_{i+1} \uparrow$  by  $+ \delta_{i+1} \uparrow$ .  
 Replace  $- \delta_i \uparrow + \delta_{i+1} \uparrow$  by  $- \delta_{i+1} \uparrow$ .

If at some stage, there are no terms left, then the result is 0.

These replacements are of course valid in  $Z$  arithmetic. So it is clear that this process results in a signed  $X$  term  $t^*$  such that

3)  $t = t^*$   
 with  $N$  arithmetic on the left and  $Z$  arithmetic on the  
 right,  
 provided  $X$  holds.

Note that every step in the process raises the constants used by at most 1. In addition,  $\text{lth}(t^*) \leq \text{lth}(r^*) + \text{lth}(s^*) \leq m$ . Hence  $\#(t^*) \leq (m-1)^2 + m \leq m^2$ . Also,  $t^*$  is of form 3), where the  $\delta$ 's must obey the conditions iii-v in the

definition of signed X sum. So  $t^*$  is the desired signed X sum.

Finally, suppose  $t$  is  $(r)-(s)$ ,  $\text{lth}(r)+\text{lth}(s) = m$ . By the induction hypothesis, let  $r^*, s^*$  be signed X sums,  $\text{lth}(r^*), \text{lth}(s^*) < m$ ,  $\#(r^*), \#(s^*) \leq (m-1)^2$ , where  $r$  agrees with  $r^*$  provided X holds, and  $s$  agrees with  $s^*$  provided X holds. Then

$$4) t = (\beta_1 \uparrow \pm \dots \pm \beta_p \uparrow) - (\gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow)$$

with N arithmetic on the left and Z arithmetic for the  
two summands on the right,  
provided X holds.

We can obviously assume that  $p, q \geq 1$ . The  $-$  on the right is in N arithmetic. We will convert to Z arithmetic by comparing

$$\begin{array}{c} \beta_1 \uparrow \pm \dots \pm \beta_p \uparrow \\ \gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow \end{array}$$

simply on the basis of X, and not dependent on the values of variables. Recall that the  $\beta$ 's are strictly decreasing in X, and the  $\gamma$ 's are strictly decreasing in X.

Let  $i \in [0, \min(p, q)]$  be greatest such that the first  $i$  terms of  $\beta_1 \uparrow \pm \dots \pm \beta_p \uparrow$  and the first  $i$  terms of  $\gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow$  are equal according to X (with the same signs).

If  $\pm \beta_{i+1} <_X \pm \gamma_{i+1}$  then for all  $x_1, \dots, x_n$  obeying X,

$$\begin{array}{c} \beta_1 \uparrow \pm \dots \pm \beta_p \uparrow < \gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow \\ \text{with Z arithmetic.} \end{array}$$

If  $\pm \beta_{i+1} >_X \pm \gamma_{i+1}$  then for all  $x_1, \dots, x_n$  obeying X,

$$\begin{array}{c} \beta_1 \uparrow \pm \dots \pm \beta_p \uparrow > \gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow \\ \text{with Z arithmetic.} \end{array}$$

It might be the case that  $i+1 > \min(p, q)$ . In this event, use 0 for the nonexistent term.

In the former case, use the signed X sum 0. In the latter case, rewrite 4) as

$$5) t = \beta_1 \uparrow \pm \dots \pm \beta_p \uparrow - \gamma_1 \uparrow \pm \dots \pm \gamma_q \uparrow$$

with N arithmetic on left and Z arithmetic on right,

provided  $X$  holds.

where the second group of  $\pm$  are reversed from what they were in 4). Now treat 5) as we treated 1), obtaining the form 2) with decreasing terms. QED

LEMMA 6.2.10. Let  $t = y_1 \uparrow \pm y_2 \uparrow \pm \dots \pm y_m \uparrow$  be parenthesized in any way, where the  $y$ 's are distinct variables from  $\{v_1, \dots, v_n\}$ .

- i.  $t$  is equivalent to a term in  $\text{ETM}(0,1,+,-,\uparrow)$ .
- ii.  $\log(t)$  is equivalent to a term in  $\text{ETM}(0,1,+,-)$ .
- iii.  $\pm y_1 \uparrow \pm y_2 \uparrow \pm \dots \pm y_m \uparrow$ , interpreted in  $\mathbb{Z}$  arithmetic, is equivalent, in absolute value, to a term in  $\text{ETM}(0,1,+,-,\uparrow)$ .

Proof: Let  $t$  be as given. By Lemma 6.2.9, we obtain a system of signed  $X$  sums equivalent to  $t$ , under  $X$ , for the various  $n, n^2$ -orderings. This provides the appropriate definition by cases of  $t$ . This establishes i).

For ii), note that under each of these  $n, n^2$ -orderings  $X$ ,  $t$  is equivalent to a signed  $X$  sum, which takes one of the form

$$\begin{aligned} & 0. \\ & \beta \uparrow. \\ & (\dots (\beta_1 \uparrow + \beta_2 \uparrow \dots)). \\ & (\dots (\beta_1 \uparrow - \beta_2 \uparrow \dots)). \end{aligned}$$

where in the last two cases, the number of  $\beta$ 's is 2 or greater. Note that we have, respectively,

$$\begin{aligned} \log(t) &= 0. \\ \log(t) &= \beta. \\ \log(t) &= \beta_1. \\ \log(t) &= \beta_1 - 1. \end{aligned}$$

which gives rise to a definition of  $\log(t)$  by cases. The cases are given by the various  $n, n^2$ -orderings. This provides the appropriate definition by cases of  $\log(t)$ . This establishes ii).

For iii), let any  $n, n$ -ordering  $X$  be given. If the greatest  $y$ 's under  $X$  appear with  $+$ , then we use  $\pm y_1 \uparrow \pm y_2 \uparrow \pm \dots \pm y_n \uparrow$ . Otherwise, we reverse the  $\pm$ . Then we rewrite in descending  $y$ 's under  $X$ , and left associate, obtaining an equivalent expression in  $\mathbb{N}$  arithmetic. No given the

appropriate definition by cases, where the cases are given by the X's. QED

LEMMA 6.2.11. Let  $s = y_1 \uparrow \pm y_2 \uparrow \pm \dots \pm y_p \uparrow$  and  $t = z_1 \uparrow \pm z_2 \uparrow \pm \dots \pm z_q \uparrow$  be parenthesized in any way, where  $\{y_1, \dots, y_p, z_1, \dots, z_q\} \subseteq \{x_1, \dots, x_n\}$ , and  $y_1, \dots, y_p, z_1, \dots, z_q$  are distinct variables. Then  $s \cdot t$  is equivalent to a term  $r \in \text{ETM}(0, 1, +, -, \uparrow)$  whose variables are among  $y_1, \dots, y_p, z_1, \dots, z_q$ .

Proof: Let  $s, t, y_1, \dots, y_p, z_1, \dots, z_q, n$  be as given.

According Lemma 6.2.9, under each such  $n, n^2$ -ordering  $X$ , we can write  $s, t$  as signed  $X$  sums

$$\begin{aligned} s &= (\alpha_1 \uparrow \pm \dots \pm \alpha_b \uparrow). \\ t &= (\beta_1 \uparrow \pm \dots \pm \beta_c \uparrow). \end{aligned}$$

where the left sides use  $N$  arithmetic and the right sides use  $Z$  arithmetic.

We now have

$$(s) \cdot (t) = \gamma_1 \uparrow \pm \dots \pm \gamma_{bc} \uparrow.$$

where the left side uses  $N$  arithmetic and the right side uses  $Z$  arithmetic. Here each  $\gamma \uparrow$  takes the form

$$\alpha_i \uparrow \cdot \beta_j \uparrow = (\alpha_i + \beta_j) \uparrow.$$

and hence each  $\gamma$  takes the form  $\alpha_i + \beta_j$ . We can now treat the various  $\gamma_i$  as new variables, and get an appropriate definition by cases for  $\gamma_1 \uparrow \pm \dots \pm \gamma_{bc} \uparrow$  using Lemma 6.2.10 iii). We can then substitute the sums  $\alpha_i + \beta_j$  for the new variables, and get the desired definition by cases for  $(s) \cdot (t)$ . QED

DEFINITION 6.2.13. Let  $p \geq 0$ . We define  $\text{TM}(0, 1, +, -, \cdot, \uparrow, \log: p)$  as the terms in  $\text{TM}(0, 1, +, -, \cdot, \uparrow, \log)$  where every occurrence of every variable is followed by (at least)  $p$   $\uparrow$ 's.

DEFINITION 6.2.14. We define  $\text{ETM}(0, 1, +, -, \cdot, \uparrow, \log: p)$  as the terms in  $\text{ETM}(0, 1, +, \cdot, \uparrow, \log)$  where every occurrence of every variable is followed by (at least)  $p$   $\uparrow$ 's. This applies to occurrences in both the terms and the quantifier free formulas.

As usual, we can omit some of the symbols  $0, 1, +, -, \cdot, \uparrow, \log$ , for the above definition.

LEMMA 6.2.12. Let  $p \geq 1$  and  $t \in \text{TM}(0, 1, +, -, \uparrow; p)$ . Then  $t$  is equivalent to a term of the form  $s_1 \uparrow \pm \dots \pm s_k \uparrow$ , parenthesized in some way, where each  $s_i \in \text{TM}(0, 1, +, -, \uparrow; p-1)$ .

Proof: Let  $p \geq 1$ . We define  $*$  by recursion on terms  $t \in \text{TM}(0, 1, +, -, \uparrow; p)$ . The basis cases are  $t = 0, 1, \uparrow^p(x_n)$ . Define  $0^* = \uparrow^p(x_1) - \uparrow^p(x_1)$ .  $1^* = 0 \uparrow$ .  $\uparrow^p(x_n)^* = \uparrow^p(x_n)$ .  $t \uparrow^* = t^* \uparrow$ .  $(s+t)^* = s^* + t^*$ .  $(s-t)^* = s^* - t^*$ . QED

LEMMA 6.2.13. Let  $t \in \text{ETM}(0, 1, +, -, \cdot, \uparrow, \log; p)$ ,  $p \geq 1$ , with at most one occurrence of  $\log$  and  $\cdot$  combined. Then  $t$  is equivalent to a term  $t^* \in \text{ETM}(0, 1, +, -, \uparrow; p-1)$ .

Proof: By Lemma 6.2.12, this holds if there are no occurrences of  $\log$  and  $\cdot$ . We can assume that either there is a unique occurrence of  $\cdot$  and no occurrence of  $\log$ , or there is a unique occurrence of  $\log$  and no occurrence of  $\cdot$ . Thus we have a split into the following two cases.

case 1.  $\log(u)$  is a subterm of  $t$ . Then  $u \in \text{TM}(0, 1, +, -, \uparrow; p)$ . By Lemma 6.2.12, write

$$u = t_1 \uparrow \pm \dots \pm t_k \uparrow$$

parenthesized in some way, where  $t_1, \dots, t_k \in \text{TM}(0, 1, +, -, \uparrow; p-1)$ . Introduce distinct variables  $y_1, \dots, y_k$  for  $t_1, \dots, t_k$ . By Lemma 6.2.10,  $\log(y_1 \uparrow \pm \dots \pm y_k \uparrow)$  is equivalent to some term  $\alpha(y_1, \dots, y_k) \in \text{ETM}(0, 1, +, -)$ . By substitution,  $\log(u) = \log(t_1 \uparrow \pm \dots \pm t_k \uparrow)$  is equivalent to a term  $\alpha(t_1, \dots, t_k) \in \text{ETM}(0, 1, +, -, \uparrow; p-1)$ . Replace  $\log(u)$  in  $t$  by  $\alpha(t_1, \dots, t_k)$ , and expand to a term  $t^*$  in  $\text{ETM}(0, 1, +, -, \uparrow)$ . In this expansion, we use the same cases that we use for  $\alpha(t_1, \dots, t_k)$ , moving these cases out in front. Therefore  $t^* \in \text{ETM}(0, 1, +, -, \uparrow; p-1)$ .

case 2.  $r \cdot s$  is a subterm of  $t$ . Then  $r, s \in \text{TM}(0, 1, +, -, \uparrow; p)$ . By Lemma 6.2.12, write

$$\begin{aligned} r &= r_1 \uparrow \pm \dots \pm r_p \uparrow \\ s &= s_1 \uparrow \pm \dots \pm s_q \uparrow \end{aligned}$$

parenthesized in some way, where  $r_1, \dots, r_p, s_1, \dots, s_q \in \text{TM}(0, 1, +, -, \uparrow; p-1)$ . Introduce distinct variables  $y_1, \dots, y_p, z_1, \dots, z_q$  for  $r_1, \dots, r_p, s_1, \dots, s_q$ . By Lemma 6.2.11,  $(y_1 \uparrow \pm \dots \pm y_p) \cdot (z_1 \uparrow \pm \dots \pm z_q \uparrow)$  is equivalent to some term  $\beta(y_1, \dots, y_p, z_1, \dots, z_q) \in \text{ETM}(0, 1, +, -, \uparrow) = \text{ETM}(0, 1, +, -, \uparrow; 0)$ . By substitution,  $r \cdot s = (r_1 \uparrow \pm \dots \pm r_p \uparrow) \cdot (s_1 \uparrow \pm \dots \pm s_q \uparrow)$  is equivalent to the term  $\beta(s_1, \dots, s_p, t_1, \dots, t_q) \in \text{ETM}(0, 1, +, -, \uparrow; p-1)$ . Replace  $r \cdot s$  in  $t$  by  $\beta(s_1, \dots, s_p, t_1, \dots, t_q)$ , and expand to a term  $t^*$  in  $\text{ETM}(0, 1, +, -, \uparrow)$ . In this expansion, we use the same cases that we use for  $\alpha(t_1, \dots, t_k)$ , moving these cases out in front. Therefore  $t^* \in \text{ETM}(0, 1, +, -, \uparrow; p-1)$ .

QED

LEMMA 6.2.14. Let  $t \in \text{ETM}(0, 1, +, -, \cdot, \uparrow, \log; p)$ ,  $p \geq n \geq 1$ , with at most  $n$  occurrences of  $\log$  and  $\cdot$  combined. Then  $t$  is equivalent to a term  $t^* \in \text{ETM}(0, 1, +, -, \uparrow; p-n)$ .

Proof: We argue by induction on  $n \geq 1$ , that the statement is true for all  $p \geq n \geq 1$ . The case  $n = 1$  is Lemma 6.2.13. Suppose this is true for a fixed  $n \geq 1$ . Let  $t \in \text{ETM}(0, 1, +, -, \cdot, \uparrow, \log; p)$ ,  $p \geq n+1 \geq 1$ , with exactly  $n+1$  occurrences of  $\log$  and  $\cdot$  combined.

It is clear that there is an occurrence of  $\log(u)$  where  $u$  has no  $\log$  or  $\cdot$ , or there is an occurrence of  $u \cdot v$ , where  $u, v$  have no occurrence of  $\log$  or  $\cdot$ . I.e., there is a subterm  $s \in \text{TM}(0, 1, +, -, \cdot, \uparrow, \log)$  of  $t$  with exactly one occurrence of  $\log$  and  $\cdot$  combined. It is obvious that  $s \in \text{TM}(0, 1, +, -, \cdot, \uparrow, \log; p)$ .

By Lemma 6.2.13,  $s$  is equivalent to a term  $r \in \text{ETM}(0, 1, +, -, \uparrow; p-1)$ . Replace  $s$  in  $t$  by  $r$ , and expand the result to a term  $t'$  by bring the cases inside  $r$  outside. Note that the cases inside  $r$  contain no occurrences of  $\log$  and  $\cdot$ . Then  $t' \in \text{ETM}(0, 1, +, -, \cdot, \uparrow, \log; p-1)$  has at most  $n$  occurrences of  $\log$  and  $\cdot$  combined. Now apply the induction hypothesis to  $t'$  to obtain the required  $t^* \in \text{ETM}(0, 1, +, -, \uparrow; (p-1)-n) = \text{ETM}(0, 1, +, -, \uparrow; p-(n+1))$ . QED

LEMMA 6.2.15. Let  $t \in \text{ETM}(0, 1, +, -, \cdot, \uparrow, \log; p)$ ,  $p \geq 1$ , with at most  $p$  occurrences of  $\log$  and  $\cdot$  combined. Then  $t$  is equivalent to a term  $t^* \in \text{ETM}(0, 1, +, -, \uparrow)$ .

Proof: Immediate from Lemma 6.2.14. QED

LEMMA 6.2.16. Let  $f:N^k \rightarrow N$  be given by a term in  $ETM(0,1,+,-,\cdot,\uparrow,\log)$ . If  $\text{mesh}(A)$  is sufficiently large, then  $\uparrow A$  is an infinite SOI for  $f$ .

Proof: Let  $f$  be given by  $t \in ETM(0,1,+,-,\cdot,\uparrow,\log)$  with at most  $p$  occurrences of  $\log$  and  $\cdot$  combined,  $p \geq 1$ .

Let  $t'$  be the result of replacing every occurrence of every variable  $v$  in  $t$  by  $\uparrow p(v)$ . Then  $t' \in ETM(0,1,+,-,\cdot,\uparrow,\log:p)$ . By Lemma 6.2.15, let  $t'$  be equivalent to  $t'^* \in ETM(0,1,+,-,\uparrow)$ .

According to Lemma 6.2.8,

if  $\text{mesh}(A)$  is sufficiently large,  
then  $\uparrow A$  is an infinite SOI for  $t'^*$ ,  
and hence for  $t'$ .

Obviously,

if  $\text{mesh}(A) \geq p$  and  $\uparrow A$  is an infinite SOI for  $t'$ ,  
then  $\uparrow(A+p)$  is an infinite SOI for  $t$ .

Therefore,

if  $\text{mesh}(A)$  is sufficiently large,  
then  $\uparrow A$  is an infinite SOI for  $t$ .

QED

We can usefully sharpen the indiscernibility given by Lemma 6.2.16.

Recall Definition 5.2.2 of  $\#(\varphi)$  in Definition

LEMMA 6.2.17. Fix  $r \geq 1$ . If  $\text{mesh}(A)$  is sufficiently large, then  $\uparrow A$  is an infinite set of indiscernibles for all quantifier free formulas  $\varphi$  of  $(N,0,1,+,-,\cdot,\uparrow,\log)$  with  $\#(\varphi) \leq r$ .

Proof: Let  $r \geq 1$ . For each such  $\varphi(v_1, \dots, v_r)$ , define

$$f_\varphi(x_1, \dots, x_r) = 1 \text{ if } \varphi(x_1, \dots, x_r); 0 \text{ otherwise.}$$

Then  $f_\varphi \in \text{BAF}$ . Now apply Lemma 6.2.16 to each  $f_\varphi$ . The Lemma follows easily. QED



We now provide a required link between Lemma 6.2.16 and Chapter 4 in order to show that Propositions C,E-H hold in the recursive subsets of  $N$  - and in fact, in the subsets of  $N$  that have primitive recursive enumerations.

Let us now look at the proof given in Chapter 4 of Proposition B in  $ACA' + 1-Con(MAH)$ , with an eye towards showing that Propositions C,E-H hold in the sets with primitive recursive enumeration functions. This is Theorem 4.4.11.

Our strategy is to first rework much of sections 4.3 and 4.4 primitive recursively.

Before getting into full details, we now illustrate the power of Lemma 6.2.17 for this purpose. Note that in the proof of Theorem 4.4.11, we took the following step, which must now be avoided:

...By Ramsey's theorem for  $2r$ -tuples in  $ACA'$ ,  
we can find a  $p,q,b;r$ -structure  
 $M = (N, 0, 1, <, +, f, g, c_0, c_1, \dots)$ . ...

The notion of  $p,q,b;r$ -structure was defined just before Lemma 4.4.2. Note that in this context of  $N$ , the atomic indiscernibility clause  $7'$  is the only substantial clause.

We avoid this use of Ramsey's theorem for  $f, g \in BAF$ , as follows.

LEMMA 6.2.18. Let  $p, q, b, r \geq 1$ ,  $f \in ELG(p, b)$ ,  $g \in ELG(q, b)$ ,  $f, g \in SD \cap BAF$ . Then  $(N, 0, 1, <, +, f, g, (\uparrow A)_1, (\uparrow A)_2, \dots)$  is a  $p, q, b; r$ -structure, provided  $mesh(A)$  is sufficiently large. Here  $(\uparrow A)_1, (\uparrow A)_2, \dots$  is the strictly increasing enumeration of the set  $\uparrow A$ .

Proof: Lemma 6.2.17 takes care of clause  $7'$ . So this is immediate. QED

Lemma 6.2.18 takes care of one crucial step in the proof of Theorem 4.4.11. We still have to show that the  $D_1 \subseteq \dots \subseteq D_n \subseteq N$  there can be taken to be recursive, or even have primitive recursive enumeration functions.

Let us now proceed systemically. Our first aim is to obtain a new form of Theorem 4.3.8, and use it in an adaptation of section 4.4.

Recall the definition of a special SOI for  $f:N^p \rightarrow N$  in Definition 4.3.6. We repeat this definition, by rearranging its components.

DEFINITION 6.2.15. Let  $f:N^p \rightarrow N$  and  $A \subseteq N$ . We say that  $A$  is a special SOI for  $f$  if and only if the following holds.

a. The truth value of any statement

$$f(x_1, \dots, x_p) < f(y_1, \dots, y_p)$$

where  $x_1, \dots, x_p, y_1, \dots, y_p \in A$ , depends only on the order type of the  $2p$ -tuple  $(x_1, \dots, x_p, y_1, \dots, y_p)$ .

b. Let  $x_1, \dots, x_p, y_1, \dots, y_p \in A$ . Suppose  $(x_1, \dots, x_p)$  and  $(y_1, \dots, y_p)$  have the same order type. Suppose also that for all  $1 \leq i \leq p$ ,  $x_i = y_i \vee y_i > \max(x_1, \dots, x_p)$ . Then i)  $f(x_1, \dots, x_p) \leq f(y_1, \dots, y_p)$ ; ii) if  $f(x_1, \dots, x_p) < f(y_1, \dots, y_p)$  then  $f(y_1, \dots, y_p)$  is greater than all  $f(z_1, \dots, z_p)$ ,  $|z_1, \dots, z_p| \leq |x_1, \dots, x_p|$ .

The conditions on  $x, y \in A^p$  in b) play an important role. We say that  $x, y$  are specially related if and only if the conditions on  $x, y \in A^p$  in b) hold.

Recall the key indiscernible stretching Lemma 4.3.5. Since ACA' was being used freely, we did not consider any effectivity issues with regard to Lemma 4.3.5. We will refine Lemma 4.3.5 below. First we need a Lemma.

LEMMA 6.2.19. For all  $p \geq 1$  there is a primitive recursive function  $f:N^2 \rightarrow N$  such that the following holds. Let  $x_0, \dots, x_n \in N^p$ ,  $c \in N$ , where  $n = f(c, |x_1|)$  and each  $|x_{i+1}| \leq |x_i| + c$ . Then there exists  $1 \leq i < j \leq n$  such that  $x_i, x_{i+1}$  are specially related.

Proof: Fix  $p \geq 1$ . The statement

$$\begin{aligned} 1) \quad & (\forall c, x_0) (\exists n) (\forall x_1, \dots, x_n \in N^p) \\ & ((\forall i \leq n-1) (|x_{i+1}| \leq |x_i| + c) \rightarrow \\ & (\exists i < j) (x_i, x_{i+1} \text{ obey } b)) \end{aligned}$$

is provable in the formal system  $WKL_0$  (see [Si99]), as follows. Assume false, and fix  $c, x_0$ . Then apply  $WKL_0$  to produce an infinite counterexample  $x_0, x_1, \dots \in N^p$ . Then choose an infinite subsequence so that the  $p$ -tuples have

the same order type and the first terms are all = or all <. Iterate this construction for  $p$  steps, arriving at an infinite counterexample  $y_0, y_1, \dots$  where for all  $1 \leq i \leq p$ , the  $i$ -th coordinates are all = or all <. For  $j$  large enough,  $y_0, y_j$  are specially related. This is a contradiction.

It is obvious that 1) is in  $\Pi^0_2$  form, and so we can apply our Theorem that every  $\Pi^0_2$  sentence provable in  $WKL_0$  has a primitive recursive bounding function. See [Si99,09], p. 37, p. 381. QED

LEMMA 4.3.5'. The following is provable in  $ACA'$ . Let  $q \geq 3p \geq 1$ , and  $f: [0, q]^p \rightarrow \mathbb{N}$ . Assume  $[0, q]$  is a special SOI for  $f$ . There exists primitive recursive  $g: \mathbb{N}^p \rightarrow \mathbb{N}$  such that  $\mathbb{N}$  is a special SOI for  $g$ , where  $g|_{[0, q]^p}$  is isomorphic to  $f$  in the following sense. For all  $x, y \in [0, q]^p$ ,  $f(x) \leq f(y) \leftrightarrow g(x) \leq g(y)$ .

Proof: Let  $p, q, f$  be as given. The proof of Lemma 4.3.5 begins by putting the following recursive relation  $\leq^*$  on  $\mathbb{N}^p$ .  $x \leq^* y$  if and only if there exists  $\alpha, \beta \in [0, q]^p$  such that

- i.  $(x, y)$  and  $(\alpha, \beta)$  have the same order type.
- ii.  $f(\alpha) \leq f(\beta)$ .

In the proof of Lemma 4.3.5, it is shown that  $\leq^*$  is reflexive, connected, transitive, and its order type, modulo  $=^*$ , is finite or  $\omega$ .

Then we defined  $g: \mathbb{N}^p \rightarrow \mathbb{N}$  by

$g(x)$  is the position in  $\leq^*$  of  $x$  counting from 0.

We proved that  $g$  is as required here, except for "primitive recursive". We did not address any issues of effectivity for  $g$  in the proof of Lemma 4.3.5.

Thus it suffices to prove that  $g$  is primitive recursive.

We say that a finite or infinite sequence  $x_0, x_1, \dots \in \mathbb{N}^p$  is complete if and only if each  $x_i <^* x_{i+1}$ , and every  $y \in \mathbb{N}^p$  is equivalent ( $=^*$ ) to some  $x_i$ . By the proof of Lemma 4.3.5, there is a complete sequence.

Suppose  $x_0, \dots, x_n$  is a finite complete sequence. We claim that  $g$  is elementary recursive. Let  $x \in \mathbb{N}^p$ . Return  $i$  such that  $x =^* x_i$ .

So we will assume that complete sequences are infinite. We fix a complete sequence  $x_0, x_1, \dots$ . Obviously, all complete sequences are equivalent ( $=^*$ ), term by term.

We claim that for all  $x \in \mathbb{N}^p$  there exists  $y \in \mathbb{N}^p$  such that

- 1)  $|y| \leq |x| + 2^p + p$ .
- $y$  is an immediate successor of  $x$  in  $<^*$ .

To see this, let  $x = (x_1, \dots, x_p)$ , and let  $y = (y_1, \dots, y_p)$  be an immediate successor of  $x$  in  $<^*$  with least possible  $|y|$ . Assume  $|y| > |x| + 2^p + p$ .

Let  $y_i$  be a greatest coordinate of  $y$ . We claim that the greatest coordinate of  $y$  bigger than  $y_i$  is  $y_{i-1}$ . To see this, suppose otherwise, and let  $y'$  be the result of decrementing the  $y_i$ 's in  $y$  by 1. Then  $x, y'$  and  $x, y$  have the same order type, and so  $x <^* y'$ . Also  $y', y$  obeys the hypotheses of clause b), and so  $y' \leq^* y$ . Hence  $y'$  is another immediate successor of  $x$  in  $<^*$  of lower  $|y'|$ . This contradicts the choice of  $y$ .

Now the same argument will *not* show that the greatest coordinate of  $y$  bigger than  $y_{i-1}$  is  $y_{i-2}$ . However, this argument does show that the greatest coordinate of  $y$  bigger than  $y_{i-1}$  is at least  $y_{i-3}$ . This is because we can drop the  $y_i, y_{i-1}$  in  $y$  by 2 each. We repeat this argument  $p$  times, thereby obtaining  $\min(y) > |x| + p$ . Then we can push all of the coordinates of  $y$  down by  $p$ , obtaining another immediate successor of  $x$  in  $<^*$  of lower  $|y|$ . This is a contradiction.

Next we claim that for all  $x \in \mathbb{N}^p$ , not minimal in  $<^*$ , there exists  $y \in \mathbb{N}^p$  such that

- 2)  $|y| \leq |x| + 2^p + p$ .
- $y$  is an immediate predecessor of  $x$  in  $<^*$ .

To see this, let  $x = (x_1, \dots, x_p)$ , and let  $y = (y_1, \dots, y_p)$  be an immediate predecessor of  $x$  in  $<^*$  with least possible  $|y|$ . Assume  $|y| > |x| + 2^p + p$ .

Let  $y_i$  be a greatest coordinate of  $y$ . If we raise the  $y_i$  in  $y$  by 1 then we obtain  $z$  with  $y \leq^* z <^* x$ . Hence  $y =^* z$ .

We now claim that the greatest coordinate of  $y$  bigger than  $y_i$  is  $y_{i-1}$ . To see this, suppose otherwise, and let  $y'$  be the result of decrementing the  $y_i$ 's in  $y$  by 1. Then  $y' <^* x$ . Since  $y =^* z$ , we have  $y =^* y'$ . Hence  $y'$  is another immediate predecessor of  $x$  in  $<^*$  of lower  $|y'|$ . This contradicts the choice of  $y$ .

Now the same argument will *not* show that the greatest coordinate of  $y$  bigger than  $y_{i-1}$  is  $y_{i-2}$ . However, we now show that the greatest coordinate of  $y$  bigger than  $y_{i-1}$  is at least  $y_{i-3}$ . This is because if otherwise, we can first raise the  $y_i, y_{i-1}$  in  $y$  by 2 each, with  $=^*$ . Then we drop the  $y_i, y_{i-1}$  in  $y$  by 2, also with  $=^*$ , contradicting the choice of  $y$ .

We repeat this argument  $p$  times, thereby obtaining  $\min(y) > |x|+p$ . Then we can push all of the coordinates of  $y$  first up by  $p$ , and then down by  $p$ , obtaining another immediate predecessor of  $x$  in  $<^*$  of lower  $|y|$ . This is a contradiction.

We now claim the following. Let  $x <^* y <^* z$ . There exists  $w$  such that

$$\begin{aligned} 3) \quad & |w| \leq |x|+|z|+p. \\ & x <^* w <^* z. \end{aligned}$$

To see this, choose  $y$  such that  $x <^* y <^* z$ , where  $|y|$  is minimal. Assume  $|y| > |x|+|z|+p$ . We can move a nonempty tail of the coordinates of  $y$  that are  $> |x|+|z|$ , down by 1, obtaining  $y'$ , with  $x <^* y' <^* z$ . This contradicts the choice of  $y$ .

Note that 3) gives us a bounded search algorithm for testing whether  $z$  is an immediate successor of  $x$  in  $<^*$ .

From 1), 2), we have

$$4) \quad (\forall i \geq 1) (|x_{i-1}|, |x_{i+1}| \leq |x_i|+2^p+p).$$

We say that a complete sequence is minimal if and only if each  $x_i$  has minimum  $|x_i|$  among the  $x =^* x_i$ .

We can now build a minimal complete sequence algorithmically. Let  $x_1$  be any  $<^*$  minimal element of  $N^p$ . Suppose  $x_i$  has been defined. Search among the  $y$  with  $|y| \leq$

$|x_i|+2^p+p$  for an immediate successor  $y$  of  $x_i$  in  $\leq^*$ . By 1), there is such a  $y$ . By the previous paragraph, we can test whether  $y$  is an immediate successor of  $x_i$  in  $\leq^*$ .

This construction provides a complete sequence  $x_0, x_1, \dots$  and an algorithm for producing  $x_i$  from  $i$ . It is easy to see that the running time of this algorithm is bounded by an iterated exponential. I.e.,  $x_0, x_1, \dots$  is elementary recursive.

However, we still have to show that the function

$$g(x) = \text{the unique } n \text{ such that } x = x_n$$

is primitive recursive. For this, we use Lemma 6.2.19. Let  $x \in \mathbb{N}^p$ . Let  $x = x_n$ . We need to give an upper bound on  $n$ , primitive recursively in  $x$ .

Consider the sequence

$$x = x_n, x_{n-1}, \dots, x_0 \in \mathbb{N}^p.$$

Let  $f: \mathbb{N}^2 \rightarrow \mathbb{N}$  be the primitive recursive function given by Lemma 6.2.19. If  $n \geq f(2^p+p, |x|)$  then by Lemma 6.2.19,

there exists  $1 \leq i \leq n$  such that  $x_{i+1}, x_i$   
are specially related.

But then,  $x_{i+1} \leq^* x_i$ , which is a contradiction. Hence we have the primitive recursive upper bound

$$n \leq f(2^p+p, |x|).$$

We can now compute  $g(x)$  primitive recursively, by computing  $x_0, x_1, \dots$  elementary recursively, out to  $f(2^p+p, |x|)+1$  terms and testing for  $x =^* x_i$ . QED

The following adds to Lemma 4.3.7.

LEMMA 4.3.7'. The following is provable in ACA'. Every true  $\forall(p, q, \psi)$  is primitive recursively true.

Proof: Let  $\forall(p, q, \psi)$  be true. As in the proof of Lemma 4.3.7, there exists  $f: [0, q]^p \rightarrow \mathbb{N}$  in the sense of Lemma 4.3.5'. Now apply Lemma 4.3.4' and 4.3.6. QED

The following adds to Lemma 4.3.8.

THEOREM 4.3.8'. The following is provable in ACA'. Every true  $\lambda(k, n, m, R_1, \dots, R_{n-1})$  is primitive recursively true.

Proof: Use Lemma 4.3.7' and the proof of Theorem 4.3.8. QED

Recall these definitions made in section 4.4:

- $p, q, b$ -structure. (Definition 4.4.2)
- $p, q, b; r$ -structure. (Definition 4.4.4)
- $p, q, b; r, n$ -special structure. (Definition 4.4.5)
- $p, q, b; r$ -type. (Definition 4.4.7)
- $p, q, b; r, n$ -special type. (Definition 4.4.7)

We need modified forms of the last four of these notions. For this purpose, let  $M^*$  be a  $p, q, b; r$ -structure. Recall that  $M^* \langle r \rangle$  is the set of all values of closed terms of length  $\leq r$  in  $M^*$ . By the almost strict dominance of  $+^*, f^*, g^*$  in  $M^*$ , we see that  $M^* \langle r \rangle$  has order type  $\omega$ .

DEFINITION 6.2.16. We say that  $M^*$  is a  $p, q, b; r$ -structure/prim if and only if

- i.  $M^*$  is a  $p, q, b; r$ -structure.
- ii. Every element of  $M^*$  is the value of a closed term.
- iii. The  $\langle^*$  relation on closed terms is primitive recursive.

DEFINITION 6.2.17. A  $p, q, b; r$ -type/prim is the type of some  $p, q, b; r$ -structure/prim.

DEFINITION 6.2.18. We say that  $h: \mathbb{N} \rightarrow M^*$  is primitive recursive if and only if there is a primitive recursive function  $h'$  from  $\mathbb{N}$  into closed terms such that the value in  $M^*$  of each  $h'(n)$  is  $h(n)$ .

DEFINITION 6.2.19. A  $p, q, b; r, n$ -special structure/prim is a  $p, q, b; r, n$ -structure/prim in which witnessing  $D$ 's can be found whose enumeration functions are primitive recursive.

DEFINITION 6.2.20. A  $p, q, b; r, n$ -special type/prim is the  $p, q, b; r$ -type of some  $p, q, b; r, n$ -special structure/prim.

The following adds to Lemma 4.4.4.

LEMMA 4.4.4'. The following is provable in  $\text{RCA}_0$ . Let  $M^*$  be a  $p, q, b; r$ -structure. Then  $M^* \langle r \rangle$  is of order type  $\omega$ . There is

an increasing primitive recursive bijection  $f:N \rightarrow M^*\langle r \rangle$ .  
Every  $p,q,b;r$ -type is a  $p,q,b;r$ -type/prim.

Proof: Let  $M^*$  be a  $p,q,b;r$ -structure,  $M^* = (N^*, 0^*, 1^*, <^*, +^*, f^*, g^*, c_0^*, \dots)$ . Let  $\alpha$  be a closed term of length at most  $r$ , representing an element of  $M^*\langle r \rangle$ , in which some  $c_i$  appears. The value of  $\alpha$  must lie in  $[c_i^*, c_{i+1}^*)$ , where  $i$  is greatest such that  $c_i$  appears in  $\alpha$ . There are only finitely many such  $\alpha$  for each  $i$ . Also, if no  $c_i$  appears in  $\alpha$  then the value of  $\alpha$  lies in  $[0, c_1)$ , and there are only finitely many of these  $\alpha$ , as well. Hence the order type of  $M^*\langle r \rangle$  is  $\omega$ . Furthermore, there are obvious double exponential bounds on the sizes of these finite sets. We can use the  $p,q,b;r$ -type of  $M^*$  and the restricted indiscernibility of the  $c^*$ 's to obtain the increasing primitive recursive bijection  $f:N \rightarrow M^*\langle r \rangle$ .

Let  $\tau$  be the  $p,q,b;r$ -type of the  $p,q,b;r$ -structure  $M$ . We can build another  $p,q,b;r$ -structure on the basis of  $\tau$  using the appropriate equivalence relation on terms of bounded length, so that the equivalence classes are finite. This construction is very effective in  $\tau$ , and results in a  $p,q,b;r$ -structure/prim. QED

The following adds to Lemma 4.4.7.

LEMMA 4.4.7'. The following is provable in  $RCA_0$ . Every  $p,q,b;r,n$ -special type is a  $p,q,b;r,n$ -special type/prim.

Proof: Let  $\tau$  be a  $p,q,b;r,n$ -special type. By Lemma 4.4.4',  $\tau$  is a  $p,q,b;r$ -type/prim. From the proofs of Lemmas 4.4.5 and 4.4.6, we see that  $RCA_0$  proves that the witnesses to  $\tau$  being a  $p,q,b;r,n$ -special type are the same as the witnesses to some  $\lambda(k,n,p+q+2,R_1,\dots,R_{n-1})$  explicitly produced from  $p,q,b,r,n,\tau$ . Since  $\tau$  is a  $p,q,b;r,n$ -special type,  $\lambda(k,n,p+q+2,R_1,\dots,R_{n-1})$  is true. By Theorem 4.3.7',  $\lambda(k,n,p+q+2,R_1,\dots,R_{n-1})$  is primitively recursively true. Hence  $\tau$  is a  $p,q,b;r,n$ -special type/prim. QED

The following adds to Lemma 4.4.10.

LEMMA 4.4.10'. The following is provable in  $ACA' + 1\text{-Con}(\text{MAH})$ .  $(\forall p,q,b,n \geq 1) (\exists r) (\forall \tau) (\tau \text{ is a } p,q,b;r\text{-type} \rightarrow \tau \text{ is a } p,q,b;r,n\text{-special type/prim})$ .

Proof: By Lemma 4.4.7' and 4.4.10. QED



THEOREM 6.2.20. Propositions C,E-H are primitive recursively true. I.e., there exist infinite  $A,B,C$  whose enumeration functions are primitive recursive. This is provable in  $ACA' + 1-Con(MAH)$ .

Proof: We argue in  $ACA' + 1-Con(MAH)$ . Let  $p,q,b,n \geq 1$ , and  $f \in ELG(p,b)$ ,  $g \in ELG(q,b)$ , where  $f,g \in SD \cap BAF$ . Let  $r$  be given by Lemma 4.4.10'. By Lemma 6.2.18, we can find a  $p,q,b;r$ -structure  $M = (N,0,1,<,+,f,g,c_0,c_1,\dots)$ , where the  $c$ 's form a primitive recursive sequence of powers of 2. By Lemma 4.4.10',  $\tau$  is a  $p,q,b,n,r$ -special type/prim. Let  $M^* = (N^*,0^*,1^*,<^*,+^*,f^*,g^*,c_0^*,c_1^*,\dots)$  be a  $p,q,b;n,r$ -special structure/prim with  $p,q,b;r$ -type  $\tau$ . Let  $D_1^* \subseteq \dots \subseteq D_n^* \subseteq M^* \langle r \rangle$  be infinite, where  $D_1^* \subseteq \{c_0^*,c_1^*,\dots\}$ , each  $f^*D_i^* \subseteq D_{i+1}^* \cup g^*D_{i+1}^*$ , and  $D_1^* \cap f^*D_n^* = \emptyset$ , and where the enumeration functions of the  $D^*$ 's are primitive recursive. Since  $M,M^*$  have the same  $p,q,b;r$ -type,  $M^* \langle r \rangle$  and  $M \langle r \rangle$  are isomorphic by a primitive recursive bijection. This isomorphism sends  $D_1^*,\dots,D_n^*$  to infinite  $D_1 \subseteq \dots \subseteq D_n \subseteq M \langle r \rangle$  with primitive recursive enumeration functions, where  $D_1 \subseteq \{c_0,c_1,\dots\} \subseteq N \uparrow$ , and each  $fD_i \subseteq D_{i+1} \cup gD_{i+1}$ , and  $D_1 \cap fD_n = \emptyset$ . QED

Note that Theorem 6.2.20 provides us with explicitly  $\Pi^0_3$  forms of Propositions C,E-H as stated in Appendix A.

COROLLARY 6.2.21. Theorems 5.9.11 and 5.9.12 apply to Propositions C[prim], E[prim], F[prim], G[prim], H[prim].

Proof: By Theorem 6.2.20 and the fact that Propositions C[prim], E[prim], F[prim] immediately imply Propositions C,F,G. QED

Recall the tameness of the structure  $(N,+, \uparrow)$  used in Lemma 6.2.5.

DEFINITION 6.2.21. The superexponential is the function  $f:N \rightarrow N$  given by  $f(n) = 2^{2^{\dots^2}}$ , where there are  $n$  2's. Here  $f(0) = 1$ ,  $f(1) = 2$ .

We claim the same kind of tameness holds for  $(N,+, \uparrow)$ . This follows from the fact that the superexponential  $f$  satisfies the Semenov conditions discussed in section 4 of Appendix B.

The nontrivial fact that we need to verify is that for all  $m \geq 1$ , the residues of the values of  $f \bmod m$  are ultimately periodic.

Thus it follows from [Se83] that  $(\mathbb{N}, +, f)$  has a natural expansion with elimination of quantifiers, and  $(\mathbb{N}, +, f)$  is primitive recursively decidable. We make the following definitions.

LEMMA 6.2.22. If  $m$  is odd then the residues of  $f(0), f(1), \dots \bmod m$  are ultimately periodic.

Proof: Let  $2^k$  be congruent to 1 mod  $m$ . Let  $r > s \geq 1$  be such that  $g(r) \equiv g(s) \pmod{k}$ . Then  $g(r+1) \equiv g(s+1) \pmod{m}$ . To see this, we have to check that

$$2^{f(r)} - 2^{f(s)} \equiv 0 \pmod{m}.$$

Obviously,

$$2^{f(r)} - 2^{f(s)} = 2^{f(s)} (2^{f(r)-f(s)} - 1).$$

Since  $k | f(r) - f(s)$ , we see that  $2^{f(r)-f(s)} = (2^k)^{(f(r)-f(s))/k}$ . Since  $2^k \equiv 1 \pmod{m}$ , we see that  $2^{f(r)-f(s)} \equiv 1 \pmod{m}$ .

Hence we have periodicity for  $f(n)$ ,  $n \geq r$ , with period  $r-s$ . QED

LEMMA 6.2.23. If  $n \geq 1$  then the residues of  $g(0), g(1), \dots \bmod n$  are ultimately periodic.

Proof: Write  $n = 2^r m$ , where  $m \geq 1$  is odd. Then the residues of  $f(n), f(n+1), \dots \bmod n$  are just the residues of  $f(n)/2^r, f(n+1)/2^r, \dots \bmod m$ , multiplied by  $2^r$ . Since the later residues are ultimately periodic, the former residues are ultimately periodic. QED

THEOREM 6.2.24. Let  $f$  be the superexponential. The first order theory of the structure  $(\mathbb{N}, +, f)$  is primitive recursive.

Proof: By Lemma 6.2.23,  $f$  obeys the Semenov conditions from section 4 of Appendix B. QED

DEFINITION 6.2.22. The Presburger sets are the sets definable in  $(\mathbb{N}, +)$ . The exponentially Presburger sets are the sets definable in  $(\mathbb{N}, +, \uparrow)$ . The superexponentially

Presburger sets are the sets definable in  $(\mathbb{N}, +, f)$ , where  $f$  is the superexponential.

As stated earlier, we conjecture that a more careful argument will show that Propositions C, E-H hold in the superexponentially Presburger sets.

In light of the primitive recursive decision procedure for superexponential Presburger arithmetic in Theorem 6.2.24, Propositions C, E-H, when stated in the superexponentially Presburger sets, become  $\Pi_2^0$  statements. We conjecture that these  $\Pi_2^0$  statements are provably equivalent to  $1\text{-Con}(\text{SMAH})$  in  $\text{ACA}'$ .