Electronic Colloquium on Computational Complexity, Report No. 34 (2003)

Height restricted constant depth LK

Arnold Beckmann*
Institute of Algebra and Computational Mathematics
Vienna University of Technology
Wiedner Hauptstr. 8-10/118
A-1040 Vienna, Austria†

March 17, 2003

Abstract

Height restricted constant depth LK is a natural restriction of GENTZEN's propositional proof system LK. A sequence $(\varphi_n)_n$ of LK-formulas has polylogarithmic-height restricted depth-d-LK proofs iff the φ_n's possess LK-proofs where cut-formulas are of depth $d+1$ with small bottom fanin and of size quasi-polynomial in n, and the height of the proof tree is bounded polylogarithmic in n. We will proof a separation of polylogarithmic-height restricted depth-d-LK proofs from quasi-polynomial-size tree-like depth-d-LK proofs using the order induction principle. Our lower bounds technique utilizes HÅSTAD's Switching Lemmas to obtain so called "cut-reduction by switching".

We will further explain the connection of height restricted constant depth LK to theories of relativized bounded arithmetic. Separations of height restricted constant depth LK in turn yield separations of relativized bounded arithmetic.

Keywords: Propositional proof systems with height restrictions; Bounded Arithmetic; Cut-reduction by switching; Håstad's Switching Lemma

1 Introduction

LK denotes a natural modification of GENTZEN's sequent calculus for propositional logic with connectives $\neg$ and $\bigvee, \bigwedge$ (both of arbitrary but finite arity). A sequence $(\varphi_n)_n$ of LK-formulas is Σ_d-LK provable iff the φ_n have LK-proofs where cut-formulas are of depth $d+1$ with small bottom fanin, and are of size quasi-polynomial[1] in n. We will put further restrictions on proofs by bounding

*Supported by a Marie Curie Individual Fellowship #HPMF-CT-2000-00803 from the European Commission.

†email: beckmann@logic.at

[1] A function $f(n)$ grows quasi-polynomial (in n) iff $f(n) \in 2^{(\log n)^{O(1)}}$.

ISSN 1433-8092

the height of proof trees. $(\varphi_n)_n$ has polylogarithmic-height restricted Σ_d-LK proofs iff the shortest height of a Σ_d-LK derivation tree of φ_n grows polylogarithmic[2] in n. In this paper we will show that polylogarithmic-height restricted Σ_d-LK is a proper subsystem of quasi-polynomial-size tree-like Σ_d-LK – this extends our results from [4] where we have separated polylogarithmic-height restricted resolution from quasi-polynomial-size tree-like resolution (i.e., the case $d = 0$). Our separation will make use of the order induction principle which can be phrased as minimization in the form that if some propositional variables among $p_0, \ldots, p_{m-1}$ are false then there is a false one with minimal index. Our separating tautologies $\mathcal{O}\mathrm{Ind}^d(m)$ are then obtained from the order induction principle by replacing variables by SIPSER functions of depth d in m^d new variables. The separation will be obtained by characterizing the minimal height of a Σ_d-LK proof of $\mathcal{O}\mathrm{Ind}^d(f(n))$ when $f(n)$ is a function in n which grows super-polylogarithmically, i.e. faster than $(\log n)^c$ for any $c \in \mathbb{N}$. We will call the function which maps n to the minimal height of a Σ_d-LK proof of $\mathcal{O}\mathrm{Ind}^d(f(n))$ the *d-th height complexity of* $\mathcal{O}\mathrm{Ind}^d(f(n))$.

Our Main Theorem will be characterizing the growth of the d-th height complexity of $\mathcal{O}\mathrm{Ind}^d(f(n))$ by $f(n)^{\Theta(1)}$. In particular, this implies the separation of polylogarithmic-height restricted Σ_d-LK from quasi-polynomial-size tree-like Σ_d-LK, as $(\mathcal{O}\mathrm{Ind}^d(n))_n$ has tree-like cut-free-LK proofs of size linear in n, but our Main Theorem shows that provability in polylogarithmic-height restricted Σ_d-LK would imply polylogarithmic upper bounds to the identity function, hence it cannot be provable in polylogarithmic-height restricted Σ_d-LK. Furthermore, for any number-theoretic functions f, g such that $g(n)$ eventually grows stronger than the maximum of $(\log n)^c$ and $f(n)^c$ for any $c \in \mathbb{N}$, we obtain that f-height restricted Σ_d-LK is separated from g-height restricted Σ_d-LK.

Our lower bounds technique utilizes a method from Boolean complexity called "HÅSTAD's Switching Lemma" to prove a cut-reduction technique which we will call "cut-reduction by switching". The utilization of HÅSTAD's Switching Lemma follows [7] where it is applied to oracle computations. In [11] the same approach is used to reduce the complexity of Σ_d-LK refutations.

Height restricted proof systems naturally occur when proofs of bounded arithmetic theories are translated to propositional proof systems. In the following, we will explain this connection a little further.

Theories of bounded arithmetic have been introduced by BUSS in [5]. They are logical theories of arithmetic where formulas and induction are restricted (bounded) in such a way that provability in those theories can be tightly connected to complexity classes (cf. [5, 12]). A hierarchy of bounded formulas, Σ_i^b, and of theories $\mathrm{S}_2^1 \subseteq \mathrm{T}_2^1 \subseteq \mathrm{S}_2^2 \subseteq \mathrm{T}_2^2 \subseteq \mathrm{S}_2^3 \ldots$ has been defined (cf. [5]). The class of predicates definable by Σ_i^b formulas is precisely the class of predicates in the ith level Σ_i^p of the polynomial time hierarchy. The Σ_i^b-definable functions of S_2^i form precisely the ith level of the polynomial time hierarchy of functions, the latter being given by those functions which are polynomial time computable with an oracle from Σ_{i-1}^p.

[2] A function $f(n)$ grows polylogarithmic (in n) iff $f(n) \in (\log n)^{O(1)}$.

$$\begin{tikzcd}
\mathrm{S}_2^{d+1}(\alpha) \arrow[r, hook] \arrow[d, phantom, "\rotatebox[origin=c]{-90}{$\subsetneq$}"] & \text{polylogarithmic-height } \Sigma_d\text{-LK} \arrow[d, phantom, "\rotatebox[origin=c]{-90}{$\subsetneq$}"] \\
\mathrm{T}_2^{d+1}(\alpha) \arrow[r, hook] & \text{quasi-polynomial-size tree-like } \Sigma_d\text{-LK} \arrow[d, phantom, "\rotatebox[origin=c]{-90}{$\subsetneq$}"] \\
 & \text{quasi-polynomial-size sequence-like } \Sigma_d\text{-LK}
\end{tikzcd}$$

Figure 1: Translations and separations of $\mathrm{S}_2^{d+1}(\alpha)$ and $\mathrm{T}_2^{d+1}(\alpha)$ and related Σ_d-LK systems.

It is an open problem of bounded arithmetic whether the hierarchy of theories collapses. This is connected with the open problem of complexity theory whether the polynomial time hierarchy PH collapses. The hierarchy of bounded arithmetic collapses if and only if PH collapses provably in bounded arithmetic (cf. [14, 6, 18]). The case of relativized complexity classes and theories is completely different. The existence of an oracle A is proven in [1, 17, 8], such that the polynomial time hierarchy in this oracle PH^A does not collapse. Building on this one can show $\mathrm{T}_2^i(\alpha) \neq \mathrm{S}_2^{i+1}(\alpha)$ (cf. [14]). Here, the relativized theories $\mathrm{S}_2^i(\alpha)$ and $\mathrm{T}_2^i(\alpha)$ result from S_2^i and T_2^i, resp., by adding a free set variable α and the relation symbol $\in$. Similarly also, $\mathrm{S}_2^i(\alpha) \neq \mathrm{T}_2^i(\alpha)$ is proven in [10], and separation results for further relativized theories (dubbed $\Sigma_d^b(\alpha)$-L^mIND – a definition can be found e.g. in [2, 3]) are proven in [16]. Independently of these, and with completely different methods, we have shown separation results for relativized theories of bounded arithmetic using a method called *dynamic ordinal analysis* [2, 3]. Despite all answers in the relativized case, all separation questions continue to be open for theories without set parameters.

Propositional proof systems and bounded arithmetic theories are connected. In [13, 3.1] it is shown that $\mathrm{T}_2^1(\alpha)$ translates to *quasi-polynomial-size tree-like* Σ_0-LK proofs utilizing the PARIS-WILKIE-translation of language [15]. Similarily, it can be shown that provability in $\mathrm{T}_2^{d+1}(\alpha)$ translates to *quasi-polynomial-size tree-like* Σ_d-LK proofs. An examination of dynamic ordinal analysis (cf. [2, 3]) shows that provability in $\mathrm{S}_2^{d+1}(\alpha)$ and $\mathrm{T}_2^d(\alpha)$ can be translated to *polylogarithmic-height restricted* Σ_d-LK proofs. As explained above, we show a separation of polylogarithmic-height restricted Σ_d-LK from quasi-polynomial size tree-like Σ_d-LK using the order induction principle. KRAJÍČEK has proven in [11] a super-polynomial speed-up in size between sequence-like and tree-like Σ_d-LK utilizing the weak pigeonhole principle. Therefore, we obtain translations and separations of bounded arithmetic theories $\mathrm{S}_2^d(\alpha)$ and $\mathrm{T}_2^d(\alpha)$ and connected proof systems as represented in Fig. 1.

In addition to this, we will extend our results to further bounded arithmetic theories $\Sigma_d^b(\alpha)$-L^mIND and corresponding sub-linear-height restrictions given by functions $n \mapsto 2_i\left((\log^{(i+1)} n)^{O(1)}\right)$ for $i \geq 0$.

2 The Proof System Σ_d-LK

Let $\mathbb{N}$ denote the non-negative integers $0, 1, 2, \ldots$.

We recall the definition of language and formulas of GENTZEN's propositional proof system LK. LK consists of constants $0, 1$, propositional variables $p_0, p_1, p_2 \ldots$ (also called atoms; we may use $x, y, \ldots$ as meta-symbols for variables), the connectives negation $\neg$, conjunction $\bigwedge$ and disjunction $\bigvee$ (both of unbounded finite arity), and auxiliary symbols like brackets. Formulas are defined inductively: constants, atoms and negated atoms are formulas (they are called literals), and if φ_i is a formula for $i < I$, so are $\bigwedge_{i<I} \varphi_i$ and $\bigvee_{i<I} \varphi_i$. $\neg\varphi$ is an abbreviation of the formula formed from φ by interchanging $\bigwedge$ and $\bigvee$, 0 and 1, and atoms and their negations. The *logical depth*, or just *depth*, $\mathrm{dp}(\varphi)$ of a formula φ, is the maximal nesting of $\bigwedge$ and $\bigvee$ in it. In particular, constants and atoms have depth 0, the depths of φ and $\neg\varphi$ are equal, and $\mathrm{dp}(\bigvee_{i<I} \varphi_i)$ equals $1 + \max_{i<I} \mathrm{dp}(\varphi_i)$.

In our setting, *cedents* $\Gamma, \Delta, \ldots$ are finite *sets* of formulas, not *sequences* as in [11], and the meaning of a cedent Γ is $\bigvee \Gamma$. We often abuse notation by writing Γ, φ or $\Gamma \vee \varphi$ instead of $\Gamma \cup \{\varphi\}$, or by writing $\varphi_1, \ldots, \varphi_k$ instead of $\{\varphi_1, \ldots, \varphi_k\}$.

Our version of LK does not have structural rules as special inferences, they will be available as derivable rules. LK consists of four inference rules: initial cedent rule, introduction rules for $\bigwedge$ and $\bigvee$, and a cut-rule.

Definition 1. *We inductively define that Γ is $\mathcal{C}$-LK provable with height η, in symbols $\vdash_{\mathcal{C}}^{\eta} \Gamma$, for Γ a cedent, $\mathcal{C}$ a set of formulas and $\eta \in \mathbb{N}$. $\vdash_{\mathcal{C}}^{\eta} \Gamma$ holds iff*

(Init) *$\eta \geq 0$ and Γ is an initial cedent, i.e. $1 \in \Gamma$, or $x, \neg x \in \Gamma$ for some variable x.*

($\bigwedge$) *There are some $\bigwedge_{i<I} \varphi_i \in \Gamma$, $\eta' < \eta$ such that $\vdash_{\mathcal{C}}^{\eta'} \Gamma, \varphi_i$ for all $i < I$.*

($\bigvee$) *There are some $\bigvee_{i<I} \varphi_i \in \Gamma$, $i_0 < I$ and $\eta' < \eta$ such that $\vdash_{\mathcal{C}}^{\eta'} \Gamma, \varphi_{i_0}$.*

(Cut) *There are some $\varphi \in \mathcal{C}$ and $\eta' < \eta$ such that $\vdash_{\mathcal{C}}^{\eta'} \Gamma, \varphi$ and $\vdash_{\mathcal{C}}^{\eta'} \Gamma, \neg\varphi$.*

We say that Γ is cut-free-LK provable with height η iff $\vdash_{\emptyset}^{\eta} \Gamma$.

In order to make our definition of Σ_d-LK precise we have to define a fine structure on constant depth formulas.

Definition 2. *Let S, t, d be in $\mathbb{N}$. $\Sigma_d^{S,t}$ is the set of all formulas φ with*

i) $\mathrm{dp}(\varphi) \leq d + 1$;

ii) if $\mathrm{dp}(\varphi) = d + 1$, *then the outermost connective of φ is $\bigvee$;*

iii) all depth > 1 sub-formulas of φ have the arity of their outermost connective bounded by S; and *iv) all depth* 1 *sub-formulas of* φ *have the arity of their outermost connective bounded by* t.

A formula is in $\Pi^{S,t}_d$ *iff its negation is in* $\Sigma^{S,t}_d$.

Now we are prepared to say what we mean by Σ_d-LK.

Definition 3. *Let* $d \in \mathbb{N}$, $f, \eta : \mathbb{N} \to \mathbb{N}$ *be functions, and* $(\Gamma_n)_n$ *be a sequence of tautological cedents.*

We say that $(\Gamma_n)_n$ *is* (d, f)-LK *(or* (Σ_d, f)-LK*) provable with height* η *iff there is a sequence of subsets* $\mathcal{C}_n \subseteq \Sigma_d^{2^{f(n)},f(n)}$ *of cardinality bounded by* $2^{f(n)}$ *such that eventually* Γ_n *is* $\mathcal{C}_n$-LK *provable of height* $\eta(n)$.

Then Σ_d-LK *denotes* $(\Sigma_d, (\log n)^{O(1)})$-LK, *i.e.* $(\Gamma_n)_n$ *is* Σ_d-LK *provable with height* η *iff there is a* $c \in \mathbb{N}$ *such that* $(\Gamma_n)_n$ *is* $(d, (\log n)^c)$-LK *provable with height* η.

We will often abuse notation and write Γ_n is Σ_d-LK provable with height $\eta(n)$ instead of $(\Gamma_n)_n$ is Σ_d-LK provable with height η.

Structural rules are not included in the definition of LK. They are obtained as derivable rules which is stated in the next proposition. It is readily proven by induction on η.

Proposition 4 (Structural Rule). *Assume* $\eta \le \eta'$, $\mathcal{C} \subseteq \mathcal{C}'$ *and* $\Gamma \subseteq \Gamma'$, *then* $\vert\!\frac{\eta}{\mathcal{C}}\, \Gamma$ *implies* $\vert\!\frac{\eta'}{\mathcal{C}'}\, \Gamma'$.

The following propositions on $(\bigwedge)$-Inversion and $(\bigvee)$-Exportation are proven by induction on η.

Proposition 5 **($(\bigwedge)$-Inversion).** *Assume* $\vert\!\frac{\eta}{\mathcal{C}}\, \Gamma, \bigwedge_{i<I} \varphi_i$, *then* $\vert\!\frac{\eta}{\mathcal{C}}\, \Gamma, \varphi_i$ *holds for all* $i < I$.

Proposition 6 **($(\bigvee)$-Exportation).** *Suppose* $\vert\!\frac{\eta}{\mathcal{C}}\, \Gamma, \bigvee_{i<I} \varphi_i$ *holds, then* $\vert\!\frac{\eta}{\mathcal{C}}\, \Gamma, \varphi_0, \ldots, \varphi_{I-1}$.

The proof of the next Lemma and Proposition follows the standard one which can be found e.g. in [2, 3].

Lemma 7 (Cut-Elimination Lemma). *Let* $\varphi \in \Sigma^{S,t}_{d+1}$ *and* $\mathcal{C} \subseteq \Sigma^{S,t}_d$ *such that* $\mathcal{C}$ *includes all* $\Sigma^{S,t}_d$*-sub-formulas and all negations of* $\Pi^{S,t}_d$*-sub-formulas of* φ. *If* $\vert\!\frac{\eta_0}{\mathcal{C}}\, \Gamma, \varphi$ *and* $\vert\!\frac{\eta_1}{\mathcal{C}}\, \Delta, \neg\varphi$, *then* $\vert\!\frac{\eta_0+\eta_1}{\mathcal{C}}\, \Gamma, \Delta$.

Proposition 8 (Cut-Elimination Theorem). *Let* $\mathcal{C} \subseteq \Sigma^{S,t}_{d+1}$ *be closed under sub-formulas and let* $\mathcal{C}' := \mathcal{C} \cap (\Sigma^{S,t}_d \cup \Pi^{S,t}_d)$. *Then* $\vert\!\frac{\eta}{\mathcal{C}}\, \Gamma$ *implies* $\vert\!\frac{2^\eta}{\mathcal{C}'}\, \Gamma$.

We repeat the translation (also called embedding) of provability in $\mathrm{S}^d_2(\alpha)$, $\mathrm{T}^d_2(\alpha)$, and more general of $\Sigma^b_d(\alpha)$-L^{m+1}IND , to LK from [2, 3]. We do not introduce language and theories of bounded arithmetic. All what we need from bounded arithmetic is that formulas translate in a certain way to the language of LK as described below, and that provability translates in the way described by the next theorem. Readers not familiar with bounded arithmetic simply can view these connections to bounded arithmetic as a motivation for studying the resulting propositional proof systems. For more background on bounded arithmetic see [5, 12]

There exists a canonical translation due to PARIS and WILKIE [15] from the language of bounded arithmetic to the language of LK (see [12, 9.1.1], or [2, 3]). Let φ be a formula in the language of bounded arithmetic in which no individual (i.e. first order) variable occurs free – we call such a formula (first order) closed. Then $[\![\varphi]\!]$ denotes the translation of φ to the language of LK, which for example maps the atom $\alpha(t)$, for t a closed term of value $m_t \in \mathbb{N}$, to the propositional variable p_{m_t}, and bounded quantifiers to connectives $\bigwedge$ resp. $\bigvee$, e.g. $[\![(\forall x \leq t)\varphi(x)]\!] = \bigwedge_{i \leq m_t} [\![\varphi(i)]\!]$. It follows that a formula $\varphi(x)$ from Σ^b_d (with x being the only variable occurring free in φ) translates to $\left([\![\varphi(n)]\!]\right)_n$ in $\Sigma_d^{\text{quasipoly}}$, i.e. in $\Sigma_d^{2^{(\log n)^c},(\log n)^c}$ for some $c \in \mathbb{N}$.

Let $\log^{(k)}(n)$ be the k-times iterated logarithm applied to n, and $2_k(n)$ the k-times iterated exponentiation applied to n.

Theorem 9 ([2, 3]). *Let $\varphi(x)$ be a formula in the language of bounded arithmetic, in which at most the variable x occurs free.*

i) If $\mathrm{S}^d_2(\alpha) \vdash \varphi(x)$, then $[\![\varphi(n)]\!]$ is Σ_d-LK provable with height $O\left(\log^{(2)} n\right)$.

ii) If $\mathrm{T}^d_2(\alpha) \vdash \varphi(x)$, then $[\![\varphi(n)]\!]$ is Σ_d-LK provable with height $(\log n)^{O(1)}$.

iii) If $\Sigma^b_d(\alpha)$-$\mathrm{L}^m\mathrm{IND} \vdash \varphi(x)$, then $[\![\varphi(n)]\!]$ is Σ_d-LK provable with height $O\left(\log^{(m+1)} n\right)$. □

Combining this Theorem with the Cut-Elimination Theorem we obtain

Corollary 10 ([2, 3]). *Let $\varphi(x)$ be a formula in the language of bounded arithmetic, in which at most the variable x occurs free.*

i) If $\mathrm{T}^d_2(\alpha) \vdash \varphi(x)$ or $\mathrm{S}^{d+1}_2(\alpha) \vdash \varphi(x)$, then $[\![\varphi(n)]\!]$ is Σ_d-LK provable with height $(\log n)^{O(1)}$. In this case we say that $[\![\varphi(n)]\!]$ is polylogarithmic-height restricted Σ_d-LK *provable.*

ii) If $\Sigma^b_{m+d+1}(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND} \vdash \varphi(x)$, then $[\![\varphi(n)]\!]$ is Σ_d-LK provable with height $2_m\left((\log^{(m+1)} n)^{O(1)}\right)$. In this case we say that $[\![\varphi(n)]\!]$ is $2_m\left((\log^{(m+1)} n)^{O(1)}\right)$-height restricted Σ_d-LK *provable.* □

3 Cut-reduction by switching

Usual cut-elimination procedures (like GENTZEN or TAIT style cut-elimination) eliminate outermost connectives of cut-formulas first. In general, the cost of applying such cut-elimination techniques is an exponential blow-up of certain parameters of derivations like their height, as seen in the previous section. Later we want to show that the order induction principle needs a certain height of LK-proofs. Our lower bounds technique will only work if the heights of the proofs grow sub-linear. Thus, in order to reduce the degree of cut formulas in the derivations in Corollary 10 we cannot apply the Cut-Elimination-Theorem any further – this would result in upper bounds on heights of at least quasi-polynomial growth.

At this point, the reduction of cuts, which is necessary in our proof of lower bounds, needs a different cut-reduction technique which we will call cut-reduction by switching. It relies on methods from boolean complexity called HÅSTAD's Switching Lemmas. Cut-reduction by switching will reduce cuts "inside-out", but will leave the proof-skeleton unchanged, e.g. the heights will remain the same. The price will be that not only the cut-formulas are reduced, but also the formula which is derived. The idea is to find a so-called restriction (i.e. a partial substitution of propositional variables by truth values) for a given derivation of a formula φ such that after applying that restriction to the proof cut-formulas are sufficiently reduced but the restriction of φ is sufficiently meaningful.

We will follow [7] where such boolean complexity techniques are successfully applied to reduce the complexity of oracle computations related to definable functions in bounded arithmetic. In [11] the same approach is used to reduce the complexity of Σ_d-LK refutations.

In order to formulate our Cut-Elimination-by-Switching-Theorem, we need some notation. Our logarithms are always base 2.

(1) Fix $m \geq 1$, $d \geq 0$. Let $[m]$ denote the set $\{0, \dots, m-1\}$. For $x, y_1, \dots, y_d \in \mathbb{N}$ let $p_{x,y_1,\dots,y_d}$ be a BOOLEAN variable, and let

$$B_d(m) = \{p_{x,y_1,\dots,y_d} \ : \ x, y_1, \dots, y_d < m\} \ .$$

The cardinality of $B_d(m)$ is m^{d+1}. We shall henceforth use $\vec{y}$ as an abbreviation of $y_1, \dots, y_d$ or $y_1, \dots, y_{d-1}$, depending on the context it occurs. Note that $B_0(m)$ is the set of variables p_x with $x < m$.

(2) A propositional formula is Σ_1^t iff it is a disjunction of conjunctions of at most t literals, i.e. if it is in $\Sigma_1^{S,t}$ for some S. A propositional formula is Π_1^t iff its negation is Σ_1^t, and it is Δ_1^t iff it is equivalent to both Σ_1^t and Π_1^t. A formula φ is *hereditarily* Δ_1^t, denoted by $\varphi \in \mathbb{\Delta}_1^t$ iff every sub-formula of φ is Δ_1^t. We inductively define for $d \geq 0$:

$$\varphi \in \mathbb{\Pi}_d^{S,t} \Leftrightarrow \neg\varphi \in \Sigma_d^{S,t}$$

$$\varphi \in \Sigma_0^{S,t} \Leftrightarrow \varphi \in \mathbb{\Delta}_1^t$$

$$\varphi \in \Sigma_1^{S,t} \Leftrightarrow \varphi \equiv \bigvee_{i<w} \varphi_i \text{ and } \varphi_i \in \mathbb{\Delta}_1^t \text{ for all } i < w$$

$$\varphi \in \Sigma_{d+2}^{S,t} \Leftrightarrow \varphi \equiv \bigvee_{i<w} \varphi_i \text{ and } w \leq S \text{ and } \varphi_i \in \mathbb{\Pi}_{d+1}^{S,t} \text{ for all } i < w$$

Observe that in case $\Sigma_1^{S,t}$ we do *not* assume $w \leq S$!

(3) We define for $x < m$ some general $\Sigma_d^{m,1}$-formulas $D_{d,m}(x)$ in m^d variables from $B_d(m)$. They compute SIPSER functions and are defined by

$$D_{d,m}(x) \quad = \quad \bigwedge_{y_1<m} \quad \bigvee_{y_2<m} \quad \cdots \quad \underset{y_{d-1}<m}{Q^{d-1}} \quad \underset{y_d<m}{Q^d} \quad p_{x,\vec{y}}$$

where either Q^{d-1} or Q^d is $\bigwedge$, depending on whether d is even or odd, respectively, and the other is $\bigvee$.

(4) We are now ready to formulate cut-reduction by switching. The notation $B[p_x \leftarrow \varphi_x \,:\, x \in M]$ denotes the result of simultaneously replacing variable p_x by formula φ_x for all $x \in M$.

Theorem 11 (Cut-Elimination by Switching). *Let $d \in \mathbb{N}$ and $\epsilon \in \mathbb{R}$ with $d \geq 1$ and $0 < \epsilon < \frac{1}{2}$. Let $M \subseteq \mathbb{N}$ be some infinite set. For $m \in M$, let $\eta_m \in \mathbb{N}$, $t = t(m) = m^{\frac{1}{2}-\epsilon}$, $S = S(m) = 2^t$, B_m a formula with variables in $B_0(m)$, and $\mathcal{C}_m \subset \Sigma_d^{S,t}$ with $|\mathcal{C}_m| \leq S$. Furthermore, assume that $B_m\big[p_x \leftarrow D_{d,m}(x) \,:\, x < m\big]$ is $\mathcal{C}_m$-*LK *provable with height η_m.*

Then, for all $m \in M$ which are sufficiently large, there is some $Q \subset [m]$ such that

i) $|[m] \setminus Q| \geq \sqrt{m \cdot \log m}$;

ii) $B_m\big[p_x \leftarrow 0 \,:\, x \in Q\big]$ *is* Δ_1^t-LK *provable with height* η_m.

We now sketch the proof of this Theorem. We go on introducing notations.

(5) Let $d, m \geq 1$. We have already defined sets $B_d(m)$ of propositional variables. They are partitioned into blocks via

$$(B_d(m))_{(x,y_1,\ldots,y_{d-1})} \quad := \quad \{p_{x,y_1,\ldots,y_{d-1},z} \,:\, z < m\}$$

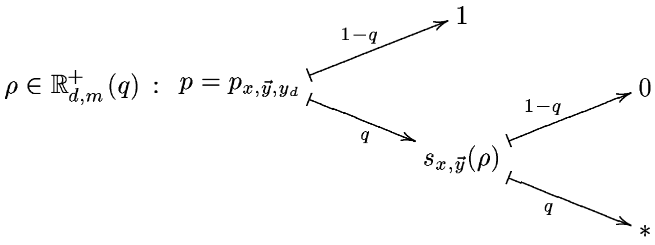
for $(x, y_1, \ldots, y_{d-1}) \in [m]^d$.

(6) A restriction ρ on $B_d(m)$ is a map going from $B_d(m)$ to $\{0, 1, *\}$:

$$\rho \,:\, B_d(m) \;\to\; \{0, 1, *\} \; .$$

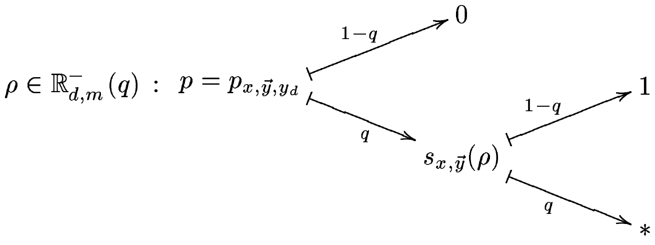
We should think of $\rho(p) = 0$ or $\rho(p) = 1$ as *p is replaced by* 0 or 1 respectively, and of $\rho(p) = *$ as *p is left unchanged.* Alternatively, we can think of ρ as a partial map going from $B_d(m)$ to $\{0, 1\}$.

(7) The probability space $\mathbb{R}_{d,m}^{+}(q)$ of restrictions ρ for $0 < q < 1$ is given as follows. Let $x < m$, $\vec{y} \in [m]^{d-1}$ and $y_d < m$.



Meaning: first choose $s_{x,\vec{y}}$ such that $s_{x,\vec{y}} = *$ with probability q and $s_{x,\vec{y}} = 0$ with probability $1-q$; then choose $\rho(p)$ such that $\rho(p) = s_{x,\vec{y}}$ with probability q and $\rho(p) = 1$ with probability $1-q$.

Define $\mathbb{R}^-_{d,m}(q)$ by interchanging 0 and 1:



(8) Let $\rho \in \mathbb{R}^+_{d,m}(q)$. We define a transformation $\lceil_{\mathrm{g}\rho}$ which maps formulas with variables in $B_d(m)$ to formulas with variables in $B_{d-1}(m)$:

i) Apply ρ.

ii) Assign 1 to every $p_{x,\vec{y},z}$ with $\rho(p_{x,\vec{y},z}) = *$ such that there is some $z < z' < m$ with $\rho(p_{x,\vec{y},z'}) = *$. I.e., all but one variable in a block are touched.

iii) Rename each $p_{x,\vec{y},z}$ by $p_{x,\vec{y}}$.

For $\rho \in \mathbb{R}^-_{d,m}(q)$ replace 1 by 0.

(9) The following lemma is HÅSTAD's second switching lemma, see [9].

Lemma 12 **(HÅSTAD [9]).** *Let $d, i \geq 1$ and $\nu \in \{+,-\}$. Let φ be a $\Sigma^{S,t}_{i+1}$-formula with variables from $B_d(m)$ and $0 < q < 1$. Then*

$$\mathrm{Pr}_{\rho \in \mathbb{R}^{\nu}_{d,m}(q)} \left[\varphi\lceil_{\mathrm{g}\rho} \notin \Sigma^{S,t}_i\right] \leq S^i \cdot (6qt)^t \ .$$

I.e., the probability of a randomly chosen ρ from $\mathbb{R}^{\nu}_{d,m}(q)$ that the formula $\varphi\lceil_{\mathrm{g}\rho}$ is not equivalent to some $\Sigma^{S,t}_i$-formula is at most $S^i \cdot (6qt)^t$.

(10) For the following inductive proof, the previously defined SIPSER functions $D_{d,m}(x)$ have to be modified. We define $\bar{D}_{d,m}(x)$ for every $x < m$ with

variables from $B_d(m)$. They compute modified SIPSER functions (cf. [9, 7]) and are defined by

$$\bar{D}_{d,m}(x) \quad = \quad \bigwedge_{y_1<m} \quad \bigvee_{y_2<m} \quad \cdots \quad \underset{y_{d-1}<m}{Q^{d-1}} \quad \underset{y_d<\sqrt{\frac{1}{2}\,(d+1)\,m\log m}}{Q^{d}} \quad p_{x,\bar{y}}$$

where either Q^{d-1} or Q^d is $\bigwedge$, depending on whether d is even or odd, respectively, and the other is $\bigvee$. Our logarithms are always base 2. Note that for distinct x, the formulas $\bar{D}_{d,m}(x)$ contain distinct propositional variables.

(11) The next lemma is also due to HÅSTAD [9]. We repeat essentially the version stated by BUSS and KRAJÍČEK [7].

We say that a formula φ contains formula ψ, written as $\psi \subseteq \varphi$, if by renaming and/or erasing some variables we can transform φ into ψ.

Lemma 13. *Let m be big (i.e. $m \geq 10^{30}$), $d \geq 1$, $\overline{m} := \sqrt{\frac{1}{2}(d+1)\,m\,\log m}$, $q := \sqrt{\frac{2\,(d+1)\,\log m}{m}}$ and assume $q \leq \frac{1}{5}$. Then the following holds:*

i) Assume $d \geq 2$ and let $v(d) = +$ or $v(d) = -$ if d is odd or even respectively. For all $x < m$:

$$\Pr_{\rho\in\mathbb{R}^{\nu(d)}_{d,m}(q)}\left[\bar{D}_{d-1,m}(x) \not\subseteq \bar{D}_{d,m}(x)\restriction_{g\rho}\right] \leq \frac{1}{3}m^{-2} \quad .$$

I.e., the probability of a randomly chosen ρ from $\mathbb{R}^{\nu(d)}_{d,m}(q)$ that the formula $\bar{D}_{d,m}(x)\restriction_{g\rho}$ does not contain $\bar{D}_{d-1,m}(x)$ is at most $\frac{1}{3}m^{-2}$.

ii) For $d = 1$ we have for all $x < m$:

$$\Pr_{\rho\in\mathbb{R}^{+}_{1,m}(q)}\left[\bar{D}_{1,m}(x)\restriction_{g\rho} = 1\right] \leq \frac{1}{6}m^{-2} \quad .$$

I.e., the probability of a randomly chosen ρ from $\mathbb{R}^{+}_{1,m}(q)$ that the formula $\bar{D}_{1,m}(x)$ is transformed to 1 by $\restriction_{g\rho}$ is at most $\frac{1}{6}m^{-2}$.
For $R \subseteq [m]$ with $|R| \geq m$ we have

$$\Pr_{\rho\in\mathbb{R}^{+}_{1,m}(q)}\left[|\{x \in R \,:\, s_x(\rho) = *\}| \geq \frac{1}{2}q \cdot |R|\right] \geq 1 - \frac{1}{6}m^{-2} \quad .$$

I.e., the probability of a randomly chosen ρ from $\mathbb{R}^{+}_{1,m}(q)$ that for at least an $\frac{1}{2}q$-fraction of R the corresponding variables p_x are left unchanged by ρ (i.e. are assigned $*$) is at least $1 - \frac{1}{6}m^{-2}$.

(12) Utilizing this we obtain the following lemmas which immediately proof our Cut-Elimination-by-Switching-Theorem 11. For the rest of this appendix fix $\epsilon \in \mathbb{R}$ with $0 < \epsilon < \frac{1}{2}$. Fix some infinite set $M \subseteq \mathbb{N}$. For $m \in M$, let $t = t(m) = m^{\frac{1}{2}-\epsilon}$, $S = S(m) = 2^t$, and B_m a formula with variables in $B_0(m)$. For a set $\mathcal{C}$ of formulas let $(\star)^m_d(\mathcal{C})$ denote that $\mathcal{C} \subset \Sigma^{S,t}_d$ and $|\mathcal{C}| \leq S$.

Lemma 14. *Let $d \geq 1$, $f : \mathbb{N} \to \mathbb{N}$ some function and $\mathcal{C}_m$ be given such that $(\star)^m_{d+1}(\mathcal{C}_m)$ and $B_m\big[p_x \leftarrow \bar{D}_{d+1,m}(x) \ : \ x < m\big]$ is $\mathcal{C}_m$-*LK *provable with height $f(m)$ for all $m \in M$.*

*Then, for $m \in M$ sufficiently large, there is some $\mathcal{C}'_m$ such that $(\star)^m_d(\mathcal{C}'_m)$ and $B_m\big[p_x \leftarrow \bar{D}_{d,m}(x) \ : \ x < m\big]$ is $\mathcal{C}'_m$-*LK *provable with height $f(m)$.*

Lemma 15. *Let $f : \mathbb{N} \to \mathbb{N}$ be some function and $\mathcal{C}_m$ be given such that $(\star)^m_1(\mathcal{C}_m)$ and $B_m\big[p_x \leftarrow \bar{D}_{1,m}(x) \ : \ x < m\big]$ is $\mathcal{C}_m$-*LK *provable with height $f(m)$ for all $m \in M$.*

Then, for $m \in M$ sufficiently large, there is some $Q = Q_m \subseteq [m]$ such that

i) $|[m] \setminus Q| \geq \sqrt{m \cdot \log m}$ *;*

ii) $B_m\big[p_x \leftarrow 0 \ : \ x \in Q\big]$ *is* Δ^t_1-LK *provable with height $f(m)$.*

4 The height complexity of order induction

In this section we will characterize the *height complexity* of order induction. For a sequence $(\tau_n)_n$ of tautologies we define its *d-th height complexity* $\mathrm{hc}_d((\tau_n)_n)$, also written as $\mathrm{hc}_d(\tau_n)$, to be the function which maps n to the minimal η such that τ_n is Σ_d-LK provable with height η. In the following we will characterize the d-th height complexity of the order induction principle for some particular Σ_d-property (given by the SIPSER functions $D_{d,m}(x)$).

The principle $\mathcal{O}\mathrm{Ind}(m)$ of order induction for m is given by

$$\mathcal{O}\mathrm{Ind}(m) \quad := \quad \bigwedge_{x<m} \Big(\Big(\bigwedge_{y<x} p_y \Big) \to p_x \Big) \to \bigwedge_{x<m} p_x$$

(of course $A \to B$ is an abbreviation of $\bigvee\{\neg A, B\}$). The meaning is easily understood if we consider its contraposition which expresses minimization: if some variables among $p_0, \ldots, p_{m-1}$ are false then there is a false one with minimal index. We extend the complexity of $\mathcal{O}\mathrm{Ind}(m)$ by replacing variables p_x by the SIPSER function $D_{d,m}(x)$ from the previous section:

$$\mathcal{O}\mathrm{Ind}^d(m) \quad := \quad \mathcal{O}\mathrm{Ind}(m)\big[p_x \leftarrow \neg D_{d,m}(x) \ : \ x < m\big] \ .$$

Observe that m in $\mathcal{O}\mathrm{Ind}^d(m)$ also controls the width of the SIPSER functions. In the following we will determine the d-th height complexity of $\mathcal{O}\mathrm{Ind}^d(f(n))$ for functions $f : \mathbb{N} \to \mathbb{N}$ which grow super-polylogarithmically, i.e. $f(n) = (\log n)^{\omega(1)}$. This is satisfied for example for $f(n) = 2_i((\log^{(i+1)} n)^2)$ for $i \geq 1$.

It is easy to show that $\mathcal{O}\mathrm{Ind}^d(m)$ is cut-free-LK provable with height $O(m)$. E.g., use induction on k to show that

$$\neg \bigwedge_{i<m} \Big(\bigwedge_{j<i} p_j \to p_i \Big), \bigwedge_{i<m} p_i, \{\neg p_i : i < k\}$$

is cut-free-LK provable with height $H(k)$ for $k = m, \ldots, 0$, with $H(k) := 3(m + 1 - k)$. Furthermore, $\neg\varphi, \varphi$ is cut-free-LK provable with height $2i$ for every φ

of depth i. Thus, $\mathcal{O}\mathrm{Ind}(f(n))\big[p_x \leftarrow \varphi_x^n \,:\, x < f(n)\big]$ is cut-free-LK provable of height $O(f(n))$, for any function $f : \mathbb{N} \to \mathbb{N}$ and any sequence of constant depth formulas φ_x^n for $x < f(n)$ and $n \in \mathbb{N}$. Hence for any fixed $d, i \in \mathbb{N}$ we obtain

$$\mathrm{hc}_d\left(\mathcal{O}\mathrm{Ind}^i(f(n))\right) \quad = \quad O(f(n)) \ .$$

The next theorem states the lower bound for Δ_1^t-LK derivations of the order induction principle. It is sometimes called “Boundedness Theorem”.

Theorem 16 (Boundedness). *If $\mathcal{O}\mathrm{Ind}(m)$ is Δ_1^t-LK provable with height η, then $m \le \eta \cdot t$.*

We will give a detailed proof of this Theorem in the next subsection. But before we do this we combine the Boundedness Theorem with Cut-Elimination by Switching to obtain a lower bound on the height complexity of order induction. With $\mathrm{rng}(f)$ we will denote the range of a function f.

Theorem 17. *Let $d \in \mathbb{N}$ with $d \ge 1$. Let f be some number-theoretic function which grows super-polylogarithmically, i.e. $f(n) = (\log n)^{\omega(1)}$. Then, the d-th height complexity of $(\mathcal{O}\mathrm{Ind}^d(f(n)))_n$ has lower bound $f(n)^{\Omega(1)}$:*

$$\mathrm{hc}_d(\mathcal{O}\mathrm{Ind}^d(f(n))) = f(n)^{\Omega(1)} \ .$$

Proof. Let $\eta(n) := \mathrm{hc}_d(\mathcal{O}\mathrm{Ind}^d(f(n)))$. Assume for the sake of contradiction that the assumptions of the Theorem are satisfied, but $\eta(n) \neq f(n)^{\Omega(1)}$, or, equivalently, $f(n) \neq \eta(n)^{O(1)}$. By definition, there is $c \in \mathbb{N}$ with $c \ge 1$ such that for $n \in \mathbb{N}$ there is $\mathcal{C}_n \subseteq \Sigma_d^{S,t}$ with $|\mathcal{C}_n| \le S$ letting $t = t(n) = (\log n)^c$, $S = S(n) = 2^t$, such that $\mathcal{O}\mathrm{Ind}^d(f(n))$ is $\mathcal{C}_n$-LK provable with height $\eta(n)$. Furthermore, by assumption, $\mathrm{rng}(f)$ must be unbounded, and, as $f(n) = (\log n)^{\omega(1)}$, there is some $N_0 \in \mathbb{N}$ such that $f(n) \ge (\log n)^{4c}$ for all $n > N_0$.

We will construct some infinite subset M of $\mathrm{rng}(f)$ which can be used to apply Cut-Elimination by Switching. To this end let m_0 be given. We will construct some $m_1 \ge m_0$ which we will put into the set M. Fix some $n_0 \ge N_0$ with $(\log n_0)^{4c} \ge m_0$. As $f(n) \neq \eta(n)^{O(1)}$ there must be some $n_1 > n_0$ satisfying $f(n_1) > \eta(n_1)^4$. Let $m_1 := f(n_1)$. Then $(\log n_1)^c \le m_1^{\frac{1}{4}}$ and $m_1 \ge m_0$. Hence $\mathcal{C}_{n_1} \subseteq \Sigma_d^{\bar S,\bar t}$ and $|\mathcal{C}_{n_1}| \le \bar S$ for $\bar t := m_1^{\frac{1}{4}}$ and $\bar S := 2^{\bar t}$. Put m_1 into the set M and define $\bar{\mathcal{C}}_{m_1} := \mathcal{C}_{n_1}$ and $\eta_{m_1} := \eta(n_1)$.

Then, the prerequisites of the Cut-Elimination by Switching Theorem are satisfied, and we obtain some large $m \in M$, some set $Q \subset [m]$ not too big (i.e. $|[m] \setminus Q| \ge \sqrt{m \cdot \log m} \ge \sqrt{m}$) and a $\Delta_1^{\bar t}$-LK derivation of

$$\mathcal{O}\mathrm{Ind}(m)[p_x \leftarrow 1 \,:\, x \in Q]$$

of height η_m. By pruning and renaming of variables this derivation can be transformed into a $\Delta_1^{\bar t}$-LK derivation of $\mathcal{O}\mathrm{Ind}(m - |Q|)$ of height η_m, hence the Boundedness Theorem yields $m - |Q| \le \eta_m \cdot \bar t = \eta_m \cdot m^{\frac{1}{4}}$, which together with the largeness condition on Q rewrites to $\eta_m \ge m^{\frac{1}{4}}$. By construction of M there is some n such that $\eta(n) = \eta_m$ and $m = f(n) > \eta(n)^4$, contradicting the previously obtained $m \le \eta(n)^4$. □

$$\begin{tikzcd}
\mathrm{S}_2^d(\alpha) \arrow[r, hook] \arrow[d, phantom, "\not\cap"] & \text{polylogarithmic-height } \Sigma_d\text{-LK} \arrow[d, phantom, "\not\cap"] \\
\mathrm{sR}_2^{d+1}(\alpha) \arrow[r, hook] \arrow[d, phantom, "\not\cap"] & 2^{(\log\log n)^{O(1)}}\text{-height } \Sigma_d\text{-LK} \arrow[d, phantom, "\not\cap"] \\
s\Sigma_{d+2}^b(\alpha)\text{-L}^3\text{IND} \arrow[r, hook] \arrow[d, phantom, "\not\cap"] & 2_2\left((\log^{(3)} n)^{O(1)}\right)\text{-height } \Sigma_d\text{-LK} \arrow[d, phantom, "\not\cap"] \\
\vdots & \vdots
\end{tikzcd}$$

Figure 2: Separation of $\Sigma_{d+m}^b(\alpha)$-L^{m+1}IND and corresponding Σ_d-LK proof systems

Together with the previously obtained upper bound this shows

Corollary 18. *For functions $f : \mathbb{N} \to \mathbb{N}$ with $f(n) = (\log n)^{\omega(1)}$ we have*

$$\mathrm{hc}_d\left(\mathcal{O}\mathrm{Ind}^d(f(n))\right) \quad = \quad f(n)^{\Theta(1)} \ . \qquad \Box$$

Having characterized the height complexity of order induction, the separation of bounded arithmetic theories follows straight forwardly. We define a general $\Pi_d^b(\alpha)$-formula $A^{\alpha,d}(a,x)$ in the language of bounded arithmetic by

$$(\forall y_1 < a)\ (\exists y_2 < a) \ldots\ (Q^{d-1} y_{d-1} < a)\ (Q^d y_d < a)\ \alpha(\langle x, y_1, \ldots, y_d\rangle)$$

where either Q^{d-1} or Q^d is $\forall$, depending on whether d is even or odd, respectively, and the other is $\exists$. It is quiet easy to see that for any term $t(x)$ the formula $\mathcal{O}\mathrm{Ind}(t, \neg A^{\alpha,d}(t,.))$ is provable in $\mathrm{T}_2^{d+1}(\alpha)$ and translates to LK as $\mathcal{O}\mathrm{Ind}^d(t(n))$. Now, the d-th height complexity of $\mathcal{O}\mathrm{Ind}^d(t(n))$ is $t(n)^{\Omega(1)}$ by Corollary 18, hence $\mathcal{O}\mathrm{Ind}(t, \neg A^{\alpha,d}(t,.))$ cannot be provable in $\mathrm{S}_2^{d+1}(\alpha)$ because translating this (Corollary 10) would yield polylogarithmic upper bounds to the d-th height complexity of $\mathcal{O}\mathrm{Ind}^d(t(n))$ which is impossible for e.g. $t(n) = n$.

Similarly, we obtain for $d \geq 0$ and $m \geq 1$ a separation of $\Sigma_{d+m}^b(\alpha)$-L^{m}IND from $\Sigma_{d+m+1}^b(\alpha)$-L^{m+1}IND because the latter can prove $\mathcal{O}\mathrm{Ind}^d(t(n))$ for $t(n) = 2_m\left((\log^{(m+1)} n)^2\right)$ which again has its d-th height complexity bounded by $t(n)^{\Omega(1)}$, but provability in $\Sigma_{d+m}^b(\alpha)$-L^{m+1}IND would result in a weaker upper bound of $t(n)$ of the form $2_{m-1}\left((\log^{(m)} n)^{O(1)}\right)$.

4.1 The proof of the Boundedness Theorem

For this subsection we fix $t \in \mathbb{N}$, $t \geq 1$. By $\overset{\eta}{\models} \varphi$ we denote that φ is Δ_1^t-LK provable with height η. A formula φ will always be one from LK. We want to prove the Boundedness Theorem, i.e.

$$\overset{\eta}{\models} \mathcal{O}\mathrm{Ind}(n) \quad \Rightarrow \quad n \leq \eta \cdot t \ .$$

Before we can do this we first have to fix some suitable notations.

Let φ be an LK-formula. For a set $M \subseteq \mathbb{N}$ we define $\varphi[M]$ to be the result of replacing p_i by 1 if $i \in M$, and by 0 if $i \notin M$. Then let $M \vDash \varphi$ iff $\varphi[M]$ is true.

For two sets $M^+, M^- \subseteq \mathbb{N}$ we define $[M^+, M^-]$ to be the set of all subsets M of $\mathbb{N}$ that contain M^+ but are disjoint from M^-:

$$[M^+, M^-] \quad := \quad \{M : M^+ \subseteq M \subseteq \mathbb{N} \setminus M^-\} \ .$$

Definition 19. *For a formula φ and a truth value $\nu \in \{0,1\}$ we define that (M^+, M^-) fixes φ to ν iff M^+ and M^- are disjoint subsets of $\mathbb{N}$ (this implies $[M^+, M^-] \neq \emptyset$) and the truth of φ is fixed on $[M^+, M^-]$ to ν, i.e. $\varphi[M] = \nu$ for all $M \in [M^+, M^-]$. We say that (M^+, M^-) fixes φ iff (M^+, M^-) fixes φ to some truth value $\nu \in \{0,1\}$.*

A true Δ_1^t-formula φ can always be fixed to 1 by a pair M^+, M^- which is small, i.e. the cardinality of M^+ and M^- together is bounded by t, denoted by $|M^+| + |M^-| \leq t$. In addition, M^+, M^- will respect any satisfying assignment of φ:

Lemma 20. *Let $\varphi \in \Delta_1^t$ and $M_0 \subseteq \mathbb{N}$ such that $M_0 \vDash \varphi$. Then there are $M^+ \subseteq M_0$ and $M^- \subseteq \mathbb{N}$ satisfying $|M^+| + |M^-| \leq t$, $M_0 \cap M^- = \emptyset$ and (M^+, M^-) fixes φ to 1.*

Proof. The assumption $\varphi \in \Delta_1^t$ particularly implies $\varphi \in \Delta_1^t$. Hence, φ is equivalent to some $\bigvee_{x<S} \bigwedge_{y<t} \theta_{xy}$ for some S and some literals θ_{xy}. From the assumption $M_0 \vDash \varphi$ it follows that there is some $x_0 < S$ such that $M_0 \vDash \bigwedge_{y<t} \theta_{x_0 y}$. Fix such an $x_0 < S$. Let

$$\begin{aligned} M^+ &:= \{i : \theta_{x_0 y} = p_i \text{ for some } y < t\} \\ M^- &:= \{i : \theta_{x_0 y} = \neg p_i \text{ for some } y < t\} \ . \end{aligned}$$

Then the assertion follows. □

The following Lemma is the main technical part for proving the Boundedness Theorem 16. Let

$$\mathcal{O}\mathrm{Prog}(m) \quad := \quad \bigwedge_{x<m} \Big(\big(\bigwedge_{y<x} p_y \big) \to p_x \Big)$$

hence $\mathcal{O}\mathrm{Ind}(m)$ has the form $\neg\, \mathcal{O}\mathrm{Prog}(m) \vee \bigwedge_{x<m} p_x$.

Lemma 21. $\overset{\eta}{\mid\!\!\!\cdot}\ \neg\, \mathcal{O}\mathrm{Prog}(n), p_m \Rightarrow m < \eta \cdot t$.

Proof of the Boundedness Theorem 16. Assume $\overset{\eta}{\mid\!\!\!\cdot}\ \mathcal{O}\mathrm{Ind}(n)$. By applying first $(\bigvee)$-Exportation and then $(\bigwedge)$-Inversion from Section 2 we obtain $\overset{\eta}{\mid\!\!\!\cdot}\ \neg\, \mathcal{O}\mathrm{Prog}(n), p_{n-1}$. Hence, the above Lemma shows $n - 1 < \eta \cdot t$ and the assertion follows. □

Proof of the above lemma. Assume for the sake of contradiction that

$$|\!\frac{\eta}{\bullet}\, \neg\, \mathcal{O}\mathrm{Prog}(n), p_m \qquad \text{and} \qquad \eta \cdot t \leq m \ .$$

For a finite set $M \subseteq \mathbb{N}$ let $\overline{\mathrm{en}}_M$ denote the enumeration function of $\mathbb{N} \setminus M$. Let $\mathcal{R}^{\gamma}(M)$ be the set $\{a \,:\, a < \overline{\mathrm{en}}_M(\gamma)\} \cup M$.

We will construct by recursion on l sets $\Delta_l \subseteq \Delta_1^t$, $M_l^+, M_l^- \subseteq \mathbb{N}$ for $l = \eta, \ldots, 0$ satisfying the property $\mathcal{G}(l, \Delta_l, M_l^+, M_l^-)$ given by

i) $|\!\frac{l}{\bullet}\, \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_l$.

ii) $|M_l^+| + |M_l^-| \leq t \cdot (\eta - l)$.

iii) all $\varphi \in \Delta_l$, which are not variables, are fixed by (M_l^+, M_l^-) to 0.

iv) $\mathcal{R}^{l\cdot t}(M_l^+) \not\models \Delta_l$.

v) $\mathcal{R}^{l\cdot t}(M_l^+) \cap M_l^- = \emptyset$.

For $l = 0$ the assertion follows. Because, if we have constructed $\Delta_0 \subseteq \Delta_1^t$, $M_0^+, M_0^- \subseteq \mathbb{N}$ which satisfy $\mathcal{G}(0, \Delta_0, M_0^+, M_0^-)$, then $\mathcal{G}(0, \Delta_0, M_0^+, M_0^-)$ **i)** shows $|\!\frac{0}{\bullet}\, \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_0$, hence Δ_0 must be an axiom. But this contradicts $\mathcal{G}(0, \Delta_0, M_0^+, M_0^-)$ **iv)** and the assertion follows.

We now prove the assertion by backwards-induction from $l = \eta$ to 0. To start the induction for $l = \eta$ let $\Delta_\eta := \{p_m\}$ and $M_\eta^+ := M_\eta^- := \emptyset$. Then $\mathcal{G}(\eta, \Delta_\eta, M_\eta^+, M_\eta^-)$ **i)**, **ii)**, **iii)**, **v)** immediately follow. For $\mathcal{G}(\eta, \Delta_\eta, M_\eta^+, M_\eta^-)$ **iv)** observe that $\overline{\mathrm{en}}_\emptyset(\eta \cdot t) = \eta \cdot t \leq m$, hence $m \notin \mathcal{R}^{\eta\cdot t}(\emptyset)$.

For the induction step $l+1 \rightsquigarrow l$ assume that we have constructed $\Delta_{l+1} \subseteq \Delta_1^t$, $M_{l+1}^+, M_{l+1}^- \subseteq \mathbb{N}$ satisfying $\mathcal{G}(l+1, \Delta_{l+1}, M_{l+1}^+, M_{l+1}^-)$. We will consider the last inference in $\mathcal{G}(l+1, \Delta_{l+1}, M_{l+1}^+, M_{l+1}^-)$ **i)** which leads to $|\!\frac{l+1}{\bullet}\, \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}$. Let $\mathcal{R}^*$ abbreviate $\mathcal{R}^{(l+1)\cdot t}(M_{l+1}^+)$. In order to simplify sub-cases, we first argue that it is enough to find some $\psi \in \Delta_1^t$ and $M^+, M^- \subseteq \mathbb{N}$ satisfying the following property:

I) $|\!\frac{l}{\bullet}\, \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \psi$.

II) (M^+, M^-) fixes ψ to 0.

III) $|M^+| + |M^-| \leq t$.

IV) $M^+ \subseteq \mathcal{R}^*$.

V) $\mathcal{R}^* \cap M^- = \emptyset$.

Then, $\Delta_l := \Delta_{l+1} \cup \{\psi\}$, $M_l^+ := M_{l+1}^+ \cup M^+$, $M_l^- := M_{l+1}^- \cup M^-$ will satisfy property $\mathcal{G}(l, \Delta_l, M_l^+, M_l^-)$, because $\mathcal{G}(l, \Delta_l, M_l^+, M_l^-)$ **i)** and **ii)** are obvious; and for $\mathcal{G}(l, \Delta_l, M_l^+, M_l^-)$ **iii)**, **iv)** and **v)** we observe

A) $\mathcal{R}^{l\cdot t}(M_l^+) \subseteq \mathcal{R}^{l\cdot t+t}(M_{l+1}^+) \cup M^+ = \mathcal{R}^*$. This follows, because $\overline{\mathrm{en}}_{M\cup\{a\}}(\gamma) \leq \overline{\mathrm{en}}_M(\gamma+1)$, hence $\mathcal{R}^{\gamma}(M \cup \{a\}) \subseteq \mathcal{R}^{\gamma+1}(M) \cup \{a\}$.

B) **V)** and the induction hypothesis $\mathcal{G}(l+1, \Delta_{l+1}, M^+_{l+1}, M^-_{l+1})$ **v)** imply $\mathcal{R}^* \cap M^-_l = \emptyset$, hence $\mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **v)** follows using **A)**.

C) **A)** and **B)** show $\emptyset \neq [M^+_l, M^-_l]$. By construction $[M^+_l, M^-_l] \subseteq [M^+_{l+1}, M^-_{l+1}]$, hence (M^+_l, M^-_l) fixes all $\varphi \in \Delta_{l+1}$ which are not variables, to 0.

Furthermore, $[M^+_l, M^-_l] \subseteq [M^+, M^-]$, hence **II)** implies that ψ is fixed to 0 by (M^+_l, M^-_l). Thus, $\mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **iii)** follows.

D) Utilizing **B)** and **A)** we obtain $\mathcal{R}^{l \cdot t}(M^+_l), \mathcal{R}^* \in [M^+_l, M^-_l]$ hence $\mathcal{G}(l+1, \Delta_{l+1}, M^+_{l+1}, M^-_{l+1})$ **iv)** shows that (M^+_l, M^-_l) fixes every formula in Δ_{l+1} to 0. In particular, $\mathcal{R}^{l \cdot t}(M^+_l) \nvDash \Delta_{l+1}$, which shows $\mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **iv)**.

Now we distinguish sub-cases according to the last inference which leads to $\mid\!\frac{l+1}{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}$. In the sub-cases, we either construct ψ, M^+, M^- satisfying **I)** to **V)**, or we directly construct Δ_l, M^+_l, M^-_l satisfying $\mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$, depending which is easier.

($\bigwedge$) There is some $\varphi = \bigwedge_{j<J} \varphi_j \in \Delta_{l+1}$ such that $\mid\!\frac{l}{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \varphi_j$ for all $j < J$. By induction hypothesis $\mathcal{G}(l+1, \Delta_{l+1}, M^+_{l+1}, M^-_{l+1})$ **iv)** we have that $\mathcal{R}^* \nvDash \varphi$. Thus, there is some $j_0 < J$ such that $\mathcal{R}^* \nvDash \varphi_{j_0}$.

Let $\psi := \varphi_{j_0}$, then $\psi \in \Delta^t_1$ [$\Rightarrow$ **I)**]. By Lemma 20 there are some $M^+ \subseteq \mathcal{R}^*$ [$\Rightarrow$ **IV)**] and $M^- \subseteq \mathbb{N}$ such that $\mathcal{R}^* \cap M^- = \emptyset$ [$\Rightarrow$ **V)**], $|M^+| + |M^-| \leq t$ [$\Rightarrow$ **III)**] and (M^+, M^-) fixes ψ to 0 [$\Rightarrow$ **II)**].

($\bigvee$) The first sub case is that $\neg\, \mathcal{O}\mathrm{Ind}(n)$ is not the main formula of the inference. Then, there is some $\varphi = \bigvee_{j<J} \varphi_J \in \Delta_{l+1}$ such that $\mid\!\frac{l}{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \varphi_{j_0}$ for some $j_0 < J$. By induction hypothesis $\mathcal{G}(l+1, \Delta_{l+1}, M^+_{l+1}, M^-_{l+1})$ **iv)** we have that $\mathcal{R}^* \nvDash \varphi$, thus also $\mathcal{R}^* \nvDash \varphi_{j_0}$. Now the same argumentation as in the ($\bigwedge$)-case can be applied.

Now assume that the main formula is $\neg\, \mathcal{O}\mathrm{Ind}(n)$. Then, there is some $x < n$ such that

$$\mid\!\frac{l}{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \Big(\bigwedge_{y<x} p_y \Big) \wedge \neg p_x \ .$$

A) Assume, there is some $y < x$ such that $y \notin \mathcal{R}^{l \cdot t}(M^+_{l+1})$. By ($\bigwedge$)-Inversion we obtain $\mid\!\frac{l}{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, p_y$. Let $\Delta_l := \Delta_{l+1}, p_y$ [$\Rightarrow$ $\mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **i)**], $M^+_l := M^+_{l+1}$ and $M^-_l := M^-_{l+1}$ [$\Rightarrow$ $\mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **ii)**, **iii)**]. Now $\mathcal{R}^{l \cdot t}(M^+_l) \subseteq \mathcal{R}^*$ [$\Rightarrow \mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **v)**], hence, using the assumption $y \notin \mathcal{R}^{l \cdot t}(M^+_l)$, we obtain $\mathcal{R}^{l \cdot t}(M^+_l) \nvDash \Delta_l$ [$\Rightarrow \mathcal{G}(l, \Delta_l, M^+_l, M^-_l)$ **iv)**].

B) Now assume that **A)** does not hold, hence $y \in \mathcal{R}^{l \cdot t}(M^+_{l+1})$ for all $y < x$. This implies $x \in \mathcal{R}^{l \cdot t+1}(M^+_{l+1}) \subseteq \mathcal{R}^*$. Because, $\overline{\mathrm{en}}_M(\gamma) \notin \mathcal{R}^\gamma(M)$, hence $y \in \mathcal{R}^\gamma(M)$ for all $y < x$ implies $\overline{\mathrm{en}}_M(\gamma) \geq x$, hence $\overline{\mathrm{en}}_M(\gamma + 1) > x$ and in sequel $x \in \mathcal{R}^{\gamma+1}(M)$.

By $(\bigwedge)$-Inversion we obtain $\mathrel{|\!\frac{l}{\bullet}} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \neg p_x$. Let $\psi := \neg p_x$ $[\Rightarrow$ **I)**$]$, $M^+ := \{x\}$ and $M^- := \emptyset$ $[\Rightarrow$ **II)**, **III)**, **IV)**, **V)**$]$.

(Cut) There is some $\varphi \in \dot{\Delta}^t_1$ such that $\mathrel{|\!\frac{l}{\bullet}} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \varphi$ and $\mathrel{|\!\frac{l}{\bullet}} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \neg\varphi$. W.l.o.g. we may assume $\mathcal{R}^* \nvDash \varphi$. The same argumentation as in $(\bigwedge)$ yields the assertion.

$\square$

References

[1] Theodore Baker, John Gill, and Robert Solovay. Relativizations of the $\mathcal{P} = ?\mathcal{NP}$ question. *SIAM J. Comput.*, 4:431–442, 1975.

[2] Arnold Beckmann. *Seperating fragments of bounded predicative arithmetic.* PhD thesis, Westf. Wilhelms-Univ., Münster, 1996.

[3] Arnold Beckmann. Dynamic ordinal analysis. *Arch. Math. Logic*, 2001. accepted for publication.

[4] Arnold Beckmann. Resolution refutations and propositional proofs with height-restriction. In Julian Bradfield, editor, *Proccedings of the 16th International Workshop, CSL 2002 (Edinburgh)*, Berlin, 2002. Springer-Verlag.

[5] Samuel R. Buss. *Bounded arithmetic*, volume 3 of *Stud. Proof Theory, Lect. Notes.* Bibliopolis, Naples, 1986.

[6] Samuel R. Buss. Relating the bounded arithmetic and the polynomial time hierarchies. *Ann. Pure Appl. Logic*, 75:67–77, 1995.

[7] Samuel R. Buss and Jan Krajíček. An application of boolean complexity to separation problems in bounded arithmetic. *Proc. London Math. Soc.*, 69:1–21, 1994.

[8] Johan Håstad. *Computational Limitations of Small Depth Circuits.* MIT Press, Cambridge, MA, 1987.

[9] Johan Håstad. Almost optimal lower bounds for small depth circuits. *Randomness and Computation*, 5:143–70, 1989.

[10] Jan Krajíček. Fragments of bounded arithmetic and bounded query classes. *Trans. Amer. Math. Soc.*, 338:587–98, 1993.

[11] Jan Krajíček. Lower bounds to the size of constant-depth propositional proofs. *J. Symbolic Logic*, 59:73–86, 1994.

[12] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Cambridge University Press, Heidelberg/New York, 1995.

[13] Jan Krajíček. On the weak pigeonhole principle. *Fund. Math.*, 170:197–212, 2001.

[14] Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti. Bounded arithmetic and the polynomial hierarchy. *Ann. Pure Appl. Logic*, 52:143–153, 1991.

[15] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. In *Methods in mathematical logic (Caracas, 1983)*, pages 317–340. Springer, Berlin, 1985.

[16] Chris Pollett. Structure and definability in general bounded arithmetic theories. *Ann. Pure Appl. Logic*, 100:189–245, 1999.

[17] Andrew C. Yao. Separating the polynomial-time hierarchy by oracles. *Proc. 26th Ann. IEEE Symp. on Foundations of Computer Science*, pages 1–10, 1985.

[18] Domenico Zambella. Notes on polynomially bounded arithmetic. *J. Symbolic Logic*, 61:942–966, 1996.