Annals of Pure and Applied Logic 161 (2010) 504–510

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

journal homepage: www.elsevier.com/locate/apal

The strength of sharply bounded induction requires *MSP*

Sedki Boughattas [a], Leszek Aleksander Kołodziejczyk [b,*]

[a] *Équipe de Logique Mathématique, UFR de Mathématiques, Université Paris 7, Paris, France*

[b] *Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland*

ARTICLE INFO

Article history:
Received 7 June 2008
Received in revised form 10 March 2009
Accepted 30 March 2009
Available online 9 May 2009
Communicated by A.J. Wilkie

MSC:
03F30

Keywords:
Bounded arithmetic
Very weak arithmetic
Sharply bounded formulas
Unconditional independence results

ABSTRACT

We show that the arithmetical theory $T^0_2 + \hat{\Sigma}^b_1\text{-}IND^{|x|_5}$, formalized in the language of Buss, i.e. with $\lfloor x/2 \rfloor$ but without the *MSP* function $\lfloor x/2^y \rfloor$, does not prove that every nontrivial divisor of a power of 2 is even. It follows that this theory proves neither $NP = coNP$ nor S^0_2.

Some arithmetical theories are not merely weak but very weak, in the sense that they do not prove some very basic arithmetical fact or the totality of some extremely simple function. Among subsystems of Buss' bounded arithmetic S_2, the very weak theories are the only ones which we can separate from all of S_2 without using any unproven assumptions.

A few very weak theories have been known for a long time, but more recent discoveries of very weak (first-order) fragments of S_2 can be roughly divided into two groups. The first of these consists of induction schemes for Σ^b_n formulae, $n \geq 1$, restricted to very short initial segments. For example, Pollett proved in [9] that the theory $\hat{\Sigma}^b_1\text{-}IND^{|x|_4}$ (induction for strict Σ^b_1 formulae restricted to the range of the fourth iteration of the logarithm function), or more generally $\hat{\Sigma}^b_n\text{-}IND^{|x|_{n+3}}$, is very weak, as it does not prove the totality of the function $\lfloor x/3 \rfloor$. The result holds even if the language contains the *MSP* function, where $MSP(x, y) = \lfloor x/2^y \rfloor$. The bound on length of the induction can be improved: in [2], it was shown that Σ^b_1 induction restricted to $|x|_3$ (indeed, almost to $|x|_2$) is still very weak, although the proof of that result no longer works with *MSP* in the language.

The second group of very weak theories contains systems axiomatized by various schemes of induction for Σ^b_0, i.e. sharply bounded, formulae. It has been known since [11] that S^0_2, or polynomial induction for sharply bounded formulae, does not prove the totality of the predecessor function. The theory remains very weak even if the language is expanded by symbols for predecessor, subtraction, *MSP* and counting [6]. Sharply bounded length induction, L^0_2, is also very weak [7]. However, none of the methods applied to prove independence results for S^0_2, L^0_2 and related theories have worked for the usual sharply bounded induction scheme, T^0_2. Moreover, in a recent paper [5] Jeřábek showed that $T^0_2(MSP)$, that is, sharply bounded induction with *MSP* in the language, is surprisingly strong: it is equivalent to the well-known theory *PV*, and hence proves e.g. all the $\forall\Sigma^b_1$ consequences of S^1_2. The presence of *MSP* is essential for Jeřábek's argument, so the status of T^0_2 formulated in Buss' original bounded arithmetic language of #, $|\cdot|$ and $\lfloor \frac{\cdot}{2} \rfloor$ has remained an open problem.

* Corresponding author.
E-mail addresses: bougatas@logique.jussieu.fr (S. Boughattas), lak@mimuw.edu.pl (L.A. Kołodziejczyk).

0168-0072/$ – see front matter
doi:10.1016/j.apal.2009.03.002

The main theorem of the present paper solves this open problem and additionally provides a bridge between the two groups of results on very weak theories mentioned above. We show that Buss' original T^0_2, complemented by induction for strict Σ^b_1 formulae up to $|x|_5$, is very weak: it does not prove that all nontrivial divisors of powers of 2 are even. The theorem has two interesting corollaries: the theory $T^0_2 + \hat{\Sigma}^b_1\text{-}IND^{|x|_5}$ does not prove S^0_2 and (a certain formalization of) $NP = coNP$. A more general conclusion which can be drawn from our work is that the strength of severely restricted induction schemes depends crucially on the exact choice of language, and in particular on the presence of *MSP*.

Our methods are model-theoretic and rely strongly on [2]. We also need to extend Shepherdson's [10] classical analysis of sets defined by open formulae with $+$ and $\times$ to sharply bounded formulae involving also $\#$, $|\cdot|$ and $\lfloor \frac{\cdot}{2} \rfloor$. After discussing notational preliminaries in Section 1, we review relevant material from [2] in Section 2, present the analysis of sharply bounded formulae in Section 3, and prove our main theorem in Section 4. The final Section 5 contains proofs of the aforementioned corollaries and mentions a few open problems.

1. Definitions and notation

We assume that the reader is familiar with the basic notions and results of bounded arithmetic as presented in e.g. [3,4,8]. In particular, we assume some familiarity with the operations $\#$ and $|\cdot|$, the formula classes Σ^b_n and Π^b_n, the theory *BASIC* and notions such as "sharply bounded quantifier" etc. We work in the usual language of bounded arithmetic, with symbols for 0, 1, $\leq$, $+$, $\times$, $\#$, $|\cdot|$, and $\lfloor \frac{\cdot}{2} \rfloor$.

Recall the difference between (general) Σ^b_1 and strict Σ^b_1, or $\hat{\Sigma}^b_1$. Σ^b_1 formulae are built from sharply bounded formulae using &, $\vee$, bounded existential quantifiers and sharply bounded universal quantifiers. A $\hat{\Sigma}^b_1$ formula has to be of the form

$$\exists x_1 < t_1\, \exists x_2 < t_2\, \ldots \exists x_m < t_m\, \psi,$$

where ψ is sharply bounded (no universal sharply bounded quantifiers allowed within the initial existential block). A witness for a $\hat{\Sigma}^b_1$ formula is then simply a finite tuple of elements witnessing the initial existential quantifiers. The distinction between Σ^b_n and $\hat{\Sigma}^b_n$ also makes sense for $n > 1$, but we will not use it.

For $n \geq 0$, the theory T^n_2 is axiomatized by *BASIC* and the induction scheme for Σ^b_n formulae. In S^n_2, induction is replaced by the polynomial induction scheme,

$$\varphi(0)\ \&\ \forall x\,(\varphi(\lfloor x/2 \rfloor) \Rightarrow \varphi(x)) \Rightarrow \forall x\, \varphi(x).$$

For any k, $|x|_k$ denotes the k-th iteration of the $|\cdot|$ function on x, and $\hat{\Sigma}^b_1\text{-}IND^{|x|_5}$ is the induction scheme for $\hat{\Sigma}^b_1$ formulae with the conclusion restricted to the range of $|x|_5$.

Throughout the paper, $\mathcal{N}$, $\mathcal{R}$ are countable structures such that $(\mathcal{N}, \mathcal{R})$ is a nonstandard model of $\mathrm{Th}(\mathbb{N}, \mathbb{R}_{alg})$, where $\mathbb{R}_{alg}$ stands for the real algebraic numbers. Thus, $\mathcal{R}$ is a real-closed field, $\mathcal{N}$ has induction for all formulae involving $\mathcal{R}$ or parameters from $\mathcal{R}$, and we can code ($\mathcal{N}$-)finite sets of elements of $\mathcal{R}$ by elements of $\mathcal{N}$. $\mathcal{Q}$ is the fraction field of (the ring generated by) $\mathcal{N}$, and a is a nonstandard element of $\mathcal{N}$. Naturally, we have $\mathcal{N} \subseteq \mathcal{Q} \subseteq \mathcal{R}$, and $\mathcal{Q}$ can be interpreted in $\mathcal{N}$ in the usual way. Notation like $[b, c)$ represents the appropriate interval in $\mathcal{N}$ — we write $[b, c)_{\mathcal{Q}}$ or $[b, c)_{\mathcal{R}}$ to denote the corresponding interval in $\mathcal{Q}$ or $\mathcal{R}$, respectively. Notation like c^ω, 2^{c^ω} etc. represents the appropriate cuts in $\mathcal{N}$, but $b < c^\omega$ does not imply that $b \in \mathcal{N}$.

For $b \in \mathcal{R} \setminus \mathcal{N}$, $|b|$ is defined to equal $||\lfloor b \rfloor||$, where $\lfloor b \rfloor$ is the "true" integer part of b, contained in $\mathcal{N}$.

In any model of *BASIC*, a power of 2 is an element x satisfying $\exists y\, x = y\#1$. Being a power 2 can be equivalently expressed by the quantifier-free formula $2x = x\#1$.

A bar, as in $\bar{x}$, indicates a tuple, always of standard finite length. Notation like $\bar{x} < y$ and $\bar{x} \in X$ means that all elements of $\bar{x}$ are smaller than y or belong to X, respectively.

2. Log-euclidean chains

The present section contains a resume of relevant notions and results from [2]. In the simpler cases, we also provide brief sketches of proofs.

The key technical notion is that of a *log-euclidean chain* (*l.e. chain* for short). An l.e. chain is a coded (in $\mathcal{N}$) sequence $(A_i)_{i \leq d}$ of subsets of $\mathcal{Q}$ satisfying the following conditions:

(i) $\{a\} \cup [0, |a|] \subseteq A_0$,
(ii) for every $i < d$,
$(A_i + A_i) \cup (A_i \cdot A_i) \cup (A_i - A_i) \cup [0, |a|^{2^{i+1}}] \cup \{2^c : c \in [0, |a|^{i+1}]\} \subseteq A_{i+1}$,
(iii) for every $i < d$, $x \in A_i$, and integer $q \leq |a|^{2^i}$, A_{i+1} contains an integer part of x/q, i.e. a (unique) number y such that $y \leq x/q < y + 1$,
(iv) for every $i < d$ and $x \in (A_i)_+$, A_{i+1} contains $[0, |x|]$.
(v) A_d is discrete, i.e. $A_d \cap (0, 1)_{\mathcal{Q}} = \emptyset$.

An l.e. chain may contain both negative numbers and non-integers. In particular, the "integer part" of x/q in the sense of the chain does not have to be an integer. Nevertheless, we still use the notation $\lfloor x/q \rfloor$ in the hope that it does not lead to confusion.

We also often write (A_i) instead of $(A_i)_{i\le d}$ if no confusion arises. We say that $(B_i)_{i\le d'}$ *extends* $(A_i)_{i\le d}$ *levelwise* (written $(A_i)_{i\le d} \subseteq_\ell (B_i)_{i\le d'}$) if $d' \le d$ and for every $i \le d'$, $A_i \subseteq B_i$. Loosely speaking, (B_i) is "shorter but wider" than (A_i).

Whenever $(A_i)_{i\le d}$ is an l.e. chain and $I < d$ is a cut, $A_I := \bigcup_{i\in I} A_i \cap 2^{|a|^\omega}$ is a model of *BASIC*. This can be verified in a straightforward way: the least obvious axiom to check is $|2x+1| = |x|+1$. But the only case in which $|2x+1| > |x|+1$ occurs is when $2^{|x|} - 1/2 \le x < 2^{|x|}$, which cannot happen for $x \in A_I$ since A_d is discrete and $2^{|x|} \in A_\omega$.

Additionally, for each $(B_i)_{i\le d'} \supseteq_\ell (A_i)$ and $I < d'$, the range of the $|\cdot|$ function in B_I is always exactly equal to the cut $|a|^\omega$ in $\mathcal{N}$. This means that for $\bar{x} \in A_\omega$ and $\varphi \in \Sigma^b_0$, the truth value of $\varphi(\bar{x})$ in B_I depends only on A_ω. So, it makes sense to speak of the satisfaction of a sharply bounded formula "in the sense of the chain".

Proposition 2.1. *If $(A_i)_{i\le d}$ is an l.e. chain and $k < d$, then $(A_{i+k})_{i\le d-k}$ is also an l.e. chain.*

In other words, the "tail" of an l.e. chain is an l.e. chain as well. This follows immediately from the definition.

Proposition 2.2 (*"Kernel Lemma" in [2]*). *If $\{a\} \cup [0, |a|] \subseteq A \subseteq 2^{|a|^\omega}$, then for each $d \in \mathcal{N}$ there exists an l.e. chain $(A_i)_{i\le d}$ and a number $K \in \omega$ with $A_0 = A$ and* $\operatorname{card} A_i \le (\operatorname{card} A)^{2^{Ki}}$ *for each i.*

To obtain the l.e. chain whose existence is claimed, construct A_{i+1} from A_i simply by performing the requisite operations in $\mathcal{N}$. Note that the only situation in which (A_i) could fail to obey the stated size bound is if we need to include $[0, |b|]$ in A_{i+1} for some very large $b \in A_i$. This problem is avoided thanks to the additional assumption that $A \subseteq 2^{|a|^\omega}$.

Proposition 2.3. *Let $(A_i)_{i\le d}$ be an l.e. chain and let $b_1, \dots, b_l$ be a tuple of elements of $\mathcal{Q}_+$, $b_i < 2^{|a|^\omega}$ for each i. Assume that there exists an l.e. chain $(\tilde{B}_i)_{i\le \tilde{d}} \supseteq_\ell (A_i)$ with $\{b_1, \dots, b_l\} \subseteq \tilde{B}_0$. Then there exists $k \in \omega$ and an l.e. chain $(B_i)_{i\le \tilde{d}-k} \supseteq_\ell (A_i)$ with $\{b_1, \dots, b_l\} \subseteq B_0$ and* $\operatorname{card} B_i \le (\operatorname{card} A_i)^{2^{Ki}}$ *for some $K \in \omega$ and each i.*

So, whenever we can build an l.e. chain extending (A_i) levelwise and containing a fixed tuple of elements at the bottom level, we can build a similar l.e. chain, of almost the same length, whose levels additionally satisfy some size bounds.

The basic idea used in the construction of the new chain is to take $A_0 \cup \{b_1, \dots, b_l\}$ as the bottom level and build successive levels as the minimal sets which contain corresponding levels of (A_i) and satisfy clauses (ii), (iii) of the definition of l.e. chain (integer parts are taken in the sense of $(\tilde{B}_i)$). It then remains to make the resultant chain satisfy clause (iv): when $b_1, \dots, b_l < 2^{|a|^\omega}$, it turns out that it is enough to cut off the first finitely many levels and renumber the rest. The details are presented in the proof of Fact 2.2 part 2 in [2].

We conclude this section by stating without proof two much more difficult results which concern two important ways in which a given l.e. chain may be extended. In accordance with the practice of [2] and with the intuitive meaning of the results, we will refer to them as "Division Lemma" and "Integer Part Lemma", respectively.

Lemma 2.4 (*"Division Lemma"*). *Let $(A_i)_{i\le d}$ be an l.e. chain such that for some $K \in \omega$,* $\operatorname{card} A_i \le |a|^{2^{Ki}}$ *for each i, and $|a|^{2^{\omega d}} < a$. Then there is $r \in \mathcal{Q}_+$, $r \ne 1$, and an l.e. chain $(B_i)_{i\le \sqrt[3]{d}} \supseteq_\ell (A_i)$ such that:*

- $r, \frac{a}{r} \in B_0$,
- $\frac{r-1}{2} \in B_2$ *(i.e. r is odd in the sense of (B_i)),*
- *for some $L \in \omega$,* $\operatorname{card} B_i \le |a|^{2^{Li}}$ *for each i.*

Lemma 2.5 (*"Integer Part Lemma"*). *Let $(A_i)_{i\le d}$ be an l.e. chain such that for some $K \in \omega$,* $\operatorname{card} A_i \le |a|^{2^{Ki}}$ *for each i. Let $\beta \in \mathcal{Q}_+$, $\beta < 2^{|a|^\omega}$. Then there is $b \in \mathcal{Q}$, $\beta - 1 < b \le \beta$, and an l.e. chain $(B_i)_{i\le \sqrt[3]{d}} \supseteq_\ell (A_i)$ such that*

- $b \in B_0$,
- *for some $L \in \omega$,* $\operatorname{card} B_i \le |a|^{2^{Li}}$ *for each i.*

3. Translating sharply bounded formulae

Our aim now is to prove a technical lemma stating that the set of elements which, if added to an l.e. chain, will satisfy a sharply bounded formula in the sense of that chain, has a relatively simple structure:

Lemma 3.1. *Let $(A_i)_{i\le d}$ be an l.e. chain. Let $\varphi(x, \bar{p})$ be a Σ^b_0 formula, where $\bar{p}$ is a tuple of parameters from A_ω. Let n be the maximal nesting of $\lfloor \frac{\cdot}{2} \rfloor$ in φ. For every $k \in \omega$ there exists $K \in \omega$ and a set U of the form*

$$\bigcup_{i<|a|^K} I_i,$$

where I_i are disjoint intervals in $\mathcal{R}$, such that for every $x \in \mathcal{Q}_+$, $x < 2^{|a|^k}$, and every l.e. chain $(B_i)_{i<d'} \supseteq_\ell (A_i)$ with x contained in B_ω as a number divisible by 2^n: $\varphi(x, \bar{p})$ is true in B_ω iff $x \in U$.

Note that it is not claimed that membership in U corresponds to satisfaction of φ for all potential x, but only for those which will be included in a given l.e. chain as numbers divisible by 2^n. This restriction is nontrivial only if the formula φ contains applications of $\lfloor \frac{\cdot}{2} \rfloor$.

The main ingredient of the proof of Lemma 3.1 is:

Lemma 3.2. *Let $(A_i)_{i\leq d}$ be an l.e. chain. Let $\varphi(x, \bar{p})$ be a Σ_0^b formula, where $\bar{p}$ is a tuple of parameters from A_ω. Let n be the maximal nesting of $\lfloor \frac{\cdot}{2} \rfloor$ in φ. Let $r < 2^n$. For every $k \in \omega$ there exists a number $K \in \omega$ and a formula $\tilde{\varphi}_r(x, \bar{p})$ of the form:*

$$Q_1 i_1 < |a|^K Q_2 i_2 < |a|^K \ldots Q_m i_m < |a|^K \psi(x, \bar{p}, \bar{i}, 2^{i_1}, \ldots, 2^{i_m}, 2^{i_1 \cdot i_1}, 2^{i_1 \cdot i_2}, \ldots, 2^{i_m \cdot i_m}, 1/2),$$

where the Q_j are quantifiers and ψ is open in the language of $0, 1, \leq, +, \times, -$, such that:

for every $x \in \mathcal{Q}$, $x < 2^{|a|^k}$, and any chain $(B_i)_{i<d'} \supseteq_\ell (A_i)_{i\leq d}$ with x contained in B_ω as a number congruent to $r \bmod 2^n$, $\varphi(x, \bar{p})$ is true in B_ω iff $\tilde{\varphi}_r(x, \bar{p})$ is true (in $\mathcal{Q}$ or equivalently $\mathcal{R}$, but with the quantifiers interpreted in $\mathcal{N}$).

Proof. Fix r. The argument is by induction on the complexity of φ, but the steps for connectives and sharply bounded quantifiers are unproblematic, so essentially the only difficulty is the step for atomic formulae. Since $t_1 = t_2$ is equivalent to $t_1 \leq t_2 \,\&\, t_2 \leq t_1$, it is enough to define a correct translation of $t_1(x, \bar{p}) \leq t_2(x, \bar{p})$, where t_1, t_2 are terms of L_2. In what follows, we restrict our attention to just this task.

Let $K \in \omega$ be such that for $x < 2^{|a|^k}$, the formula $t_1(x, \bar{p}) \leq t_2(x, \bar{p})$ refers only to numbers below $2^{|a|^K}$ (note that $\bar{p} < 2^{|a|^\omega}$ by the definition of A_ω). Let T be the set of those terms t for which $|t|$, $t\#$ or $\#t$ appears in t_1 or t_2. Let $\bar{i}$ be a tuple of numbers $< |a|^K$ indexed by T (intended interpretation: i_t fixes the length $|\cdot|$ of the value of t).

For each subterm t of t_1 or t_2 we will define a term $\mathrm{repr}_{\bar{i}}(t)$ and a pair $\mathrm{rem}_{\bar{i}}(t)$ of the form $\langle u, \tilde{n}\rangle$, where $\tilde{n} \leq n$ and $u < 2^{\tilde{n}}$ (intended interpretation: $\mathrm{repr}_{\bar{i}}(t)$ represents t in the translation and has the same value as t if the lengths are as given by $\bar{i}$, while u is the value of $t \bmod 2^{\tilde{n}}$).

The definition of $\mathrm{repr}_{\bar{i}}(t)$ is as follows:

- $\mathrm{repr}_{\bar{i}}(x) = x$,
- $\mathrm{repr}_{\bar{i}}(p) = p$ for p among $\bar{p}$
- $\mathrm{repr}_{\bar{i}}(t + s) = \mathrm{repr}_{\bar{i}}(t) + \mathrm{repr}_{\bar{i}}(s)$,
- $\mathrm{repr}_{\bar{i}}(t \cdot s) = \mathrm{repr}_{\bar{i}}(t) \cdot \mathrm{repr}_{\bar{i}}(s)$,
- $\mathrm{repr}_{\bar{i}}(|t|) = i_t$,
- $\mathrm{repr}_{\bar{i}}(t\#s) = 2^{i_t \cdot i_s}$,
- $\mathrm{repr}_{\bar{i}}(\lfloor \frac{t}{2} \rfloor) = \begin{cases} \frac{\mathrm{repr}_{\bar{i}}(t)}{2} & \text{if } \mathrm{rem}_{\bar{i}}(t) = \langle 2v, \cdot\rangle, \\ \frac{\mathrm{repr}_{\bar{i}}(t)}{2} - \frac{1}{2} & \text{if } \mathrm{rem}_{\bar{i}}(t) = \langle 2v + 1, \cdot\rangle. \end{cases}$

The definition of $\mathrm{rem}_{\bar{i}}(t)$ is:

- $\mathrm{rem}_{\bar{i}}(x) = \langle r, n\rangle$,
- $\mathrm{rem}_{\bar{i}}(p) = \langle p \bmod 2^n, n\rangle$ where $p \bmod 2^n$ is taken in A_ω,
- $\mathrm{rem}_{\bar{i}}(t + s) = \langle u_1 + u_2 \bmod 2^{\min(\tilde{n}_1, \tilde{n}_2)}, \min(\tilde{n}_1, \tilde{n}_2)\rangle$ where $\mathrm{rem}_{\bar{i}}(t) = \langle u_1, \tilde{n}_1\rangle$, $\mathrm{rem}_{\bar{i}}(s) = \langle u_2, \tilde{n}_2\rangle$,
- $\mathrm{rem}_{\bar{i}}(t \cdot s)$ is defined analogously,
- $\mathrm{rem}_{\bar{i}}(|t|) = \langle i_t \bmod 2^n, n\rangle$,
- $\mathrm{rem}_{\bar{i}}(t\#s) = \langle 2^{i_t \cdot i_s} \bmod 2^n, n\rangle$,
- $\mathrm{rem}_{\bar{i}}(\lfloor \frac{t}{2} \rfloor) = \langle \lfloor \frac{u}{2} \rfloor, \tilde{n} - 1\rangle$ where $\mathrm{rem}_{\bar{i}}(t) = \langle u, \tilde{n}\rangle$.

Note that by the choice of n, the second element of $\mathrm{rem}_{\bar{i}}(t)$ is strictly positive whenever $\lfloor \frac{t}{2} \rfloor$ appears in t_1 or t_2, so that we always know whether to treat the value of t as even or odd.

The translation of $t_1(x, \bar{p}) \leq t_2(x, \bar{p})$ is now simply

$$\exists \bar{i} \leq |a|^K \left[\left(\bigwedge_{t\in T} 2^{i_t - 1} \leq \mathrm{repr}_{\bar{i}}(t) < 2^{i_t} \right) \,\&\, \mathrm{repr}_{\bar{i}}(t_1) \leq \mathrm{repr}_{\bar{i}}(t_2) \right].$$

This can be written as a single formula even though the shape of $\mathrm{repr}_{\bar{i}}(t)$ depends on $\bar{i}$. The reason is that to determine how to write each $\mathrm{repr}_{\bar{i}}(t)$ we only need a finite amount of information about $\bar{i}$: the remainders of each i_t modulo 2^n (to know $\mathrm{rem}_{\bar{i}}(|t|)$) and the information whether the value of each i_t is $0, 1, \ldots, n - 1$ or above n (to know $\mathrm{rem}_{\bar{i}}(t\#s)$).

In order to see that the translation is correct, note first that there exists exactly one tuple $\bar{i}$, dependent on x, r and $\bar{p}$ but independent of the chain (B_i), such that $\bigwedge_{t\in T}(2^{i_t - 1} \leq \mathrm{repr}_{\bar{i}}(t) < 2^{i_t})$ holds. Given this tuple $\bar{i}$, one may use induction on the complexity of a term to prove the following for all subterms t of t_1 or t_2: the value of $t(x, \bar{p})$ in the sense of the chain (B_i) is equal to $\mathrm{repr}_{\bar{i}}(t)$, and its remainder mod $2^{\tilde{n}}$ in the sense of (B_i) is u, where $\mathrm{rem}_{\bar{i}}(t) = \langle u, \tilde{n}\rangle$. The details of the inductive proof are rather straightforward and we leave them to the reader. □

Proof of Lemma 3.1. We only need to show that for each $\varphi(x,\bar{p}) \in \Sigma^b_0$, the set defined in $\mathcal{R}$ by $\tilde{\varphi}_0$, or, more generally, $\tilde{\varphi}_r$ for any $r < 2^n$, is of the required form. The proof is by induction on the complexity of subformulae of $\tilde{\varphi}_r$.

In the base step, $\psi(x,\bar{p})$ is an (in)equality between two polynomials from $\mathcal{Q}[x]$, which defines a finite union of disjoint intervals in $\mathcal{R}$ since $\mathcal{R}$ is real-closed. The step for negation is easy, as the complement of a disjoint union of at most logarithmically many intervals is also a disjoint union of at most logarithmically many intervals.

Thus, it is enough to deal with the steps for conjunction and the sharply bounded universal quantifier. To this end, we make the following:

Claim. Assume that $\{I^0_i\}_{i<r}$ and $\{I^1_i\}_{i<s}$ are families of pairwise disjoint intervals. Then the set $(I^0_0\cup\cdots\cup I^0_{r-1})\cap(I^1_0\cup\cdots\cup I^1_{s-1})$ can be presented as a disjoint union of at most $r+s$ intervals $J_0\cup\cdots\cup J_{r+s-1}$.

Except for the trivial case when both r and s are 0, the number of intervals needed is actually $r+s-1$. The claim is readily proved by induction on $r+s$. The base step is obvious. In the induction step, assume that in each of the two families the intervals are numbered from left to right and consider the interval with the rightmost left end among $I^0_0,\ldots,I^0_{r-1},I^1_0,\ldots,I^1_{s-1}$, say I^0_{r-1}. By the inductive assumption, we know that $(I^0_0\cup\cdots\cup I^0_{r-2})\cap(I^1_0\cup\cdots\cup I^1_{s-1})$ is a disjoint union of at most $r+s-1$ intervals. I^0_{r-1} cannot intersect any of the I^1_i other than I^1_{s-1}, so it contributes at most one more interval to that union.

By the claim, the number of disjoint intervals increases by a factor which is standard in the step for conjunction and a standard power of $|a|$ in the step for sharply bounded universal quantifier. This is exactly what we need to complete the proof. □

4. The main construction

Theorem 4.1. *The theory $T^0_2+\hat{\Sigma}^b_1$-$IND^{|x|_5}$ does not prove that every nontrivial divisor of a power of 2 is even.*

To prove the theorem, we start with an l.e. chain $(A^0_i)_{i\le d}$ obtained by applying the Division Lemma 2.4 to a power of 2. That is, A^0_0 contains a, r, $\frac{a}{r}$ where $a=2^{|a|-1}$ and $r\neq 1$ is odd in the sense of (A^0_i). The Division Lemma lets d be any number satisfying $|a|^{2^{\omega d^3}}<a$, which is equivalent to $\omega d^3<|a|_2$.

Define $b_0:=2$ and $d_0:=d$. Choose s such that $2^{2^{s^\omega}}<d$. In particular, for large enough d, s can be $\ge |a|_5$. Note that by overspill, $2^{c^{s^c}}<d$ for some small nonstandard c (since $2^{c^{s^c}}<2^{2^{s^{c+1}}}$ for sufficiently small c).

Our construction has ω stages. At each stage m, we will have b_m, d_m and an l.e. chain $(A^m_i)_{i\le d_m}$ such that:

- the sequence $(b_m)_{m<\omega}$ is increasing, $(d_m)_{m<\omega}$ is decreasing,
- $b_m{}^{2^{s^\omega}}<d_m$,
- $(A^{m-1}_i)_{i\le d_{m-1}}\subseteq_\ell (A^m_i)_{i\le d_m}$,
- for some $L\in\omega$ dependent on m, card $A^m_i\le |a|^{2^{Li}}$ for each i.

Our final model will be $\bigcup_{m<\omega}A^m_\omega$. We will use the odd stages to guarantee that this structure satisfies induction for Σ^b_0 formulae, and the even stages to make sure that it satisfies induction for $\hat{\Sigma}^b_1$ formulae up to s.

Fix an enumeration of pairs consisting of a Σ^b_0 formula with parameters from $\mathcal{Q}$ and a number from $[0,2^{|a|^\omega})_{\mathcal{Q}}$. Fix separately an enumeration of $\hat{\Sigma}^b_1$ formulae with parameters from $\mathcal{Q}$. We may assume that in both enumerations each element occurs infinitely often.

Stage m odd. Let $\varphi(x,\bar{p})$ be the $\frac{m-1}{2}$-th Σ^b_0 formula and q the $\frac{m-1}{2}$-th number from $[0,2^{|a|^\omega})_{\mathcal{Q}}$. Put $b_m:=b_{m-1}$ and $d_m:=\sqrt[3]{d_{m-1}}$. If $\bar{p}\notin A^{m-1}_\omega$, $q\notin A^{m-1}_\omega$ or $A^{m-1}_\omega\models\neg\varphi(0,\bar{p})\vee\varphi(q,\bar{p})$, do nothing else (i.e. let the A^ms be the A^{m-1}s). Otherwise we have one of the following three cases:

(i) there exists $y<|a|^\omega$ such that $A^{m-1}_\omega\models\neg\varphi(y,\bar{p})$,
(ii) there exists $y<|a|^\omega$ such that $A^{m-1}_\omega\models\varphi(q-y,\bar{p})$,
(iii) none of the above.

In cases (i) and (ii), we again do nothing: an element witnessing induction for $\varphi(x,\bar{p})$ is already in A^{m-1}_ω. This can be proved using induction in $\mathcal{N}$, since for $x\in[0,y]$ the properties $A^{m-1}_\omega\models\varphi(x,\bar{p})$ and $A^{m-1}_\omega\models\varphi(q-x,\bar{p})$, both of which refer only to finitely many levels of A^{m-1}_ω and to a bounded fragment of $2^{|a|^\omega}$, can be expressed in $\mathcal{N}$.

If case (iii) occurs, let n be the nesting depth of $\lfloor\frac{\cdot}{2}\rfloor$ in φ, let k be such that $q<2^{|a|^k}$ and consider the set $\bigcup_{i<|a|^K}I_i$ given by Lemma 3.1. Since there are more than $|a|^K$ numbers divisible by 2^{n+1} below $|a|^\omega$, at least two of them have to be in the same I_i, which must therefore have length at least 2^{n+1}.

The complement of $\bigcup_{i<|a|^K}I_i$ in $[0,q]_{\mathcal{R}}$ is also a disjoint union of intervals $\bigcup_{j<|a|^K}J_j$. Again, as there are more than $|a|^K$ numbers of the form $q-x$, $x<|a|^\omega$, divisible by 2^{n+1} in the sense of (A^{m-1}_i), there exists a J_j of length at least 2^{n+1}.

Call intervals of length $\ge 2^{n+1}$ large. Among the I_i and J_j such that I_i,J_j are large and $I_i<J_j$, choose those for which the distance between I_i and J_j is minimal. Since there are fewer than $2|a|^K$ intervals in between, and all of them are small, the distance between I_i and J_j is smaller than $2^{n+2}|a|^K$ — in particular, it is smaller than $|a|^\omega$.

By the Integer Part Lemma and the fact that $\mathcal{Q}$ is dense in $\mathcal{R}$, there exists $y \in I_i \cap \mathcal{Q}$ and an l.e. chain $(B_i)_{i\le d_m} \supseteq_\ell (A_i^{m-1})_{i\le d_{m-1}}$ obeying the required size bound such that y is contained in B_0. Due to the length of I_i, this implies that some $\tilde{y} \in I_i$ is contained in B_1 as a number divisible by 2^n, so that $B_\omega \models \varphi(\tilde{y}, \bar{p})$.

We may assume that the distance between $\tilde{y}$ and the right end of I_i is smaller than 2^{n+1}, so the distance between $\tilde{y}$ and J_j is smaller than $2^{n+2}|a|^K + 2^{n+1}$. Thus, by the definition of an l.e. chain and the length of J_j, some element of J_j of the form $\tilde{y} + z$, where z is an integer smaller than $|a|^\omega$, is contained in $B_{|K|+1}$ as number divisible by 2^n. But this means that $B_\omega \models \neg\varphi(\tilde{y} + z, \bar{p})$, and, like in cases (i) and (ii), induction in $\mathcal{N}$ finds an element witnessing induction for $\varphi(x, \bar{p})$ in B_ω. Hence, we may take (A_i^m) to be (B_i).

Stage $m > 0$ even. Let $\psi(x, \bar{p})$ be the $\frac{m}{2}$-th $\hat{\Sigma}_1^b$ formula. Assume $\bar{p} \in A_\omega^{m-1}$ (otherwise we do not have to do anything). We want to divide the interval $[b_{m-1}, d_{m-1})$ in a definable way into $s+2$ disjoint intervals $[\beta_j, \beta_{j+1})$ so that $\beta_j^{2^{s^\omega}} < \beta_{j+1}$. This can be done: if $(b_{m-1})^{c^{(s+2)^c}} < d_{m-1}$ for a small nonstandard c, take $\beta_j := (b_{m-1})^{c^{j(s+2)^{c-1}}}$.

We will now use the pigeonhole principle in a similar way as in [1,2]. Consider the definable function which sends $r \le s$ to the smallest $j \le s+1$ for which there is no l.e. chain $(B_i)_{i\le\beta_{j+1}} \supseteq_\ell (A_i^{m-1})$ with a witness for $\psi(r, \bar{p})$ contained in B_0 (send r to $s+1$ if no such j exists). By the pigeonhole principle in $\mathcal{N}$, this function cannot be surjective, so there exists some $j \le s+1$ such that $\forall r \le s\,(\xi(r, j) \Rightarrow \xi(r, j+1))$, where $\xi(r, j)$ is the formula:

> "there exists an l.e. chain $(B_i)_{i\le\beta_j} \supseteq_\ell (A_i^{m-1})$
> such that B_0 contains a witness for $\psi(r, \bar{p})$."

Fix such a j, let $b_m := \beta_j$, and take d_m to be some number $< \beta_{j+1} - \omega$ such that $\beta_j^{2^{s^\omega}} < d_m$ remains satisfied. By the choice of j, for every $r \le s$ such that there exists $(B_i)_{i\le\beta_j} \supseteq_\ell (A_i^{m-1})$ with a witness for $\psi(r, \bar{p})$ in B_0 and β_j levels, there also exists a similar chain with β_{j+1} levels, hence with more than $d_m + \omega$ levels. So, using Proposition 2.3, take $(A_i^m)_{i\le d_m}$ to be some $(B_i)_{i\le d_m} \supseteq_\ell (A_i^{m-1})$ obeying the required size bound such that:

(i) if $\neg\xi(0, j)$, then $B_t = A_t^{m-1}$ for each $t \le d_m$,
(ii) if $\xi(s, j)$, then B_0 contains a witness for $\psi(s, \bar{p})$,
(iii) if $\xi(0, j) \,\&\, \neg\xi(s, j)$, which implies the existence of $r < s$ such that $\xi(r, j) \,\&\, \neg\xi(r+1, j)$, then B_0 contains a witness for $\psi(r, \bar{p})$ for some such r.

This completes the description of stage m for even m.

Now let $\mathcal{M}$ be $\bigcup_{m<\omega} A_\omega^m$. It is relatively easy to see that $\mathcal{M}$ satisfies T_2^0, and that $\mathcal{M}$ contains a power of 2 which is divisible by an odd number greater than 1. Additionally, the range of $|x|_5$ in $\mathcal{M}$ is bounded by s. Thus, we only need to check that $\mathcal{M} \models \hat{\Sigma}_1^b\text{-}IND^s$.

Let $\psi(x, \bar{p})$ be a $\hat{\Sigma}_1^b$ formula with parameters from $\mathcal{M}$ and choose m such that $\psi(x, \bar{p})$ was considered at stage m and all the parameters were already in A_ω^{m-1}. If at that point case (ii) occurred, then clearly $\mathcal{M} \models \psi(s, \bar{p})$. On the other hand, if case (i) occurred then $\mathcal{M} \models \neg\psi(0, \bar{p})$. This can be seen as follows: if a witness for $\psi(0, \bar{p})$ shows up in $\mathcal{M}$, then it must already be in some A_i^n, $m < n < \omega$, $i < \omega$. But if we renumber $A_i^n \subseteq \cdots \subseteq A_{d_n}^n$ as $B_0 \subseteq \cdots \subseteq B_{d_n - i}$, then this chain of Bs contradicts $\neg\xi(0, j)$ at stage m (note that the β_j at stage m is b_m, and $b_m < d_n - \omega$).

A similar analysis shows that if case (iii) occurred, then $\mathcal{M}$ contains some $r < s$ such that $\psi(r, \bar{p}) \,\&\, \neg\psi(r+1, \bar{p})$. Altogether, $\mathcal{M}$ satisfies induction for ψ up to s, which completes the proof of the theorem.

Remark. The reader may wonder why our proof works for formulae containing $\lfloor x/2 \rfloor$ but does not work for *MSP*. The basic difference is as follows. Consider a sharply bounded formula φ and an element x which we might want to add to some l.e. chain. By Lemma 3.1, to determine what the value of $\varphi(x)$ will be in the new chain it is enough to know the intended value of x mod 2^n, or equivalently $\lfloor x/2^n \rfloor$, for some $n \in \omega$. Additionally, for any specific choice of values of remainders modulo 2^n, an element with exactly those remainders can be found reasonably close to any given element of the chain (cf. case(iii) in the odd stage in the proof of Theorem 4.1). If φ contained *MSP*, we would need to specify x mod 2^y and $\lfloor x/2^y \rfloor$ for all $y < |x|$. But remainders/integer parts of division by large powers of 2 in general do not exist in an l.e. chain, and even when they do, elements with the "right" values of remainders are so sparsely distributed that we have very little control over them.

Although we have not checked the details, we believe that the borderline case to which our argument could be applied is formulae with a symbol for $\lfloor x/2^{|y|} \rfloor$. We also note that T_2^0 does prove the totality of the *MSP* function (already open induction does) — the point is that this function cannot be freely used in induction formulae.

5. Corollaries and open problems

One consequence of our main theorem is that, somewhat informally speaking, the theory $T_2^0 + \hat{\Sigma}_1^b\text{-}IND^{|x|_5}$ does not prove that $NP = coNP$. The following corollary presents two precise versions of that statement.

Corollary 5.1. (1) *There exists a model $\mathcal{M} \models T_2^0 + \hat{\Sigma}_1^b\text{-}IND^{|x|_5}$ and a $\hat{\Pi}_1^b$ formula $\varphi(x)$ which is not equivalent in $\mathcal{M}$ to a $\hat{\Sigma}_1^b$ formula, even with parameters.*

(2) *The formula "x is a prime number" is not provably equivalent in* $T_2^0 + \hat{\Sigma}_1^b$-$IND^{|x|_5}$ *to any* Σ_1^b *formula* $\psi(x)$.

Proof. The basic idea behind both proofs is simple and has been applied before, for example in [2]. If (1) were false, then in every $\mathcal{M} \models T_2^0 + \hat{\Sigma}_1^b$-$IND^{|x|_5}$ each bounded formula would be equivalent to a $\hat{\Sigma}_1^b$ formula with parameters. But this would mean that $\mathcal{M}$ satisfies bounded induction up to $|x|_5$, hence full bounded induction, contradicting the fact that full bounded induction proves that nontrivial divisors of powers of 2 are even.

To prove (2), assume that primality is equivalent in $T_2^0 + \hat{\Sigma}_1^b$-$IND^{|x|_5}$ to a (not necessarily strict) Σ_1^b formula $\psi(x)$. Let $\mathcal{N}$ be a model of a strong arithmetic as before, but let $a \in \mathcal{N}$ now be a nonstandard prime instead of a power of 2. $\mathcal{N} \models \psi(a)$, so we can now repeat the construction of the previous section with A_0^0 containing a, a nontrivial divisor of a, and for any interpretation of the universal quantifiers of $\psi(a)$, a tuple witnessing all the existential quantifiers (this is possible by Proposition 2.2, since we need $< |a|^\omega$ witnesses, and each of them is $< 2^{|a|^\omega}$). We get a model $\mathcal{M}$ in which $\psi(a)$ is still true, but a is no longer a prime. □

Remark. Parts (1) and (2) of the corollary are logically incomparable. The advantage of part (2) is that it speaks of a concrete Π_1^b formula not equivalent to a Σ_1^b formula and that it deals with all Σ_1^b formulae, not just the strict ones. However, part (2) concerns only provable equivalence in the theory: it does not rule out the possibility that in every model of the theory primality can be defined by a Σ_1^b formula which depends on the model and perhaps contains parameters. To know that there are models in which some Π_1^b property really is not (strict) Σ_1^b, we must use part (1).

We now turn to the problem whether T_2^0 proves S_2^0. For $n \geq 1$, it is easy to check that T_2^n implies S_2^n, but the argument does not work for $n = 0$ without *MSP* in the language, and the question whether $T_2^0 \vdash S_2^0$ has been an open problem.

Corollary 5.2. S_2^0 *proves that every nontrivial divisor of a power of* 2 *is even. Hence,* $T_2^0 \nvdash S_2^0$.

Proof. Work in S_2^0 and assume that $r > 1$ is odd. We will use polynomial induction to prove that for every $x \geq 1$, rx is not a power of 2, where being a power of 2 is expressed by the open formula $2x = x\#1$. Thus, we need to show that r is not a power of 2, and if rx is not a power of 2, then neither $2rx$ nor $r(2x+1)$ is a power of 2.

It is easy to prove in S_2^0 that all powers of 2 greater than 1 are even, so $r \cdot 1 = r$ is not a power of 2, and neither is $r(2x+1)$ for any x. Now assume that rx is not a power of 2. If $2rx$ is, then $4rx = (2rx)\#1$. But by the *BASIC* axioms, $(2rx)\#1 = 2 \cdot ((rx)\#1)$, so $2 \cdot 2rx = 2 \cdot ((rx)\#1)$, which implies $2rx = (rx)\#1$, a contradiction. □

Remark. It follows from the corollary and results mentioned in the introduction that S_2^0 and T_2^0 are incomparable.

A number of open problems related to very weak theories remain. For example, it would be nice to extend the amount of $\hat{\Sigma}_1^b$ induction in our theory to $|x|_3$ or $|x|_4$, or to drop the strictness condition on Σ_1^b formulae. We also do not know whether S_2^0 remains very weak when complemented by some amount of $\hat{\Sigma}_1^b$ induction. Finally, virtually nothing nontrivial is known about the strength of $T_2^0 + S_2^0$.

Acknowledgements

The work presented in this paper grew out of the meetings of a research group on "Model-theoretic methods in the study of weak arithmetics". The meetings took place in Warsaw in 2008 and were supported by the Stefan Banach International Mathematical Centre. We would like to thank the other members of the group: Zofia Adamowicz, Jean-Pierre Ressayre, and Konrad Zdanowski, for stimulating conversations and criticism. We also thank the two anonymous referees for a number of helpful comments.

The second author was partially supported by grant N N201 382234 of the Polish Ministry of Science and Higher Education.

References

[1] Z. Adamowicz, L.A. Kołodziejczyk, Well-behaved principles alternative to bounded induction, Theoretical Computer Science 322 (2004) 5–16.
[2] S. Boughattas, J.P. Ressayre, Bootstrapping, Annals of Pure and Applied Logic (under review).
[3] S. Buss, Bounded Arithmetic, Bibliopolis, 1986.
[4] P. Hájek, P. Pudlák, Metamathematics of First-Order Arithmetic, Springer-Verlag, 1993.
[5] E. Jeřábek, The strength of sharply bounded induction, Mathematical Logic Quarterly 52 (2006) 613–624.
[6] J. Johannsen, On the weakness of sharply bounded polynomial induction, in: G. Gottlob, A. Leitsch, D. Mundici (Eds.), Computational Logic and Proof Theory, in: Lecture Notes in Computer Science, vol. 713, Springer-Verlag, 1993, pp. 223–230.
[7] J. Johannsen, A model-theoretic property of sharply bounded formulae, with some applications, Mathematical Logic Quarterly 44 (1998) 205–215.
[8] J. Krajíček, Bounded Arithmetic, Propositional Logic, and Complexity Theory, Cambridge University Press, 1995.
[9] C. Pollett, Multifunction algebras and the provability of PH↓, Annals of Pure and Applied Logic 104 (2000) 279–303.
[10] J.C. Shepherdson, A non-standard model for a free variable fragment of number theory, Bulletin de l'Académie Polonaise des Sciences. Série des Sciences Mathématiques, Astronomiques et Physiques 12 (1964) 79–86.
[11] G. Takeuti, Sharply bounded arithmetic and the function $a-1$, in: W. Sieg (Ed.), Logic and computation, in: Contemporary Mathematics, vol. 106, AMS, 1990, pp. 281–288.