Generalised Dynamic Ordinals – universal measures for implicit computational complexity

Arnold Beckmann*
University of Wales Swansea
Singleton Park
Swansea SA2 8PP, UK
A.Beckmann@swansea.ac.uk

June 29, 2005

Abstract

We extend the definition of dynamic ordinals to *generalised dynamic ordinals*. We compute generalised dynamic ordinals of all fragments of relativised bounded arithmetic by utilising methods from Boolean complexity theory, similar to Krajíček in [14]. We indicate the role of generalised dynamic ordinals as universal measures for implicit computational complexity. I.e., we describe the connections between generalised dynamic ordinals and witness oracle Turing machines for bounded arithmetic theories. In particular, through the determination of generalised dynamic ordinals we re-obtain well-known independence results for relativised bounded arithmetic theories.

Keywords: Bounded arithmetic; dynamic ordinals; universal measures; witness oracle Turing machines; implicit computational complexity; independence results; Håstad's Switching Lemmas; cut-reduction by switching.

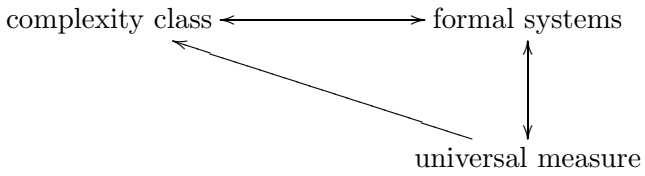
MSC: 03F20; 03F30, 68Q15, 68R99.

1 Introduction

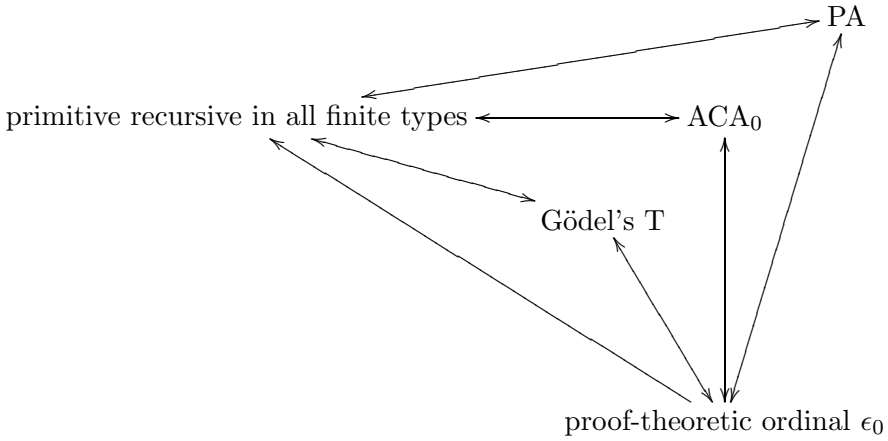
Implicit computational complexity denotes the collection of approaches to computational complexity which define and classify the complexity of computations without direct reference to an underlying machine model. These approaches are formal systems which cover a wide range, including applicative functional programming languages, linear logic, bounded arithmetic and finite model theory (cf. [17]). In this paper, we contribute to the idea

*This work has been supported by a Marie Curie Individual Fellowship #HPMF-CT-2000-00803 from the European Commission.

of characterising the computational complexity of such formal systems by universal measures, such that the formal systems describe exactly the same complexity class, if and only if they agree in their universal measures. In general, we aim at connections which can be represented as follows:



Many formal systems admit such kind of universal measures. For example, in case of "strong" implicit computational complexity, e.g. for number-theoretic functions which are computable by primitive recursive functionals in finite types, so-called proof-theoretic ordinals have proven useful as universal measures of proof and computation (and also consistency) strength (cf. [19]). With respect to our general picture this situation can be represented as follows:



In this paper, we will focus on weak, also called low-level, complexity classes, i.e. complexity classes below EXPTIME. We will approach the general idea of finding universal measures by doing a case study for a particular framework of weak implicit computational complexity called bounded arithmetic. We already argued in [3] that so-called dynamic ordinals can be viewed as universal measures for *some* fragments of bounded arithmetic and corresponding bounded witness oracle Turing machine classes. In this paper, we will extend this project by defining and computing generalised dynamic ordinals and indicating their role as universal measures for *all* bounded arithmetic theories.

Bounded arithmetic theories are logical theories of arithmetic given as restrictions of Peano arithmetic. Quantification and induction are restricted ("bounded") in such a manner that complexity-theoretic classes can be

closely tied to provability in these theories. 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 by Buss [6]. The class of predicates definable by Σ_i^b (or Π_i^b) formulas is precisely the class of predicates in the ith level Σ_i^p (respectively Π_i^p) of the polynomial time hierarchy. The Σ_i^b-definable functions of S_2^i are precisely the functions which are polynomial time computable with an oracle from Σ_{i-1}^p (cf. [6]). Krajíček [13] has characterised the Σ_{i+1}^b-definable multivalued functions of S_2^i as $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(\log n))$. Here, $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(\log n))$ denotes the class of multivalued functions computable by a polytime Σ_i^b-witness oracle Turing machine with the number of queries bounded by $O(\log n)$, see Section 3 for a precise definition. These results are extended and generalised by Pollett [20] to all bounded arithmetic theories.

It is an open problem of bounded arithmetic whether the hierarchy of theories collapses. This problem is connected with the open problem in complexity theory whether the polynomial time hierarchy PH collapses – the P=?NP problem is a sub-problem of this – in the following way: The hierarchy of bounded arithmetic theories collapses, if and only if the polynomial time hierarchy collapses provably in bounded arithmetic (cf. [16, 8, 23]). The case of relativised complexity classes and theories is completely different. The existence of an oracle A is proven in [1, 22, 10], such that the polynomial time hierarchy in this oracle PH^A does not collapse, hence in particular $\mathrm{P}^A \neq \mathrm{NP}^A$ holds. Building on this one can show $\mathrm{T}_2^i(\alpha) \neq \mathrm{S}_2^{i+1}(\alpha)$ [16]. Here, the relativised theories $\mathrm{S}_2^i(\alpha)$ and $\mathrm{T}_2^i(\alpha)$ result from S_2^i, and T_2^i respectively, 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 [13], and separation results for further relativised theories (dubbed $\Sigma_n^b(\alpha)$-$\mathrm{L}^m\mathrm{IND}$) are proven in [20]. Independently of these, and with completely different methods (see below), we have shown separation results for theories of relativised bounded arithmetic in [2, 4]. Despite all answers in the relativised case, all separation questions continue to be open for theories without set parameters.

The above mentioned alternative approach to the study of relativised bounded arithmetic theories is called dynamic ordinal analysis [2, 4]. Inspired from proof-theoretic ordinal analysis, which has its origin in Gentzen's consistency proof for PA, the proof theoretic strengths of bounded arithmetic theories are characterised by so-called dynamic ordinals. The dynamic ordinals $\mathrm{DO}(T(\alpha))$ for some relativised bounded arithmetic theories $T(\alpha)$ have been defined and computed in [2, 4]. $\mathrm{DO}(T(\alpha))$ is a set of unary number-theoretic functions, which characterises the amount of $\Pi_1^b(\alpha)$-order-induction provable in $T(\alpha)$. In [3], we have described how this fits into our general program on finding universal measure by connecting dynamic ordinals with witness oracle computations. The above mentioned characterisation of definable multivalued functions of higher bounded arithmetic theories suggests the following definition of generalised dynamic ordinals

(for more details on this motivation see the discussion in [3]): The i-th generalised dynamic ordinal $\mathrm{DO}_i(T(\alpha))$ of a relativised theory of bounded arithmetic $T(\alpha)$ characterises the amount of $\Pi^b_i(\alpha)$-order-induction provable in $T(\alpha)$ (thus, the usual dynamic ordinal is just the first generalised dynamic ordinal).

In this paper, we will define and compute generalised dynamic ordinals for all bounded arithmetic theories. This computation utilises methods from Boolean complexity like Håstad's Switching Lemmas [10, 11] to obtain a special cut-elimination technique, which we denote by "cut-reduction by switching". Krajíček has been the first utilising such methods from Boolean complexity to reduce the complexity of propositional proofs [14], and Buss and Krajíček successfully adapted these methods to reduce the oracle complexity of witnessing arguments [9]. Cut-reduction by switching will be formulated as a cut-elimination method. 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. This blow up would destroy the computation of generalised dynamic ordinals. But still, the computation needs a reduction of the complexity of cut-formulas. Cut-reduction by switching will reduce cuts "inside-out", but will leave the proof-skeleton unchanged, e.g. the height of the derivation will remain the same. The price will be that not only the cut-formulas are reduced, but also the formula which is derived. This can be addressed by well-known utilisations of so-called Sipser functions ([14, 9]), again originating from Boolean complexity [10, 11].

Our results will be, that for all $i > 0$, the generalised dynamic ordinals are computed to

$$\begin{aligned}
\mathrm{DO}_i(\mathrm{T}^i_2(\alpha)) &= \{\lambda n.2^{|n|^c} \,:\, c \text{ a number}\} \\
\mathrm{DO}_i(\mathrm{S}^i_2(\alpha)) &= \{\lambda n.|n|^c \,:\, c \text{ a number}\} \\
\mathrm{DO}_i(\mathrm{sR}^{i+1}_2(\alpha)) &= \{\lambda n.2^{||n||^c} \,:\, c \text{ a number}\} \ ,
\end{aligned}$$

and more generally for $m > 0$

$$\mathrm{DO}_i(\Sigma^b_{i+m-1}(\alpha)\text{-L}^m\text{IND}) = \{\lambda n.2_m(c \cdot (|n|_{m+1})) \,:\, c \text{ a number}\} \ .$$

In particular we re-obtain the above mentioned separations of bounded arithmetic theories by dynamic ordinal analysis. We have displayed this situation in Fig. 1. The method of proving separations by dynamic ordinal analysis heavily differs from the above mentioned separation results, as no characterisations of definable functions and no oracle constructions are involved. In the figure, we mean with $S <_i T$ that the theories S and T are separated by a $\forall\Sigma^b_i$-sentence and that S is included in the consequences of T; with $S \not\subseteq_i T$ that S is separated from T by a $\forall\Sigma^b_i$-sentence, but not necessarily included;

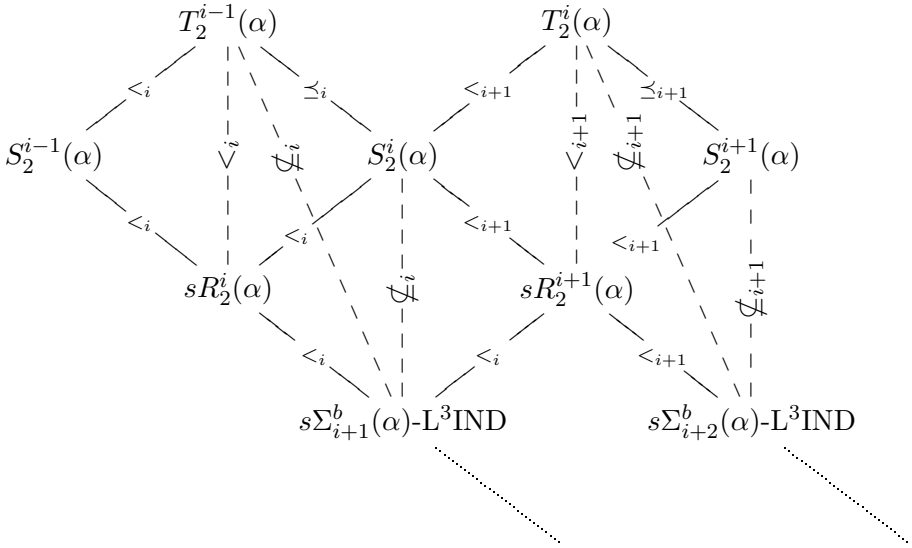


Figure 1: Independence results obtained by dynamic ordinal analysis

and with $S \preceq_i T$ that T is $\forall\Sigma_i^b$-conservative over S. The conservation results displayed in the figure have been proven by Buss [7].

Furthermore, we obtain the following connections between the i-th dynamic ordinal of relativised bounded arithmetic theories and the Σ_{i+1}^b-definable multivalued functions of their unrelativised companions. For $i > 0$ and for T from the following infinite list of theories

$$\mathrm{T}_2^i,\ \mathrm{S}_2^{i+1},\ \mathrm{S}_2^i,\ \mathrm{sR}_2^{i+1},\ \text{and } \Sigma_{i+m-1}^b\text{-L}^m\text{IND for all } m > 0,$$

we obtain:

> A multivalued function f is Σ_{i+1}^b-definable in T, if and only if f is computable by some polytime Σ_i^b-witness oracle Turing machine with the number of queries bounded by $\log(\mathrm{DO}_i(T(\alpha)))$.

This indicates that dynamic ordinals do in fact also characterise the *computational complexity* of bounded arithmetic theories. What is still missing is an intrinsic insight into this connection; this is work in progress.

The paper is organised as follows. In the following section we review the definition of bounded arithmetic theories. In Section 3 we define witness oracle Turing machines and review results characterising definable multivalued functions of bounded arithmetic theories by witness oracle Turing machines. The fourth section summarises definition of and results on dynamic ordinals, and gives the definition as well as lower bounds of the i-th generalised dynamic ordinal. In Section 5 we introduce a version of Gentzen's propositional

proof system LK and prove basic properties like usual cut-elimination, and review translations from bounded arithmetic to LK. Section 6 introduces cut-reduction by switching and sketches of proof of this, which will be used in Section 7 to prove lower bounds to the height of derivations of the order induction principle. The results from Sections 5 to 7 have meanwhile been subject of a technical report [5]. In Section 8 we utilise the lower bound on derivation heights proved in Section 7 to compute the missing upper bounds on dynamic ordinals, which in turn will be used to obtain the connections between generalised dynamic ordinals and witness oracle Turing machines.

2 Bounded arithmetic

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

Bounded arithmetic can be formulated as the fragment $I\Delta_0 + \Omega_1$ of Peano arithmetic in which induction is restricted to bounded formulas and Ω_1 expresses a growth rate strictly smaller than exponentiation, namely that $2^{|x|^2}$ exists for all x. Here, $|x|$ denotes the length of the binary representation of x, i.e. an integer valued logarithm of x. The same fragment is obtained by extending the language of Peano arithmetic, and we will follow this approach first given by Buss, cf. [6]. Let us recall some definitions.

The language of bounded arithmetic[1] $\mathcal{L}_{\mathrm{BA}}$ consists of function symbols 0 (zero), S (successor), + (addition), $\cdot$ (multiplication), $|x|$ (binary length), $\lfloor \frac{1}{2}x \rfloor$ (binary shift right), $x \# y$ (smash, $x\#y := 2^{|x|\cdot|y|}$), $x \dot{-} y$ (arithmetical subtraction), $\mathrm{MSP}(x,i)$ (Most Significant Part) and $\mathrm{LSP}(x,i)$ (Less Significant Part), and relation symbols $=$ (equality) and $\leq$ (less than or equal). The meaning of MSP and LSP as number-theoretic functions is uniquely determined by stipulating that

$$x = \mathrm{MSP}(x,i) \cdot 2^i + \mathrm{LSP}(x,i) \qquad \text{and} \qquad \mathrm{LSP}(x,i) < 2^i$$

holds for all x and i. Restricted exponentiation $2^{\min(x,|y|)}$ can be defined by the term

$$2^{\min(x,|y|)} \quad = \quad \mathrm{MSP}(y \# 1, |y| \dot{-} x) \ ,$$

hence we can assume that restricted exponentiation is also part of our language $\mathcal{L}_{\mathrm{BA}}$. We often write 2^t and mean $2^{\min(t,|x|)}$ if $t \leq |x|$ is clear from the context. Relativised bounded arithmetic is formulated in the language $\mathcal{L}_{\mathrm{BA}}(\alpha)$ which is $\mathcal{L}_{\mathrm{BA}}$ extended by one set variable α and the element relation symbol $\in$.

[1] For the sake of completeness we will fix a language for bounded arithmetic. In principle, our results can be obtained for any sufficient formulation, because they are stable under extending the language by arbitrary functions which have polynomial growth rate. See [4] for a discussion.

BASIC is a finite set of open axioms (cf. [6, 21, 12]) which axiomatises the non-logical symbols. When dealing with $\mathcal{L}_{\mathrm{BA}}(\alpha)$ we assume that BASIC also contains the equality axioms for α.

Bounded quantifiers play an important role in bounded arithmetic. We abbreviate

$$\begin{array}{llll} (\forall x \le t)A & := & (\forall x)(x \le t \to A) & \qquad (\exists x \le t)A \;:=\; (\exists x)(x \le t \wedge A) \\ (\forall x < t)A & := & (\forall x \le t)(t \not\le x \to A) & (\exists x < t)A \;:=\; (\exists x \le t)(t \not\le x \wedge A) \end{array}$$

The quantifiers $(Q\, x \le t)$, $(Q\, x < t)$, $Q \in \{\forall, \exists\}$, are called *bounded quantifiers*. A bounded quantifier of the form $(Q\, x \le |t|)$, $Q \in \{\forall, \exists\}$, is called a *sharply bounded quantifier*. A formula in which all quantifiers are (sharply) bounded is called a *(sharply) bounded formula*. Bounded formulas are stratified into levels:

i) $\Delta_0^b = \Sigma_0^b = \Pi_0^b$ is the set of all sharply bounded formulas.

ii) Σ_n^b-formulas are those which have a block of n alternating bounded quantifiers, starting with an existential one, in front of a sharply bounded kernel.

iii) Π_n^b is defined dually, i.e. the block of alternating quantifiers starts with a universal one.

In the relativised case $\Delta_0^b(\alpha)$, $\Sigma_n^b(\alpha)$, $\Pi_n^b(\alpha)$ are defined analogously.

Attention: In our definition, the class Σ_n^b consists only of *prenex*, also called *strict*, formulas. In other places in the literature like [6, 15], the definition of Σ_n^b is more liberal, and the class defined here is then denoted $s\Sigma_n^b$, where the "s" indicates "strict".

Induction is also stratified. Let $|x|_m$ denote the m-fold iteration of the binary length function, which can recursively be defined by $|x|_0 := x$ and $|x|_{m+1} := |(|x|_m)|$.

> For Ψ is a set of $\mathcal{L}_{\mathrm{BA}}$-formulas and m is a natural number, let Ψ-L^{m}IND denote the schema
>
> $$\varphi(0) \wedge (\forall x < |t|_m)(\varphi(x) \to \varphi(\mathrm{S}\, x)) \to \varphi(|t|_m)$$
>
> for all $\varphi \in \Psi$ and $\mathcal{L}_{\mathrm{BA}}$-terms t.

For $m = 0$ this is the usual successor induction schema and will be denoted by Ψ-IND. In case $m = 1$ we often write Ψ-LIND.

The bounded arithmetic theories under consideration are given by

$$\mathrm{BASIC} + \Sigma_n^b\text{-L}^m\mathrm{IND}\ .$$

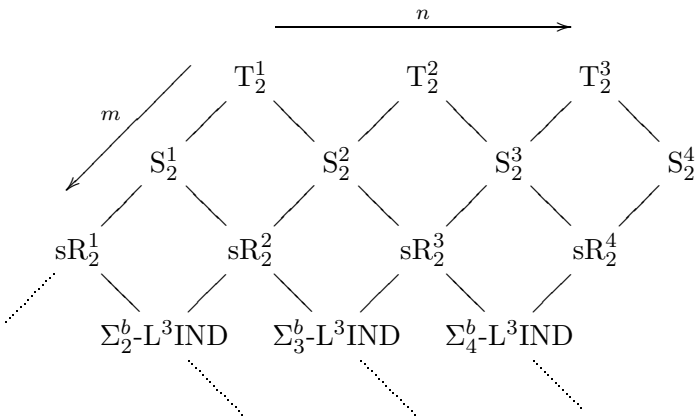


Figure 2: The theories Σ_n^b-L^mIND. Following any line rightwards takes one to super-theories. For example, $sR_2^1 \subseteq T_2^2$ following e.g. the path sR_2^1, S_2^1, T_2^1, S_2^2, T_2^2

Usually we do not mention BASIC and simply call this theory Σ_n^b-L^mIND. Some of the theories have special names:

$$\begin{aligned} T_2^i &:= \Sigma_i^b\text{-IND} \ , \\ S_2^i &:= \Sigma_i^b\text{-LIND} \ , \\ sR_2^i &:= \Sigma_i^b\text{-}L^2\text{IND} \ . \end{aligned}$$

For theories S, T let $S \subseteq T$ denote that all axioms in S are consequences of T. From the definition of the theories, the following two inclusions immediately follow:

$$\begin{aligned} \Sigma_n^b\text{-}L^{m+1}\text{IND} &\subseteq \Sigma_n^b\text{-}L^m\text{IND} \ , \\ \Sigma_n^b\text{-}L^m\text{IND} &\subseteq \Sigma_{n+1}^b\text{-}L^m\text{IND} \ . \end{aligned}$$

A little bit more insight is needed to obtain

$$\Sigma_n^b\text{-}L^m\text{IND} \subseteq \Sigma_{n+1}^b\text{-}L^{m+1}\text{IND} \ ,$$

see [6] for a proof. Fig. 2 reflects the just obtained relations – going from left to right in the diagram means that the theory on the lefthand side of an edge is included in the theory on the righthand side.

Similar definitions and results can be stated for relativised bounded arithmetic theories.

3 Witness oracle query complexity

In this section we repeat the definition of witness oracle Turing machines and summarise how definable multivalued functions in bounded arithmetic theories are connected to witness oracle Turing machines.

A Turing machine with a witness oracle $Q(x) = (\exists y)R(x, y)$ is a Turing machine with a query tape for queries to Q that answers a query a as follows:

i) if $Q(a)$ holds, then it returns YES and some b such that $R(a, b)$ holds;

ii) if $\neg Q(a)$ holds, then it returns NO.

In general this type of Turing machines, called witness oracle Turing machines (WOTM), compute only *multivalued* functions rather than functions, as there may be multiple witnesses to affirmative oracle answers. A multivalued function is a relation $f \subseteq \mathbb{N} \times \mathbb{N}$ such that for all $x \in \mathbb{N}$ there exists some $y \in \mathbb{N}$ with $(x, y) \in f$. We express $(x, y) \in f$ as $f(x) = y$. A natural stratification of WOTMs, called bounded WOTMs, is obtained by bounding the number of oracle queries.

For Φ is a set of formulas, a multivalued function f is called Φ-definable in some theory T if there is a formula $\varphi(x, y)$ in Φ such that φ describes the graph of f and T proves the totality of f via φ, i.e.

$$T \vdash (\forall x)(\exists y)\varphi(x, y)$$
$$\mathbb{N} \vDash (\forall x)(\forall y)[f(x) = y \leftrightarrow \varphi(x, y)]$$

Krajíček [13] has characterised the Σ^b_{i+1}-definable multivalued functions of T^i_2 and S^i_2 as $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, poly)$, and $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, O(\log n))$ respectively. $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, poly)$ and $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, O(\log n))$ are the classes of multivalued functions computable by a polynomial time WOTM which on inputs of length n uses fewer than respectively $n^{O(1)}$ and $O(\log n)$ witness queries to a Σ^b_i-oracle.

Pollett [20] obtains further relationships of definable multivalued functions and bounded polynomial time WOTM classes. The following version of bounded polynomial time WOTM classes goes back to [20].

Definition 1. Let τ be a set of unary functions represented by terms in $\mathcal{L}_{\mathrm{BA}}$. $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, \tau)$ is the class of multivalued functions computable by a polynomial time WOTM which on input x uses fewer than $l(t(x))$ witness queries to a Σ^b_i-oracle for some $l \in \tau$ and $\mathcal{L}_{\mathrm{BA}}$-term t.

With id we denote the identity function, $\mathrm{id}(n) = n$. The classes $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, poly)$ and $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, O(\log n))$ considered by Krajíček can be expressed as respectively $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, |\,\mathrm{id}\,|)$ and $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, O(|\,\mathrm{id}\,|_2))$ using the previous definition. The following characterisations of definable multivalued

functions by bounded polynomial time WOTMs can be read of the results by Pollett [20], see [20] or [3] for more details. Let us remind that $2_m(x)$ and $|x|_m$ denote the m-fold iterations of the exponentiation function, respectively binary length function.

Theorem 2 (Pollett [20]). *Let $i \geq 0$ and $m \geq 1$.*

A multivalued function f is Σ^b_{i+2}-definable in Σ^b_{m+i}-L^{m}IND, if and only if $f \in \mathrm{FP}^{\Sigma^b_{i+1}}(\mathrm{wit}, 2_{m-1}(O(|\,\mathrm{id}\,|_{m+1})))$.

4 Generalised dynamic ordinals

We start this section by repeating definitions of and results on dynamic ordinals for some fragments of bounded arithmetic from [4] and [3]. The underlying language will always be the language $\mathcal{L}_{\mathrm{BA}}(\alpha)$ of relativised bounded arithmetic.

For $A(a)$ is a formula, let $\mathcal{S}\mathrm{Ind}(t, A)$ and $\mathcal{O}\mathrm{Ind}(t, A)$ be defined by

$$\begin{aligned} \mathcal{S}\mathrm{Ind}(t, A) &:= A(0) \wedge (\forall x < t)(A(x) \to A(\mathrm{S}\, x)) \to A(t) \\ \mathcal{O}\mathrm{Ind}(t, A) &:= (\forall x < t)((\forall y < x)A(y) \to A(x)) \to (\forall x < t)A(x) \end{aligned}$$

Order induction, denoted by $\mathcal{O}\mathrm{Ind}$, applied to a formula A is logically equivalent to minimisation applied to the *negation* of A. It is well-known that over the base theory BASIC the schema Σ^b_i-IND is equivalent to minimisation for Σ^b_i-formulas which is equivalent (by coding one existential quantifier) to minimisation for Π^b_{i-1}-formulas [6, 15].

For Φ is a set of formulas, let $\mathcal{O}\mathrm{Ind}(t, \Phi)$ denote the schema of all instances $\mathcal{O}\mathrm{Ind}(t, A)$ for $A \in \Phi$ and $\mathcal{L}_{\mathrm{BA}}$-terms t. Similarly for $\mathcal{S}\mathrm{Ind}$. When saying "let T be a theory" we always mean that T contains some weak base theory, say $\mathrm{S}^0_2 \subseteq T$.

In [4] we have defined the dynamic ordinal $\mathrm{DO}(T)$ of a theory T by

$$\mathrm{DO}(T) \quad := \quad \{\lambda x.t \colon T \vdash (\forall x)\ \mathcal{O}\mathrm{Ind}(t, \Pi^b_1(\alpha))\} \ .$$

In this definition, it is understood that t ranges over $\mathcal{L}_{\mathrm{BA}}$-terms in which at most x occurs as a variable. Dynamic ordinals are sets of number theoretic functions, i.e. subsets of ${}^{\mathbb{N}}\mathbb{N}$. Subsets of ${}^{\mathbb{N}}\mathbb{N}$ can be arranged by eventual majorisability:

$$f \trianglelefteq g \quad :\Leftrightarrow \quad g \text{ eventually majorises } f \quad \Leftrightarrow \quad (\exists m)(\forall n \geq m) f(n) \leq g(n) \ .$$

For subsets of number theoretic functions $D, E \subseteq {}^{\mathbb{N}}\mathbb{N}$ we define

$$\begin{aligned} D \trianglelefteq E \quad &:\Leftrightarrow \quad (\forall f \in D)(\exists g \in E) f \trianglelefteq g \\ D \equiv E \quad &:\Leftrightarrow \quad D \trianglelefteq E \ \ \& \ \ E \trianglelefteq D \\ D \triangleleft E \quad &:\Leftrightarrow \quad D \trianglelefteq E \ \ \& \ \ E \not\trianglelefteq D \end{aligned}$$

$\trianglelefteq$ is a partial, transitive, reflexive ordering, $\triangleleft$ is a partial, transitive, irreflexive, not well-founded ordering, and $\equiv$ is an equivalence relation.

Using the big-O notation we will denote sets of unary number-theoretic functions in the following way:

$$f(O(g(\mathrm{id}))) \quad := \quad \{\lambda n.f(c \cdot g(n)) \colon c \in \mathbb{N}\}$$

for unary number-theoretic functions f and g.

The dynamic ordinals for certain bounded arithmetic theories are well established (cf. [4]):

$$\begin{array}{lcll} \mathrm{DO}(\mathrm{T}^1_2(\alpha)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_2)) & \equiv \quad \mathrm{DO}(\mathrm{S}^2_2(\alpha)) \\ \mathrm{DO}(\mathrm{S}^1_2(\alpha)) & \equiv & 2_1(O(|\,\mathrm{id}\,|_2)) & \\ \mathrm{DO}(\mathrm{sR}^2_2(\alpha)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_3)) & \end{array}$$

and more generally for $m > 0$

$$\mathrm{DO}(\Sigma^b_m(\alpha)\text{-}\mathrm{L}^m\mathrm{Ind}) \quad \equiv \quad 2_m(O(|\,\mathrm{id}\,|_{m+1})) \ .$$

In [3] we have described the following connections between the dynamic ordinal of some relativised bounded arithmetic theories and the Σ^b_2-definable multivalued functions of their unrelativised companions. For T from the following infinite list of theories

> T^1_2, S^2_2, S^1_2, sR^2_2, and Σ^b_m-L^mIND for all $m > 0$,

we obtain:

> A multivalued function f is Σ^b_2-definable in T, if and only if f is computable by some polytime Σ^b_1-witness oracle Turing machine with the number of queries bounded by $\log(\mathrm{DO}(T(\alpha)))$.

Hence, the characterisation of definable multivalued functions of bounded arithmetic theories from the previous section suggests the following definition of generalised dynamic ordinals (see discussion in [3] for more details):

Definition 3. The i-th generalised dynamic ordinal of an $\mathcal{L}_{\mathrm{BA}}(\alpha)$-theory T is defined by

$$\mathrm{DO}_i(T) \quad := \quad \{\lambda x.t \colon T \vdash (\forall x)\ \mathcal{O}\mathrm{Ind}(t, \Pi^b_i(\alpha))\} \ .$$

In this definition and in the next theorem, it is understood that t ranges over $\mathcal{L}_{\mathrm{BA}}$-terms in which at most x occurs as a variable. Observe that the previous definition of the dynamic ordinal of a theory T, $\mathrm{DO}(T)$, is the same as the first generalised dynamic ordinal of T, $\mathrm{DO}_1(T)$.

As generalised dynamic ordinals consist of terms in the language $\mathcal{L}_{\mathrm{BA}}$, a crude upper bound on generalised dynamic ordinals is always given by the growth rates of the functions representable by $\mathcal{L}_{\mathrm{BA}}$-terms:

$$\mathrm{DO}_i(T) \quad \trianglelefteq \quad 2^{|\,\mathrm{id}\,|^{O(1)}} \quad = \quad 2_2(O(|\,\mathrm{id}\,|_2)) \ .$$

Generalised dynamic ordinals can also be characterised in terms of $\mathcal{S}\mathrm{Ind}$. In [4] we have shown that for sets of bounded formulas Φ which are closed under bounded universal quantification, we have $T \vdash \mathcal{O}\mathrm{Ind}(t, \Phi)$ if and only if $T \vdash \mathcal{S}\mathrm{Ind}(t, \Phi)$. Hence we have the following alternative characterisation of generalised dynamic ordinals:

Corollary 4. $\mathrm{DO}_i(T) \quad = \quad \{\lambda x.t \colon T \vdash (\forall x)\ \mathcal{S}\mathrm{Ind}(t, \Pi^b_i(\alpha))\}$.

In [4] we have shown that different dynamic ordinals imply a separation of the underlying theories. A similar property holds for generalised dynamic ordinals.

Lemma 5. *Let S, T be two theories in the language of bounded arithmetic and assume $\mathrm{DO}_i(S) \neq \mathrm{DO}_i(T)$. Then S is separated from T by some $\forall\Sigma^b_{i+1}(\alpha)$-sentence.*

Proof. Assume $f \in \mathrm{DO}_i(T) \setminus \mathrm{DO}_i(S)$. By the definition of generalised dynamic ordinals there is a term $t(x)$ and a $\Pi^b_i(\alpha)$-formula A such that $f(n) = t(n)$ and $T \vdash (\forall x)\,\mathcal{O}\mathrm{Ind}(t(x), A)$. But $f \notin \mathrm{DO}_i(S)$ implies $S \nvdash (\forall x)\,\mathcal{O}\mathrm{Ind}(t(x), A)$. Obviously, $\mathcal{O}\mathrm{Ind}(t(x), A) \in \Sigma^b_{i+1}(\alpha)$. □

The language $\mathcal{L}_{\mathrm{BA}}$ includes the successor function, $+$ and $\cdot$, which enables us to speed-up induction polynomially. This has been carried out in [4] showing

Theorem 6 ([4, Theorem 9]). $\Sigma^b_n\text{-L}^m\text{IND} \vdash \mathcal{O}\mathrm{Ind}(p(|x|_m), \Pi^b_n)$ *for polynomials p, if $m > 0$ or $n > 0$.*

Order induction for higher formula complexity is connected to order induction on larger orderings by speed-up techniques. The reader unfamilier with such speedup techniques may consult [19, Chaper 15] for the transfinite case of speeding up induction in Peano arithmetic, or [2, Chaper 9] respectively [4, Section 3] for the adapted case to bounded arithmetic. The main ingredient which formalises this is the following jump set $\mathrm{Jp}(t, x, \alpha)$:

$$\Big\{y \leq t \colon t \leq |x| \wedge (\forall z \leq 2^t)[z \subseteq \alpha \wedge z + 2^y \leq 2^t + 1 \to z + 2^y \subseteq \alpha]\Big\} \ .$$

Iterations of Jp are defined by

$$\begin{aligned} \mathrm{Jp}_0(t, x, \alpha) &= \alpha \ , \\ \mathrm{Jp}_{i+1}(t, x, \alpha) &= \mathrm{Jp}(t, |x|_i, \mathrm{Jp}_i(t, x, \alpha)) \ . \end{aligned}$$

Let us remind that $|\cdot|_i$ denotes the i-fold iteration of $|\cdot|$, and that 2_m denotes the m-fold iteration of exponentiation. Using the iterated jump set we obtain the following connections:

Theorem 7 ([4, Corollary 15]).

$$\mathrm{BASIC} \vdash t \leq |x|_m \to [\mathcal{O}\mathrm{Ind}(2_m(t), A) \leftrightarrow \mathcal{O}\mathrm{Ind}(t, \mathrm{Jp}_m(t, x, A))] \ .$$

Proof idea. The direction from left to right follows directly. For the other direction we would have to prove the following statement, see [4, Section 3] for a definition of $\mathcal{O}\mathrm{Prog}$ and a proof of this:

$$\mathrm{BASIC} \vdash t \leq |x| \wedge \mathcal{O}\mathrm{Prog}(2^t, A) \to \mathcal{O}\mathrm{Prog}(t, \mathrm{Jp}(t, x, A)) \ . \qquad \square$$

Concerning the complexity of the iterated jump we observe that

$$\mathrm{Jp}_n(t, x, \Pi^b_i) \subset \Pi^b_{n+i}$$

hence Theorem 6 and Theorem 7 together show the following Corollary, which has been formulated for the base case $i = 1$ in [4, Theorem 16].

Corollary 8. *Let $0 \leq n < m$ or $n = m = 1$, let $i > 0$ and let c be some natural number, then Σ^b_{n+i}-$\mathrm{L}^m\mathrm{IND} \vdash \mathcal{O}\mathrm{Ind}(2_n(|x|^c_m), \Pi^b_i)$ and Σ^b_{n+i}-$\mathrm{L}^m\mathrm{IND} \vdash \mathcal{O}\mathrm{Ind}(2_{n+1}(c \cdot |x|_{m+1}), \Pi^b_i)$.* $\square$

This establishes lower bounds on general dynamic ordinals. E.g., we obtain for $m > 0$:

$$\mathrm{DO}_{i+1}(\Sigma^b_{m+i}(\alpha)\text{-}\mathrm{L}^m\mathrm{Ind}) \quad \trianglerighteq \quad 2_m(O(|\,\mathrm{id}\,|_{m+1})) \ .$$

For upper bounds we will utilise translations to propositional proof systems, which then will be studied proof-theoretically. But first we have to specify our favourite propositional proof system.

5 The Proof System Σ^{qp}_i-LK

In the following we give a natural modification of the definition of language and formulas of Gentzen's propositional proof system LK. In the way we will describe it here, it is sometimes attributed as "Tait-style". 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 $\bigvee$ (conjunction and disjunction are both of unbounded finite arity), and auxiliary symbols like parentheses. Formulas are defined inductively: constants, atoms and negated atoms are formulas (they are called literals), and if Φ is a finite set of formulas, then $\bigwedge \Phi$ and $\bigvee \Phi$ are formulas, too. In general, negation is defined as an operation according to the de Morgan laws, i.e., $\neg\varphi$ denotes the formula obtained 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 $\mathrm{dp}(\bigvee \Phi)$ equals $1 + \max\{\mathrm{dp}(\varphi) \colon \varphi \in \Phi\}$.

In our setting, *cedents* $\Gamma, \Delta, \ldots$ are finite *sets* of formulas, not *sequences* as in [14], 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 obtained as derivable rules. LK consists of four inference rules: initial cedent rule, introduction rules for $\bigwedge$ and $\bigvee$, and cut-rule. We are going to define $\mathcal{C}$-LK where $\mathcal{C}$ denotes the set of permissable cut formulas.

Definition 9. We inductively define that Γ is $\mathcal{C}$-LK provable with height η, in symbols $\vdash^{\eta}_{\mathcal{C}} \Gamma$, for Γ a cedent, $\mathcal{C}$ a set of formulas and $\eta \in \mathbb{N}$. $\vdash^{\eta}_{\mathcal{C}} \Gamma$ holds if and only if one of the following four conditions is fulfilled:

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

($\bigwedge$) There is some $\bigwedge \Phi \in \Gamma$ and $\eta' < \eta$ such that $\vdash^{\eta'}_{\mathcal{C}} \Gamma, \varphi$ for all $\varphi \in \Phi$.

($\bigvee$) There is some $\bigvee \Phi \in \Gamma$ and $\varphi \in \Phi$ and $\eta' < \eta$ such that $\vdash^{\eta'}_{\mathcal{C}} \Gamma, \varphi$.

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

The formula φ in the application of the cut-rule is called the *cut-formula* of this inference.

In order to make our definition of Σ_i^{qp}-LK precise we have to define a fine structure on constant depth formulas.

Definition 10. Let S, t, i be in $\mathbb{N}$. We inductively define $\varphi \in \Sigma_i^{S,t}$ by the following clauses:

i) $\varphi \in \Sigma_0^{S,t}$ if and only if φ is a $\bigwedge$ or $\bigvee$ of at most t many literals.

ii) $\varphi \in \Sigma_{i+1}^{S,t}$ if and only if φ is in $\Sigma_i^{S,t} \cup \Pi_i^{S,t}$, or it has the form of a $\bigvee$ of at most S many formulas from $\Sigma_i^{S,t} \cup \Pi_i^{S,t}$.

iii) A formula is in $\Pi_i^{S,t}$, if and only if its negation is in $\Sigma_i^{S,t}$.

Now we are prepared to say what we mean by Σ_i^{qp}-LK. Here and in the following, the superscript "qp" stands for "quasi-polynomial".

Definition 11. Let $i \in \mathbb{N}$, let $f, \eta : \mathbb{N} \to \mathbb{N}$ be functions, and let $(\Gamma_n)_n$ be a sequence of tautological cedents.

We say that $(\Gamma_n)_n$ is (i, f)-LK (or (Σ_i, f)-LK) provable with height η, if and only if there is a sequence of subsets $\mathcal{C}_n \subseteq \Sigma_i^{f(n),\log(f(n))}$ of cardinality bounded by $f(n)$ such that Γ_n is $\mathcal{C}_n$-LK provable of height $\eta(n)$.

Then Σ_i^{qp}-LK denotes $(\Sigma_i, 2^{(\log n)^{O(1)}})$-LK, i.e. $(\Gamma_n)_n$ is Σ_i^{qp}-LK provable with height η iff there is a $c \in \mathbb{N}$ such that $(\Gamma_n)_n$ is $(i, 2^{(\log n)^c})$-LK provable with height η.

We will often abuse notation and write Γ_n is Σ_i^{qp}-LK provable with height $\eta(n)$, instead of $(\Gamma_n)_n$ is Σ_i^{qp}-LK provable with height η.

In the previous definition, we included a strange looking condition that the number of distinct cut-formulas is bounded, too. The reason is technical: during the computation of dynamic ordinals we will encounter LK derivations whose heights grow stronger than poly-logarithmically. For derivations with poly-logarithmic height we would not need such a condition as it would be fulfilled implicitly: a derivation, in which all cut-formulas are in $\Sigma_i^{2^{(\log n)^c},(\log n)^c}$, has the property that the fan-in to each node in the derivation tree is bounded by $2^{(\log n)^c}$. Hence, if the height of such a derivation tree is bounded by $(\log n)^c$, then the number of nodes in the tree is bounded by $2^{(\log n)^{2c}}$, and thus the number of different cut-formulas in the derivation has the same bound. This argument obviously fails if the heights of the derivation trees grow stronger than poly-logarithmically. Now, having a quasi-polynomial upper bound on the number of different cut-formulas is essential for the cut-reduction by switching method needed to compute the generalised dynamic ordinals. It should be said at this point, that this condition will be fulfilled by translations of bounded arithmetic derivations, hence we obtain a stronger result this way.

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

Proposition 12 (Structural Rule). *Assume $\eta \leq \eta'$, $\mathcal{C} \subseteq \mathcal{C}'$ and $\Gamma \subseteq \Gamma'$, then $\vdash_{\mathcal{C}}^{\eta} \Gamma$ implies $\vdash_{\mathcal{C}'}^{\eta'} \Gamma'$.*

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

Proposition 13 ($\bigwedge$-Inversion). *Assume $\vdash_{\mathcal{C}}^{\eta} \Gamma, \bigwedge \Phi$, then $\vdash_{\mathcal{C}}^{\eta} \Gamma, \varphi$ holds for all $\varphi \in \Phi$.*

Proposition 14 ($\bigvee$-Exportation). *Suppose $\vdash_{\mathcal{C}}^{\eta} \Gamma, \bigvee \Phi$ holds, then $\vdash_{\mathcal{C}}^{\eta} \Gamma, \Phi$.*

The proof of the next Lemma and Proposition follows the same pattern as the standard one which can be found e.g. in [2, 4].

Lemma 15 (Cut-Elimination Lemma). *Let $\varphi \in \Sigma_{i+1}^{S,t}$ and $\mathcal{C} \subseteq \Sigma_i^{S,t}$ such that $\mathcal{C}$ includes all $\Sigma_i^{S,t}$-sub-formulas and all negations of $\Pi_i^{S,t}$-sub-formulas of φ. If $\vdash_{\mathcal{C}}^{\eta_0} \Gamma, \varphi$ and $\vdash_{\mathcal{C}}^{\eta_1} \Delta, \neg\varphi$, then $\vdash_{\mathcal{C}}^{\eta_0+\eta_1} \Gamma, \Delta$.*

Proposition 16 (Cut-Elimination Theorem). *Let $\mathcal{C} \subseteq \Sigma_{i+1}^{S,t}$ be closed under sub-formulas and let $\mathcal{C}' := \mathcal{C} \cap (\Sigma_i^{S,t} \cup \Pi_i^{S,t})$. Then $\vdash_{\mathcal{C}}^{\eta} \Gamma$ implies $\vdash_{\mathcal{C}'}^{2^\eta} \Gamma$.*

We repeat the translation (also called embedding) of provability in $\mathrm{S}_2^i(\alpha)$, $\mathrm{T}_2^i(\alpha)$, and more general of $\Sigma_i^b(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND}$, to LK from [2, 4]. 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.

There exists a canonical translation due to Paris and Wilkie [18] from the language of bounded arithmetic to the language of LK (see [15, 9.1.1], or [2, 4]). 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 $\bigwedge$, respectively $\bigvee$, e.g. $[\![(\forall x \leq t)\varphi(x)]\!] = \bigwedge_{j \leq m_t} [\![\varphi(j)]\!]$. It follows that a formula $\varphi(x)$ from $\Sigma_i^b(\alpha)$ (with x being the only variable occurring free in φ) translates to $\left([\![\varphi(n)]\!]\right)_n$ in Σ_i^{qp}, i.e. there is some $c \in \mathbb{N}$ such that $[\![\varphi(n)]\!] \in \Sigma_i^{2^{(\log n)^c},(\log n)^c}$ for all $n \in \mathbb{N}$.

Remark 17. The last statement is not totally correct in the way it is stated, because, Δ_0^b formulas may have unbounded depth. If we want to be really precise we could proceed as follows: First we define a more restricted version of Σ_i^b and Π_i^b. E.g., we define $\hat{\Sigma}_1^b$ formulas to be of the form: one bounded existential quantifier followed by disjunctions of one sharply bounded universal quantifier followed by conjunctions of atomic formulas. It can be shown in weak theories of Bounded Arithmetic that Σ_1^b formulas are equivalent to $\hat{\Sigma}_1^b$ formulas. Hence we obtain an equivalent definition of our theories using the more restricted classes. Second, we let $\hat{\Sigma}_i^{S,t}$ be the stratification of propositional formulas corresponding to the restrictions $\hat{\Sigma}_i^b$. E.g., $\hat{\Sigma}_0^{S,t}$ are the formulas having at most two levels of fan-in t disjunctions. Then we obviously have that $\hat{\Sigma}_i^b$ formulas translate into $\hat{\Sigma}_i^{\mathrm{qp}}$-formulas. Now the translation of proofs in bounded arithmetic which we are going to describe will produce $\hat{\Sigma}_i^{\mathrm{qp}}$-LK-derivations, which finally can be transformed into Σ_i^{qp}-LK-derivations by merging two levels of connectives of the same type using

$$\vdash_{\mathcal{C}}^{h} \Gamma, \textstyle\bigvee_{i<n} (\bigvee \Phi_i) \quad \Rightarrow \quad \vdash_{\mathcal{C}}^{h} \Gamma, \bigvee \left(\bigcup_{i<n} \Phi_i\right)$$

and

$$\vdash_{\mathcal{C}}^{h} \Gamma, \textstyle\bigwedge_{i<n} (\bigwedge \Phi_i) \quad \Rightarrow \quad \vdash_{\mathcal{C}}^{h} \Gamma, \bigwedge \left(\bigcup_{i<n} \Phi_i\right) \ .$$

For notational simplicity we will assume in this Section that Δ_0^b formula have the form one sharply bounded quantifier followed by an atomic formula. Assuming this, the above statement is correct.

The same proofs as in [2, 4] also show the following Theorem, which is here formulated using Σ_i^{qp}-LK.

Theorem 18. *Let $\varphi(x)$ be a formula in the language of bounded arithmetic, in which at most the variable x occurs free.*

i) If $\mathrm{S}_2^i(\alpha) \vdash \varphi(x)$, *then* $[\![\varphi(n)]\!]$ *has some* Σ_i^{qp}-LK *derivation of height* $O\left(\log^{(2)} n\right)$.

ii) If $\mathrm{T}_2^i(\alpha) \vdash \varphi(x)$, *then* $[\![\varphi(n)]\!]$ *has some* Σ_i^{qp}-LK *derivation of height* $(\log n)^{O(1)}$.

iii) If $\Sigma_i^b(\alpha)$-$\mathrm{L}^m\mathrm{IND} \vdash \varphi(x)$, *then* $[\![\varphi(n)]\!]$ *has some* Σ_i^{qp}-LK *derivation of height* $O\left(\log^{(m+1)} n\right)$. □

Combining this Theorem with the Cut-Elimination Theorem we obtain

Corollary 19. *Let $\varphi(x)$ be a formula in the language of bounded arithmetic, in which at most the variable x occurs free.*

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

ii) If $\Sigma_{m+i+1}^b(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND} \vdash \varphi(x)$, *then* $[\![\varphi(n)]\!]$ *is* Σ_i^{qp}-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_i^{qp}-LK *provable.* □

Height restricted proof systems have been subject of a technical report [5], which in particular covers the content of the next two sections. It is the second part of the previous Corollary where the technical condition discussed after Definition 11 comes into play. For example, if $m = 1$ then the resulting heights are of size $2^{(\log\log n)^c}$ which grow stronger than poly-logarithmically in general. Hence, having the additional restriction on the number of cut-formulas is a proper assertion, which is fulfilled as we are considering translations of bounded arithmetic derivations.

6 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 heights, as seen in the previous section. Later we want to show that the translations of the order induction principles need certain heights 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 19 we

cannot apply the Cut-Elimination Theorem any further, as this would result in upper bounds on heights which grow too fast.

At this point, the elimination of cuts, which is necessary in our proof of lower bounds, needs a different cut-elimination technique which we call cut-reduction by switching. It relies on methods from boolean complexity, i.e. Håstad's Switching Lemmas [10, 11]. In [14] such boolean complexity techniques are successfully applied to reduce the complexity of Σ_i^{qp}-LK refutations. We will follow [9] where the same approach is used to reduce the complexity of oracle computations related to definable functions in bounded arithmetic. 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.

In order to formulate cut-reduction by switching, we need some notation. Our logarithms are always base 2.

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

$$B_i(m) = \{p_{x,y_1,\ldots,y_i} \colon x, y_1, \ldots, y_i < m\} \ .$$

The cardinality of $B_i(m)$ is m^{i+1}. We shall henceforth use $\vec{y}$ as an abbreviation of $y_1, \ldots, y_i$ or $y_1, \ldots, y_{i-1}$, 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, if and only if 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 if and only if its negation is Σ_1^t, and it is Δ_1^t if and only if it is equivalent to both Σ_1^t and Π_1^t. A formula φ is *hereditarily* Δ_1^t, denoted by $\varphi \in \mathbf{\Delta}_1^t$, if and only if every sub-formula of φ is Δ_1^t. We inductively define for $i \geq 0$:

$$\begin{aligned}
\varphi \in \Pi_i^{S,t} &\Leftrightarrow \neg\varphi \in \Sigma_i^{S,t} \\
\varphi \in \Sigma_0^{S,t} &\Leftrightarrow \varphi \in \mathbf{\Delta}_1^t \\
\varphi \in \Sigma_1^{S,t} &\Leftrightarrow \varphi \equiv \bigvee_{j<w} \varphi_j \text{ and } \varphi_j \in \mathbf{\Delta}_1^t \text{ for all } j < w \\
\varphi \in \Sigma_{i+2}^{S,t} &\Leftrightarrow \varphi \equiv \bigvee_{j<w} \varphi_j \text{ and } w \leq S \text{ and } \varphi_j \in \Pi_{i+1}^{S,t} \text{ for all } j < w
\end{aligned}$$

Observe that for the definition of $\Sigma_1^{S,t}$, we do *not* assume $w \leq S$!

(3) We define for $x < m$ some general $\Sigma_i^{m,1}$-formulas $D_{i,m}(x)$ in m^i variables from $B_i(m)$. They compute so-called Sipser functions [11] and are

defined by

$$D_{i,m}(x) \quad = \quad \bigwedge_{y_1<m} \quad \bigvee_{y_2<m} \quad \dots \quad Q^{i-1}_{y_{i-1}<m} \quad Q^{i}_{y_i<m} \quad p_{x,\vec{y}}$$

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

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

Theorem 20 (Cut-Reduction by Switching). *Let $i \in \mathbb{N}$ and $\epsilon \in \mathbb{R}$ with $i \geq 1$ 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 $\mathcal{C}_m \subset \Sigma_i^{S,t}$ with $|\mathcal{C}_m| \leq S$. Furthermore, assume that $B_m\big[p_x \leftarrow D_{i,m}(x) \colon x < m\big]$ 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) $B_m\big[p_x \leftarrow 0 \colon x \in Q\big]$ *is* Δ_1^t*-LK provable with height* η_m*.*

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

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

$$(B_i(m))_{(x,y_1,\dots,y_{i-1})} \quad := \quad \{p_{x,y_1,\dots,y_{i-1},z} \colon z < m\}$$

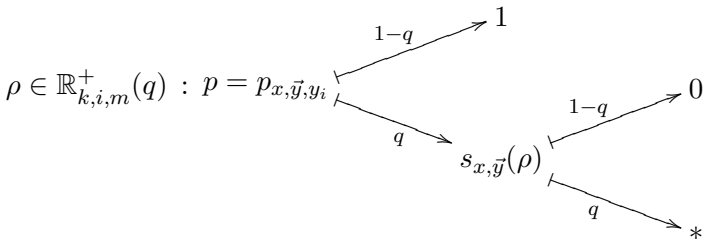
for $(x, y_1, \dots, y_{i-1}) \in [m]^i$.

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

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

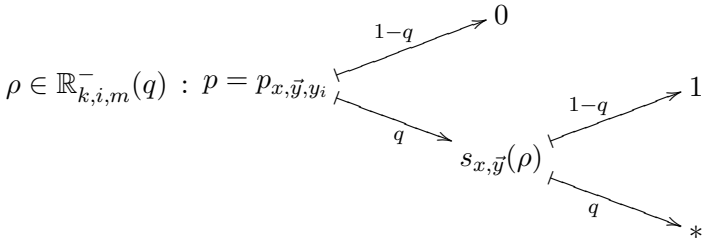
We should think of $\rho(p) = 0$ or $\rho(p) = 1$ as p *is replaced by* 0 or 1 respectively, and of $\rho(p) = *$ as p *is left unchanged*. Alternatively, we can think of ρ as a partial map going from $B_i(m)$ to $\{0, 1\}$.

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



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



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

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

(9) The following lemma is Håstad's second switching lemma, see [11].

Lemma 21 (Håstad [11]). *Let $i \geq 1$ and $\nu \in \{+,-\}$. Let φ be a $\Sigma^{S,t}_{i+1}$-formula with variables from $B_i(m)$ and $0 < q < 1$. Then*

$$\Pr_{\rho \in \mathbb{R}^v_{k,i,m}(q)} \left[\varphi\restriction_{\mathrm{g}\rho} \notin \Sigma^{S,t}_i \right] \leq S^i \cdot (6qt)^t \ .$$

I.e., the probability of a randomly chosen ρ from $\mathbb{R}^v_{k,i,m}(q)$ that the formula $\varphi\restriction_{\mathrm{g}\rho}$ 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 $D_{i,m}(x)$ have to be modified. We define $\bar{D}_{i,m}(x)$ for every $x < m$ with variables from $B_i(m)$. They compute modified Sipser functions (cf. [11, 9]) and are defined by

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

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

(11) The next lemma is also due to Håstad [11]. We repeat essentially the version stated by Buss and Krajíček [9].

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

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

$$\Pr_{\rho \in \mathbb{R}^{v(i)}_{k,i,m}(q)} \Big[\bar{D}_{i-1,m}(x) \not\subseteq \bar{D}_{i,m}(x) \restriction_{\mathrm{g}\rho} \Big] \leq \frac{1}{3} m^{-2} \ .$$

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

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

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

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 $\restriction_{\mathrm{g}\rho}$ is at most $\frac{1}{6}m^{-2}$.
For $R \subseteq [m]$ with $|R| \geq m$ we have

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

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) Utilising this we obtain the following lemmas which immediately proof our Cut-Reduction by Switching Theorem 20. For the rest of this section 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 $B_0(m)$.

Lemma 23. *Let $i \geq 1$, let $f : \mathbb{N} \to \mathbb{N}$ be some function, and let $\mathcal{C}_m \subset \Sigma^{S,t}_{i+1}$ be given such that $|\mathcal{C}_m| \leq S$ and $B_m\big[p_x \leftarrow \bar{D}_{i+1,m}(x) \colon x < m\big]$ 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 $\mathcal{C}'_m \subset \Sigma^{S,t}_i$ such that $|\mathcal{C}'_m| \leq S$ and $B_m\big[p_x \leftarrow \bar{D}_{i,m}(x) \colon x < m\big]$ is $\mathcal{C}'_m$-LK provable with height $f(m)$.

Lemma 24. *Let $f : \mathbb{N} \to \mathbb{N}$ be some function, and let $\mathcal{C}_m \subset \Sigma_1^{S,t}$ be given such that $|\mathcal{C}_m| \leq S$ and $B_m\big[p_x \leftarrow \bar{D}_{1,m}(x) \colon x < m\big]$ 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) $B_m\big[p_x \leftarrow 0 \colon x \in Q\big]$ *is* Δ_1^t-LK *provable with height* $f(m)$*.*

7 Lower bounds on heights of Σ_i^{qp}-LK-proofs of order induction

In this section we will prove lower bounds on heights of Σ_i^{qp}-LK proofs of the order induction principle for some particular Σ_i^{qp}-property (given by the Sipser functions $D_{i,m}(x)$). This will be obtained by applying the Cut-Reduction by Switching Theorem from the previous Section and the lower bound theorem for Δ_1^t-resolution proofs of the order induction principle to be proven next. This lower bound is also called "Boundedness Theorem" in the setting of ordinal analysis.

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

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

(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 minimisation: if some variables among $p_0, \ldots, p_{m-1}$ are false then there is one with minimal index. It is the translation of our previously defined $\mathcal{L}_{\mathrm{BA}}$-formula $\mathcal{O}\mathrm{Ind}(m, \alpha)$ to LK.

Theorem 25 (Boundedness). $\big|\!\!\frac{\eta}{\Delta_1^t}\ \mathcal{O}\mathrm{Ind}(n) \quad \Rightarrow \quad n \leq \eta \cdot t$.

We will give a detailed proof of this Theorem in the next subsection. But before we do this we utilise the Boundedness Theorem. The complexity of the order induction principle is extended by replacing variables p_x by the Sipser function $D_{i,m}(x)$ from the previous section. The next theorem states the lower bound for Σ_i^{qp}-LK derivations of the extended order induction principle. With $\mathrm{rng}(f)$ we will denote the range of a number-theoretic function f.

Theorem 26. *Let $i \in \mathbb{N}$ with $i \geq 1$. Let $f, \eta : \mathbb{N} \to \mathbb{N}$ be some number-theoretic functions such that $\eta(n) = (\log n)^{\Omega(1)}$. Assume that $\mathcal{O}\mathrm{Ind}(f(n))\big[p_x \leftarrow \neg D_{i,f(n)}(x) \colon x < f(n)\big]$ is Σ_i^{qp}-LK provable with height $\eta(n)$. Then, $\eta(n) = f(n)^{\Omega(1)}$, or, equivalently, $f(n) = \eta(n)^{O(1)}$.*

Proof. Assume for the sake of contradiction that the assumptions of the Theorem are satisfied, but $f(n) \neq \eta(n)^{O(1)}$. In particular, $\mathrm{rng}(f)$ must be unbounded.

By assumption, we have that $\mathcal{O}\mathrm{Ind}(f(n))\big[p_x \leftarrow \neg D_{i,f(n)}(x) \colon x < f(n)\big]$ is Σ_i^{qp}-LK provable with height $\eta(n)$. This means that there is some $c \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ we can fix a set of formulas $\bar{\mathcal{C}}_n$ with the following properties: let $\bar{t} = \bar{t}(n) = (\log n)^c$ and $\bar{S} = \bar{S}(n) = 2^{\bar{t}}$, then $\bar{\mathcal{C}}_n \subseteq \Sigma_i^{\bar{S},\bar{t}}$, $|\bar{\mathcal{C}}_n| \leq \bar{S}$ and $\mathcal{O}\mathrm{Ind}(f(n))\big[p_x \leftarrow \neg D_{i,f(n)}(x) \colon x < f(n)\big]$ is $\bar{\mathcal{C}}_n$-LK provable with height $\eta(n)$. By assumption $\log n = \eta(n)^{O(1)}$, hence there is some d and $N_0 \in \mathbb{N}$ such that $\log n \leq \eta(n)^d$ for $n \geq N_0$. W.l.o.g., we can choose $c \cdot d > 1$.

We will construct some infinite subset M of $\mathrm{rng}(f)$ which can be used to apply the Cut-Elimination by Switching Theorem. Let m_0 be any number. We will construct some $m_1 > m_0$ which we will put into the set M. Fix some $n_0 \geq N_0$ with $(\log n_0)^{4c} \geq m_0$. As $f(n) \neq \eta(n)^{O(1)}$ there must be some $n_1 > n_0$ satisfying $f(n_1) > \eta(n_1)^{d \cdot 4 \cdot c}$. Let $m_1 := f(n_1)$, then $m_1 > \eta(n_1)^{d \cdot 4 \cdot c} \geq (\log n_1)^{4c} \geq m_0$. Thus $(\log n_1)^c \leq m_1^{\frac{1}{4}}$ and $m_0 < m_1$. Hence $\bar{\mathcal{C}}_{n_1} \subseteq \Sigma_i^{S,t}$ and $|\bar{\mathcal{C}}_{n_1}| \leq S$ for $t := m_1^{\frac{1}{4}}$ and $S := 2^t$. Put m_1 into the set M and define $\mathcal{C}_{m_1} := \bar{\mathcal{C}}_{n_1}$ and $\eta_{m_1} := \eta(n_1)$. Go on defining $m_2, m_3, \ldots$ in the same fashion.

Then, the prerequisites of the Cut-Reduction by Switching Theorem are satisfied, and we obtain some large $m \in M$, some set $Q \subset [m]$ not too big (i.e. $|[m] \backslash Q| \geq \sqrt{m \cdot \log m} \geq \sqrt{m}$) and a Δ_1^t-LK derivation of $\mathcal{O}\mathrm{Ind}(m)[p_x \leftarrow 1 \colon x \in Q]$ of height η_m. By pruning and renaming of variables this can be transformed into a Δ_1^t-LK derivation of $\mathcal{O}\mathrm{Ind}(m - |Q|)$ of height η_m, hence the Boundedness Theorem yields $m - |Q| \leq \eta_m \cdot t = \eta_m \cdot m^{\frac{1}{4}}$, which together with the largeness condition on Q rewrites to $\eta_m \geq m^{\frac{1}{4}}$. By construction of M there is some n such that $\eta(n) = \eta_m$ and $m = f(n) > \eta(n)^{d \cdot 4 \cdot c}$, contradicting the previously obtained $m \leq \eta(n)^4$, as $c \cdot d > 1$. □

7.1 The proof of the Boundedness Theorem

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

$$\vdash_{\bullet}^{\eta} \mathcal{O}\mathrm{Ind}(n) \quad \Rightarrow \quad n \leq \eta \cdot t \ .$$

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

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 $M \vDash \varphi$ if and only if $\varphi[M]$ 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^-:

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

Definition 27. For a formula φ and a truth value $\nu \in \{0,1\}$ we define that (M^+, M^-) fixes φ to ν, if and only if 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, if and only if (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^- can be chosen to respect any given satisfying assignment of φ:

Lemma 28. *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

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

Then the assertion follows. □

The following Lemma is the main technical part for proving the Boundedness Theorem 25. 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 29. $\vdash^{\eta}_{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), p_m \Rightarrow m < \eta \cdot t$.

Proof of the Boundedness Theorem 25. Assume $\vdash^{\eta}_{\bullet} \mathcal{O}\mathrm{Ind}(n)$. By applying first $\bigvee$-Exportation and then $\bigwedge$-Inversion from Section 5 we obtain $\vdash^{\eta}_{\bullet} \neg\, \mathcal{O}\mathrm{Prog}(n), p_{n-1}$. 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

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

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 $\{a\colon a < \overline{\mathrm{en}}_M(\gamma)\} \cup M$.

We will construct by recursion on l sets $\Delta_l \subseteq \mathfrak{Δ}_1^t$, $M_l^+, M_l^- \subseteq \mathbb{N}$ for $l = \eta, \ldots, 0$ satisfying the property $\mathcal{G}(l, \Delta_l, M_l^+, M_l^-)$ given by

i) $\vdash_\bullet^l \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_l$.

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 $\Delta_0 \subseteq \mathfrak{Δ}_1^t$, $M_0^+, M_0^- \subseteq \mathbb{N}$ which satisfy $\mathcal{G}(0, \Delta_0, M_0^+, M_0^-)$, then $\mathcal{G}(0, \Delta_0, M_0^+, M_0^-)$ **i)** shows $\vdash_\bullet^0 \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_0$, 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 $\Delta_{l+1} \subseteq \mathfrak{Δ}_1^t$, $M_{l+1}^+, M_{l+1}^- \subseteq \mathbb{N}$ 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 $\vdash_\bullet^{l+1} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}$. 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 $\psi \in \mathfrak{Δ}_1^t$ and $M^+, M^- \subseteq \mathbb{N}$ satisfying the following property:

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

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) Utilising **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, $\mathcal{R}^{l\cdot t}(M_l^+) \not\models \Delta_{l+1}$, 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 $\vdash_\bullet^{l+1} \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}$. 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 $\vdash_\bullet^l \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \varphi_j$ for all $j < J$. By induction hypothesis $\mathcal{G}(l+1, \Delta_{l+1}, M_{l+1}^+, M_{l+1}^-)$ **iv)** we have that $\mathcal{R}^* \not\models \varphi$. Thus, there is some $j_0 < J$ such that $\mathcal{R}^* \not\models \varphi_{j_0}$.

Let $\psi := \varphi_{j_0}$, then $\psi \in \Delta_1^t$ [$\Rightarrow$ **I)**]. By Lemma 28 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 $\vdash_\bullet^l \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \varphi_{j_0}$ 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 $\mathcal{R}^* \not\models \varphi$, thus also $\mathcal{R}^* \not\models \varphi_{j_0}$. 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

$$\vdash_\bullet^l \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \left(\bigwedge_{y<x} p_y\right) \wedge \neg p_x \ .$$

A) Assume, there is some $y < x$ such that $y \notin \mathcal{R}^{l\cdot t}(M_{l+1}^+)$. By $\bigwedge$-Inversion we obtain $\vdash_\bullet^l \neg\, \mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, p_y$. 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 $\mathcal{R}^{l\cdot t}(M_l^+) \not\models \Delta_l$ [$\Rightarrow$ $\mathcal{G}(l, \Delta_l, M_l^+, M_l^-)$ **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 $\vdash^l_\bullet \neg\,\mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \neg p_x$. Let $\psi := \neg p_x$ [$\Rightarrow$ **I**)], $M^+ := \{x\}$ and $M^- := \emptyset$ [$\Rightarrow$ **II**), **III**), **IV**), **V**)].

(Cut) There is some $\varphi \in \Delta_1^t$ such that $\vdash^l_\bullet \neg\,\mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \varphi$ and $\vdash^l_\bullet \neg\,\mathcal{O}\mathrm{Prog}(n), \Delta_{l+1}, \neg\varphi$. W.l.o.g. we may assume $\mathcal{R}^* \not\models \varphi$. The same argumentation as in the $\bigwedge$-case yields the assertion.

□

8 Generalised dynamic ordinals revisited

We have now collected all tools which are needed to compute the missing upper bounds on generalised dynamic ordinals. Our strategy will be to translate a $\Sigma^b_{m+i}(\alpha)$-L^{m}IND-proof of $\mathcal{O}\mathrm{Ind}(t(x), \Pi^b_i)$ to Σ^{qp}_i-LK, and then use the result on lower bounds of the order induction principle, Theorem 26, to obtain tight upper bounds on generalised dynamic ordinals.

For the following considerations fix some $i, m \in \mathbb{N}$ with $m > 0$ and some

$$f \in \mathrm{DO}_{i+1}(\Sigma^b_{m+i}(\alpha)\text{-L}^m\mathrm{IND}) \ .$$

First, we define some general $\Pi^b_i(\alpha)$-formula $A^{\alpha,i}(a, x)$, which is translated by the Paris-Wilkie translation to the Sipser function $D_{i,a}$ as defined before. $A^{\alpha,i}(a, x)$ is given by the formula

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

where either Q^{i-1} or Q^i is $\forall$, depending on whether i is even or odd, respectively, and the other is $\exists$. Here, $\langle z_1, \ldots, z_j\rangle$ denotes some sequence coding function expressible in the language of bounded arithmetic. Then, the definition of DO_{i+1} yields that there is some term t such that $f = \lambda x.t(x)$ and

$$\Sigma^b_{m+i}(\alpha)\text{-L}^m\mathrm{IND} \vdash (\forall x)\,\mathcal{O}\mathrm{Ind}(t, \neg A^{\alpha,i}(t, .)) \ .$$

Utilising Theorem 19 shows that there is some $c \geq 1$ such that eventually

$$[\![\mathcal{O}\mathrm{Ind}(t(n), \neg A^{\alpha,i}(t(n), .))]\!]$$

is Σ^{qp}_i-LK provable with height $2_{m-1}\left((\log^{(m)} n)^c\right)$. By identifying $p_{\langle x,\vec{y}\rangle}$ with $p_{x,\vec{y}}$, we see that these derivations transform to Σ^{qp}_i-LK proofs of

$$\mathcal{O}\mathrm{Ind}(t(n))\big[p_x \leftarrow \neg D_{i,t(n)}(x) \colon x < t(n)\big]$$

of height $2_{m-1}\left((\log^{(m)} n)^c\right)$.

Now we are in the situation that we can apply the Lower Bound Theorem 26, because $2_{m-1}\left((\log^{(m)} n)^c\right) = (\log n)^{\Omega(1)}$. Hence, we obtain that

$$f(n) \quad = \quad t(n) \quad = \quad 2_{m-1}\left((\log^{(m)} n)^c\right)^{O(1)} \quad = \quad 2_m(O(\log^{(m+1)} n)) \ .$$

Together with Corollary 8, this shows:

Theorem 30. *Let $m > 0$. The $i+1$ generalised dynamic ordinal of the theory $\Sigma^b_{m+i}(\alpha)$-L^mIND can be described as:*

$$\mathrm{DO}_{i+1}(\Sigma^b_{m+i}(\alpha)\text{-}L^m Ind) \quad \equiv \quad 2_m(O(|\,\mathrm{id}\,|_{m+1})) \ .$$

Hence we have for $i > 0$:

$$\begin{array}{lcll} \mathrm{DO}_i(\mathrm{T}^i_2(\alpha)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_2)) & \equiv \quad \mathrm{DO}_i(\mathrm{S}^{i+1}_2(\alpha)) \\ \mathrm{DO}_i(\mathrm{S}^i_2(\alpha)) & \equiv & 2_1(O(|\,\mathrm{id}\,|_2)) & \\ \mathrm{DO}_i(\mathrm{sR}^{i+1}_2(\alpha)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_3)) & \end{array}$$

We also compare definable multivalued functions of unrelativised theories with the generalised dynamic ordinals of their relativised companions.

Theorem 31. *Let $i \geq 0$. For any theory T from the infinite list*
T^{i+1}_2, S^{i+2}_2, S^{i+1}_2, $\mathrm{sR}^{i+2}_2 (= \Sigma^b_{i+2}\text{-L}^2\text{IND})$, $\Sigma^b_{i+3}\text{-L}^3\text{IND}, \ldots$
we have:
A multivalued function f is Σ^b_{i+2}-definable in T, if and only if $f \in \mathrm{FP}^{\Sigma^b_{i+1}}(\mathrm{wit}, \log(\mathrm{DO}_{i+1}(T(\alpha))))$. □

This indicates that generalised dynamic ordinals do in fact also characterise the *computational complexity* of bounded arithmetic theories.

References

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

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

[3] Arnold Beckmann. A note on universal measures for weak implicit computational complexity. In Matthias Baaz and Andrei Voronkov, editors, *Proccedings of the 9th International Conference, LPAR 2002 (Tbilisi)*, Lecture Notes in Computer Science, pages 53–67, Berlin, 2002. Springer-Verlag.

[4] Arnold Beckmann. Dynamic ordinal analysis. *Arch. Math. Logic*, 42:303–334, 2003.

[5] Arnold Beckmann. Height restricted constant depth LK. Research Note Report TR03-034, Electronic Colloquium on Computational Complexity, 2003. http://www.eccc.uni-trier.de/eccc-reports/2003/TR03-034/.

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

[7] Samuel R. Buss. Axiomatizations and conservation results for fragments of bounded arithmetic. In Wilfried Sieg, editor, *Proceedings of the workshop held at Carnegie Mellon University, Pittsburgh, Pennsylvania, June 30–July 2, 1987*, volume 106 of *Contemporary Mathematics*, pages 57–84, Providence, RI, 1990. American Mathematical Society.

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

[9] 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.

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

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

[12] Jan Johannsen. A note on sharply bounded arithmetic. *Arch. Math. Logik Grundlag.*, 33:159–165, 1994.

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

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

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

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

[17] Daniel Leivant. Substructural termination proofs and feasibility certification. In *Proceedings of the 3rd Workshop on Implicit Computational Complexity (Aarhus)*, pages 75–91, 2001.

[18] Jeff B. Paris and Alex J. Wilkie. Counting problems in bounded arithmetic. In Carlos Augusto di Prisco, editor, *Methods in Mathematical Logic*, number 1130 in Lect. Notes Math., pages 317–340, Heidelberg/New York, August 1985. Springer.

[19] Wolfram Pohlers. *Proof theory*, volume 1407 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1989. An introduction.

[20] Chris Pollett. Structure and definability in general bounded arithmetic theories. *Ann. Pure Appl. Logic*, 100(1-3):189–245, 1999.

[21] Gaisi Takeuti. RSUV isomorphism. In Peter Clote and Jan Krajíček, editors, *Arithmetic, proof theory, and computational complexity*, Oxford Logic Guides, pages 364–86. Oxford University Press, New York, 1993.

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

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