Resolution Refutations and Propositional Proofs with Height-Restrictions

Arnold Beckmann*

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

Abstract. Height restricted resolution (proofs or refutations) is a natural restriction of resolution where the height of the corresponding proof tree is bounded. Height restricted resolution does not distinguish between tree- and sequence-like proofs. We show that polylogarithmic-height resolution is strongly connected to the bounded arithmetic theory $S_2^1(\alpha)$. We separate polylogarithmic-height resolution from quasi-polynomial size tree-like resolution.
Inspired by this we will study infinitely many sub-linear-height restrictions given by functions $n \mapsto 2_i\left((\log^{(i+1)} n)^{O(1)}\right)$ for $i \geq 0$. We show that the resulting resolution systems are connected to certain bounded arithmetic theories, and that they form a strict hierarchy of resolution proof systems. To this end we will develop some proof theory for height restricted proofs.

Keywords: Height of proofs; Length of proofs; Resolution refutation; Propositional calculus; Frege systems; Order induction principle; Cut elimination; Cut introduction; Bounded arithmetic.

MSC: Primary 03F20; Secondary 03F07, 68Q15, 68R99.

1 Introduction

In this article, we will focus on two approaches to the study of computational complexity classes, *propositional proof systems* and *bounded arithmetic theories.* Cook and Reckhow in their seminal paper [8] have shown that the existence of "strong" *propositional proof systems* in which all tautologies have proofs of polynomial size is tightly connected to the NP vs. co-NP question. This has been the starting point for a currently very active area of research where one tries to separate all kinds of proof systems by proving super-polynomial lower bounds.

Theories of bounded arithmetic have been introduced by Buss in [6]. 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. [6, 12]). A hierarchy of bounded formulas, Σ_i^b,

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

and of theories $S^1_2 \subseteq T^1_2 \subseteq S^2_2 \subseteq T^2_2 \subseteq S^3_2 \ldots$ has been defined (cf. [6]). The class of predicates definable by Σ^b_i formulas is precisely the class of predicates in the ith level Σ^p_i of the polynomial hierarchy. The Σ^b_i-definable functions of S^i_2 form precisely the ith level $\square^p_i$ of the polynomial hierarchy of functions, which consists of the functions which are polynomial time computable with an oracle from Σ^p_{i-1}.

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 hierarchy PH collapses – the P=?NP problem is a sub-problem of this. The hierarchy of bounded arithmetic collapses if and only if PH collapses provably in bounded arithmetic (cf. [14, 7, 18]). The case of relativized complexity classes and theories behaves completely differently. The existence of an oracle A is proven in [1, 17, 9], such that the polynomial 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 $T^i_2(\alpha) \neq S^{i+1}_2(\alpha)$ [14]. Here, the relativized theories $S^i_2(\alpha)$ and $T^i_2(\alpha)$ result from S^i_2 and T^i_2, resp., by adding a free set variable α and the relation symbol $\in$. Similarly also, $S^i_2(\alpha) \neq T^i_2(\alpha)$ is proven in [10], and separation results for further relativized theories (dubbed $\Sigma^b_n(\alpha)$-$\mathrm{L}^m\mathrm{IND}$) are proven in [16]. Independently of these, and with completely different methods, we have shown separation results for relativized theories of bounded arithmetic using as 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. For example, Paris and Wilkie have shown in [15] that the study of constant-depth propositional proofs is relevant to bounded arithmetic. In particular, the following translations are known for the first two levels of bounded arithmetic $S^1_2(\alpha)$ and $T^1_2(\alpha)$ (a definition of these theories can be found e.g. in [6, 12]). Krajíček has observed (cf. [13, 3.1]) that provability in $T^1_2(\alpha)$ translates to *quasi-polynomial*[1] *size sequence-like* resolution proofs. Furthermore, it is known that provability in $S^1_2(\alpha)$ translates to *quasi-polynomial size tree-like* resolution proofs.[2] It is also known that quasi-polynomial size tree-like resolution proofs are separated from quasi-polynomial size sequence-like resolution proofs (the best known separation can be found in [5]).

An examination of dynamic ordinal analysis (cf. [2, 3]) shows that provability in $S^1_2(\alpha)$ can even be translated to *polylogarithmic*[3]*-height* resolution proofs. We will prove that polylogarithmic-height resolution proofs form a proper sub-system of quasi-polynomial size tree-like resolution proofs. Hence we will obtain the relationships represented in Fig. 1.

In this article we pick up this observation and examine height restricted propositional proofs and refutations. To this end we develop some proof theory for height restricted propositional proofs. This includes several cut elimination

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

[2] The author of this paper could not find a reference for this, but it follows by similar calculations as in [13, 3.1].

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

$$\begin{array}{rl} S^1_2(\alpha) \hookrightarrow & \text{polylogarithmic-height resolution} \\ & \qquad\qquad\qquad\qquad \rotatebox{-90}{$\subsetneq$} \\ & \text{quasi-polynomial-size tree-like resolution} \\ & \qquad\qquad\qquad\qquad \rotatebox{-90}{$\subsetneq$} \\ T^1_2(\alpha) \hookrightarrow & \text{quasi-polynomial-size sequence-like resolution} \end{array}$$

Fig. 1. Translation of $S^1_2(\alpha)$ and $T^1_2(\alpha)$ to resolution

results, and the following so called boundedness theorem (cf. [4]): Any resolution proof of the order induction principle for n, i.e. for the natural ordering of numbers less than n, must have height at least n. On the other hand there are tree-like resolution proofs of the order induction principle for n which have height linear in n and size quadratic in n. This gives us the separation of polylogarithmic-height resolution from quasi-polynomial size tree-like resolution. In particular, we obtain simple proofs of separation results of relativized theories of bounded arithmetic which reprove some separation results mentioned before.

This way we will study infinitely many sub-linear-height restrictions given by functions $n \mapsto 2_i\left((\log^{(i+1)} n)^{O(1)}\right)$ for $i \geq 0$. We will show that the resulting resolution systems are connected to certain bounded arithmetic theories $\Sigma^b_{i+1}(\alpha)$-L^{i+1}IND (a definition of these theories can be found e.g. in [2, 3]), and that they form a strict hierarchy of resolution proof systems utilizing the order induction principle.

The paper is organized as follows: In the next section we recall the definition of the proof system LK. We introduce an inductively defined provability predicate for LK which measures certain parameters of proofs. Furthermore, we introduce the order induction principle for n and give suitable resolution proofs of height linear in n and size quadratic in n. We recall the lower bound (linear in n) to the height of resolution *proofs* of the order induction principle for n, and we give a proof for the lower bound to the height of resolution *refutations* of that principle. In section 3 we develop some proof theory for height restricted propositional proofs. This includes several cut elimination techniques. We further recall the translation from bounded arithmetic to height restricted resolution from [2]. We conclude this section by stating the relationship between resulting height restricted resolution systems. The last section gives an attemp to prove simulations between height restricted LK systems with different so called Σ-depths. The Σ-depth of an LK-proof restricts the depth of principle formulas in cut-inferences. Cut elimination lowers the Σ-depth but raises the height of proofs. For the opposite effect (shrinking height by raising Σ-depth) we introduce some form of cut-introduction. We end this section by some final remarks and open problems.

2 The Proof System LK

We recall the definition of language and formulas of LK from [11]. 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 $\bigvee \Gamma$. Cedents are also called *clauses* (in case of resolution). 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: cut-rule, initial cedent rule, and introduction rules for $\bigwedge$ and $\bigvee$. We define a derivability predicate $\mathcal{A} \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$ meaning that there is a proof of Γ which may use axioms from $\mathcal{A}$ such that the height of the proof-tree is bounded by η, the size ($=$ number of occurrences of cedents in it) is bounded by σ, and the number of formulas $|\Gamma|$ of every cedent Γ in it is bounded by λ.

Definition 1. *We inductively define* $\mathcal{A} \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$ *for* $\mathcal{A}$ *is a set of cedents consisting only of literals,* Γ *a cedent,* $\mathcal{C}$ *a set of formulas and natural numbers* η, σ, λ. $\mathcal{A} \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$ *holds iff*

(Init) $\eta \geq 0$, $\sigma \geq 1$, $\lambda \geq |\Gamma|$ *and* Γ *is an initial cedent, i.e.* $1 \in \Gamma$, *or* $x, \neg x \in \Gamma$ *for some variable* x, *or there is some* $\Gamma' \subseteq \Gamma$ *such that* $\Gamma' \in \mathcal{A}$.

($\bigwedge$) *There are some* $\bigwedge_{i<I} \varphi_i \in \Gamma$, $\eta' < \eta$, $\sigma_i \in \mathbb{N}$ *for* $i < I$ *with* $\sum_{i<I} \sigma_i < \sigma$ *such that* $\mathcal{A} \mathrel{|}\!\frac{\eta',\sigma_i,\lambda}{\mathcal{C}}\, \Gamma, \varphi_i$ *for all* $i < I$.

($\bigvee$) *There are some* $\bigvee_{i<I} \varphi_i \in \Gamma$, $i_0 < I$, $\eta' < \eta$ *and* $\sigma' < \sigma$ *such that* $\mathcal{A} \mathrel{|}\!\frac{\eta',\sigma',\lambda}{\mathcal{C}}\, \Gamma, \varphi_{i_0}$.

(Cut) *There are some* $\varphi \in \mathcal{C}$, $\eta' < \eta$, $\sigma_0 + \sigma_1 < \sigma$ *such that* $\mathcal{A} \mathrel{|}\!\frac{\eta',\sigma_0,\lambda}{\mathcal{C}}\, \Gamma, \varphi$ *and* $\mathcal{A} \mathrel{|}\!\frac{\eta',\sigma_1,\lambda}{\mathcal{C}}\, \Gamma, \neg\varphi$.

Parameters which are unimportant are often dropped (if possible) or replaced by $-$. *E.g.,* $\mathcal{A} \mathrel{|}\!\frac{\eta}{\mathcal{C}}\, \Gamma$ *abbreviates* $(\exists\sigma, \lambda)\mathcal{A} \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$, *and* $\mathcal{A} \mathrel{|}\!\frac{-,\sigma}{\mathcal{C}}\, \Gamma$ *abbreviates* $(\exists\eta, \lambda)$ $\mathcal{A} \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$. $\mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$ *means* $\emptyset \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \Gamma$.

If $\mathcal{A} \mathrel{|}\!\frac{\eta,\sigma,\lambda}{\mathcal{C}}\, \emptyset$ then we call this proof a *refutation proof* of $\mathcal{A}$. Proofs where cut-formulas $\mathcal{C}$ are only variables are called *resolution proofs*, refutations of that kind *resolution refutations*. We denote this by $\mathrel{|}\!\frac{\eta,\sigma,\lambda}{Var}$.

Let φ be a CNF-formula, i.e. of the form $\bigwedge_{i<I} \bigvee_{j<J_i} \varphi_{ij}$ with φ_{ij} being literals. Then φ can be viewed as a set of clauses consisting of all $\{\varphi_{ij} : j < J_i\}$ for $i < I$. This gives meaning to the writing $\varphi \vdash^{\eta,\sigma,\lambda}_{\mathcal{C}} \mathit{\Gamma}$.

Structural rules are not included in the definition of LK. But we obtain structural rules as derivable rules which is stated in the next proposition. It is readily proven by induction on the height of the derivation η.

Proposition 2 (Structural Rule). *Assume* $\mathcal{A} \subseteq \mathcal{A}'$, $\eta \leq \eta'$, $\sigma \leq \sigma'$, $\mathcal{C} \subseteq \mathcal{C}'$ *and* $|\mathit{\Gamma}'| \leq \lambda'$, *then* $\mathcal{A} \vdash^{\eta,\sigma,\lambda}_{\mathcal{C}} \mathit{\Gamma}$ *implies* $\mathcal{A}' \vdash^{\eta',\sigma',\lambda+\lambda'}_{\mathcal{C}'} \mathit{\Gamma}, \mathit{\Gamma}'$. □

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

$$\left(\bigwedge_{i<n}\left(\left(\bigwedge_{j<i} p_j\right) \to p_i\right)\right) \to \bigwedge_{i<n} p_i$$

(of course $A \to B$ is an abbreviation of $\bigvee\{\neg A, B\}$). Let us also fix the set of clauses corresponding to $\neg\,\mathcal{O}\mathrm{Ind}(n)$:

type I	$\neg p_0, \ldots, \neg p_{a-1}, p_a$	for any $a < n$,
type II	$\neg p_0, \ldots, \neg p_{n-1}$.	

We can give upper bounds for certain parameters of shortest proofs of $\mathcal{O}\mathrm{Ind}(n)$.

Theorem 3. *1.* $\vdash^{O(n),O(n^2)}_{\emptyset} \mathcal{O}\mathrm{Ind}(n)$.

2. $\neg\,\mathcal{O}\mathrm{Ind}(n) \vdash^{n,O(n)}_{Var} \emptyset$.

Proof. Ad 1.: We can easily show by induction on k that

$$\vdash^{H(k),S(k)}_{\emptyset} \neg \bigwedge_{i<n}\Big(\bigwedge_{j<i} p_j \to p_i\Big), \bigwedge_{i<n} p_i, \{\neg p_i : i < k\}$$

holds for $k = n, \ldots, 0$, with $H(k) := 3(n + 1 - k)$, $S(k) := (n + 1 - k)(n + 2)$. The assertion then follows for $k = 0$.

Ad 2.: We can easily show by induction on k that

$$\neg\,\mathcal{O}\mathrm{Ind}(n) \vdash^{H(k),S(k)}_{Var} \{\neg p_i : i < k\}$$

holds for $k = n, \ldots, 0$, with $H(k) := n - k$, $S(k) := 2(n + 1 - k)$. The assertion then follows for $k = 0$. □

2.1 Lower Bounds on Heights for Resolution

Viewing the "Boundedness Theorem" from [3, 2] (which is adapted from [4]) in the light of resolution we obtain that the principle of order-induction $\mathcal{O}\mathrm{Ind}(n)$ for n gives us lower bounds to the height of resolution *proofs*:

Theorem 4 ([4, 2, 3]). $\vdash^{\eta}_{Var} \mathcal{O}\mathrm{Ind}(n) \quad \Rightarrow \quad \eta \geq n\,.$ □

Together with Theorem 3.1 this gives us a separation of polylogarithmic-height resolution proofs from quasi-polynomial size tree-like resolution proofs.

A similar result holds for resolution *refutations* of $\neg\,\mathcal{O}\mathrm{Ind}(n)$, but with a much simpler proof.

Theorem 5. $\neg\,\mathcal{O}\mathrm{Ind}(n) \vdash^{\eta}_{Var} \emptyset \quad \Rightarrow \quad \eta \geq n\,.$

Proof. Assume for the sake of contradiction that $\neg\,\mathcal{O}\mathrm{Ind}(n) \vdash^{\eta}_{Var} \emptyset$ and $\eta < n$ hold. Let P be such a resolution refutation tree of height bounded by η. The assumption $\eta < n$ implies that the type II axiom of $\neg\,\mathcal{O}\mathrm{Ind}(n)$ does not occur in P, because the size of sequents can only shrink by 1 through an application of **(Cut)**. But the set of axioms of type I is satisfiable (by assigning each variable to 1) and the rules of LK are correct, hence the last sequent in the proof, which is $\emptyset$, must be true under this assignment, too. Contradiction. □

Theorem 3.2 and Theorem 5 together give us a separation of polylogarithmic-height resolution refutations from quasi-polynomial size tree-like resolution refutations.

3 Height Restricted Propositional Proofs

We start this section by proving further properties of height restricted propositional proofs like inversions and different kinds of cut-elimination.

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

Proposition 6 ($(\bigwedge)$-Inversion). *Assume that* $\mathcal{A} \vdash^{\eta,\sigma,\lambda}_{C} \Gamma, \bigwedge_{i<I} \varphi_i$ *holds, and that* $\bigwedge_{i<I} \varphi_i \notin \Gamma$*, then* $\mathcal{A} \vdash^{\eta,\sigma,\lambda}_{C} \Gamma, \varphi_i$ *holds for all* $i < I$. □

Proposition 7 ($(\bigvee)$-Exportation). *Suppose* $\mathcal{A} \vdash^{\eta,\sigma,\lambda}_{C} \Gamma, \bigvee_{i<I} \varphi_i$ *holds, then* $\mathcal{A} \vdash^{\eta,\sigma,\lambda+I}_{C} \Gamma, \varphi_0, \ldots, \varphi_{I-1}\,.$ □

We define special sets of constant depth formulas.

Definition 8. $\Sigma^{s,t}_{d}$ *is the set of all formulas* φ *with*

1. $\mathrm{dp}(\varphi) \leq d+1$*;*
2. *if* $\mathrm{dp}(\varphi) = d+1$*, then the outermost connective of* φ *is* $\bigvee$*;*
3. *all depth* > 1 *sub-formulas of* φ *have the arity of their outermost connective bounded by* s*; and*
4. *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* $\Sigma^{s,t}_{d}$.

For sets of number-theoretic functions $\Xi, \Sigma, \Lambda, F, G$ and a sequence of cedents Γ_n, $n \in \mathbb{N}$, we write $(\mathcal{A}_n)_n \vdash^{\Xi,\Sigma,\Lambda}_{\Sigma_d^{F,G}} (\Gamma_n)_n$, or sometimes $\mathcal{A}_n \vdash^{\Xi,\Sigma,\Lambda}_{\Sigma_d^{F,G}} \Gamma_n$, to denote that there are some $\eta, \sigma, \lambda, f, g$ from $\Xi, \Sigma, \Lambda, F, G$, resp., such that $\mathcal{A}_n \vdash^{\eta(n),\sigma(n),\lambda(n)}_{\Sigma_d^{f(n),g(n)}} \Gamma_n$ holds for all n. We further use $\Sigma_d^{\mathrm{poly}(n)}$ as an abbreviation for $\bigcup\{\Sigma_d^{f,g} \ : \ f(n) \in 2^{(\log n)^{O(1)}}, g(n) \in (\log n)^{O(1)}\}$. Here $\Sigma_d^{f,g}$ denotes the set of sequences $(\varphi_n)_n$ of formulas such that $\varphi_n \in \Sigma_d^{f(n),g(n)}$ for all $n \in \mathbb{N}$. We often write $\varphi_n \in \Sigma_d^{f,g}$ instead of $(\varphi_n)_n \in \Sigma_d^{f,g}$.

Remark 9. Krajíček in [13] has defined resolution systems R^* and $R(\log)^*$ which correspond to our setting as follows: Let Φ_n be a sequence of clauses. Then $(\Phi_n)_n$ is quasi-polynomial size refutable in R^* (respectively $R(\log)^*$) iff $(\Phi_n)_n \vdash^{-,2^{(\log n)^{O(1)}}}_{Var} \emptyset$ $\Big($respectively $(\Phi_n)_n \vdash^{-,2^{(\log n)^{O(1)}}}_{\Sigma_0^{\mathrm{poly}(n)}} \emptyset\Big)$.

The next Proposition shows that by controlling heights we also obtain control over sizes and sequent-lengths of proofs. It follows directly by induction on the height.

Proposition 10. $\mathcal{A} \vdash^{\eta}_{\Sigma_d^{s,t}} \Gamma \subset \Sigma_{d'}^{s,t}$ *and* $t \le s \quad \Rightarrow \quad \mathcal{A} \vdash^{\eta,s^\eta,|\Gamma|+\eta}_{\Sigma_d^{s,t}} \Gamma .$ □

Remark 11. Krajíček in [11] has defined a notion called Σ-depth of a proof. This can be expressed in our terms as follows: φ has a Σ-depth d tree-like LK-proof of size σ iff $\vdash^{-,\sigma}_{\Sigma_d^{\sigma,\log\sigma}} \varphi$. Hence, the sequence $(\varphi_n)_n$ has quasi-polynomial-size Σ-depth d tree-like proofs iff $\vdash^{-,2^{(\log n)^{O(1)}}}_{\Sigma_d^{\mathrm{poly}(n)}} (\varphi_n)_n$. The last Proposition shows that $\vdash^{(\log n)^{O(1)}}_{\Sigma_d^{\mathrm{poly}(n)}} (\varphi_n)_n$ implies that $(\varphi_n)_n$ has Σ-depth d tree-like LK-proofs of size quasi-polynomial in n in which every cedent is of length polylogarithmic in n. Similar statements hold for refutations.

The proof of the next Lemma and Proposition follows the standard one which can be found e.g. in [2, 3] – we only have to control additional parameters.

Lemma 12 (Cut Elimination Lemma). *If* $\mathcal{A} \vdash^{\eta_0,\sigma_0,\lambda_0}_{\Sigma_d^{s,t}} \Gamma, \varphi$, $\mathcal{A} \vdash^{\eta_1,\sigma_1,\lambda_1}_{\Sigma_d^{s,t}} \Delta, \neg\varphi$ *and* $\varphi \in \Sigma_{d+1}^{s,t}$, *then* $\mathcal{A} \vdash^{\eta_0+\eta_1,\sigma_0\cdot\sigma_1,\lambda_0+\lambda_1}_{\Sigma_d^{s,t}} \Gamma, \Delta$. □

Proposition 13 (Cut Elimination Theorem).

$$\mathcal{A} \vdash^{\eta,\sigma,\lambda}_{\Sigma_{d+1}^{s,t}} \Gamma \quad \Rightarrow \quad \mathcal{A} \vdash^{2^\eta,\sigma^{2^\eta},2^\eta\cdot\lambda}_{\Sigma_d^{s,t}} \Gamma \ .$$ □

The next Proposition gives a form of cut elimination which makes use of the parameters size and sequent-length (and arity of outermost connective of cut formulas) while at the same time ignoring height of proofs. The one after the next one ignores size and sequent-length and depends only on height (and length of cut formulas).

Proposition 14 (Krajíček's Cut Elimination [11, 12.2.1]).

$$\mathcal{A} \vdash^{\eta,\sigma,\lambda}_{\Sigma^{s,t}_{d+1}} \varGamma \quad \Rightarrow \quad \mathcal{A} \vdash^{-,\sigma\cdot s^{\lambda}}_{\Sigma^{s,t}_{d}} \varGamma \ . \qquad \square$$

The following Bounded-Cut Elimination is central for the study of height restricted proof systems. We repeat the proof from [3].

Proposition 15 (Bounded-Cut Elimination [2, 3]).

$$\mathcal{A} \vdash^{\eta}_{\Sigma^{s,t}_{0}} \varGamma \quad \Rightarrow \quad \mathcal{A} \vdash^{\eta\cdot t}_{Var} \varGamma \ .$$

Proof. The Proposition follows from the following Bounded-Cut Elimination lemma, which even gives rise to a more general Bounded-Cut Elimination – we keep the proposition in the form we have because that is all we need here.

Let $\mathrm{noa}(\varphi)$ be the number of (occurrences of) atoms in φ.

$$\mathcal{A} \vdash^{\eta}_{Var} \varGamma, \varphi \quad \text{and} \quad \mathcal{A} \vdash^{\eta}_{Var} \varGamma, \neg\varphi \quad \Rightarrow \quad \mathcal{A} \vdash^{\eta+\mathrm{noa}(\varphi)}_{Var} \varGamma \ . \tag{1}$$

We prove (1) by induction on φ. If φ is atomic we just apply **(Cut)**.

Now assume w.l.o.g. that φ has the form $\bigvee_{i<k} \varphi_i$. By $(\bigwedge)$-Inversion and $(\bigvee)$-Exportation from Section 3 we obtain $\mathcal{A} \vdash^{\eta}_{Var} \varGamma, \varphi_0, \ldots, \varphi_{k-1}$ and $\mathcal{A} \vdash^{\eta}_{Var} \varGamma, \neg\varphi_i$ for all $i < k$. By successively applying the induction hypothesis k times we obtain $\mathcal{A} \vdash^{\eta+\mathrm{noa}(\varphi_0)+\cdots+\mathrm{noa}(\varphi_{k-1})}_{Var} \varGamma$. Observe that $\mathrm{noa}(\varphi) = \sum_{i<k} \mathrm{noa}(\varphi_i)$. □

We repeat the translation (also called embedding) of provability in $S^1_2(\alpha)$, $T^1_2(\alpha)$, and more general of $\Sigma^b_{m+1}(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND}$, 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.

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 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 $\big([\![\varphi(n)]\!]\big)_n$ in $\Sigma^{\mathrm{poly}(n)}_d$.

Theorem 16 ([2, 3]). *Let $\varphi(x)$ be a formula in the language of bounded arithmetic, in which at most the variable x occurs free.*

1. *If* $S^1_2(\alpha) \vdash \varphi(x)$*, then* $\vdash^{O\left(\log^{(2)} n\right)}_{\Sigma_1^{\mathrm{poly}(n)}} [\![\varphi(n)]\!]$.
2. *If* $T^1_2(\alpha) \vdash \varphi(x)$*, then* $\vdash^{O(\log n)}_{\Sigma_1^{\mathrm{poly}(n)}} [\![\varphi(n)]\!]$.
3. *If* $\Sigma^b_{m+1}(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND} \vdash \varphi(x)$*, then* $\vdash^{O\left(\log^{(m+2)} n\right)}_{\Sigma_{m+1}^{\mathrm{poly}(n)}} [\![\varphi(n)]\!]$. □

By combining this Theorem first with the Cut Elimination Theorem and afterwards with the Bounded-Cut Elimination we obtain

Theorem 17 ([2, 3]). *Let* $\varphi(x)$ *be a formula in the language of bounded arithmetic, in which at most the variable* x *occurs free.*

1. *If* $S^1_2(\alpha) \vdash \varphi(x)$*, then* $\vdash^{(\log n)^{O(1)}}_{Var} [\![\varphi(n)]\!]$.
2. *If* $\Sigma^b_{m+1}(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND} \vdash \varphi(x)$*, then* $\vdash^{2_m\left((\log^{(m+1)} n)^{O(1)}\right)}_{Var} [\![\varphi(n)]\!]$. □

If we take Theorem 16, and first apply the Cut Elimination Theorem, then Proposition 10, and finally Krajíček's Cut Elimination, we obtain the following Theorem:

Theorem 18 ([13, 3.1]). *Let* $\varphi(x)$ *be a formula in the language of bounded arithmetic, in which at most the variable* x *occurs free.*
If $T^1_2(\alpha) \vdash \varphi(x)$ *or* $\Sigma^b_{m+1}(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND} \vdash \varphi(x)$*, then* $\vdash^{-,2^{(\log n)^{O(1)}}}_{\Sigma_0^{\mathrm{poly}(n)}} [\![\varphi(n)]\!]$. □

We represent the last two Theorems together with previously obtained results in Fig. 1 and 2. The separation between quasi-polynomial-size tree-like resolution and quasi-polynomial-size sequence-like resolution is well-known (the best known separation can be found in [5]).

$$\begin{tikzcd}
S^1_2(\alpha) \arrow[r, hook] & \text{polylogarithmic-height resolution} \arrow[d, phantom, sloped, "\subsetneq"] \\
sR^2_2(\alpha) \arrow[r, hook] & 2^{(\log\log n)^{O(1)}}\text{-height resolution} \arrow[d, phantom, sloped, "\subsetneq"] \\
s\Sigma^b_3(\alpha)\text{-}\mathrm{L}^3\mathrm{IND} \arrow[r, hook] & 2_2\left((\log^{(3)} n)^{O(1)}\right)\text{-height resolution} \arrow[d, phantom, sloped, "\subsetneq"] \\
 & \vdots
\end{tikzcd}$$

Fig. 2. Translation of $\Sigma^b_{m+1}(\alpha)$-$\mathrm{L}^{m+1}\mathrm{IND}$

A separation between polylogarithmic-height resolution and quasi-polynomial-size tree-like resolution follows from Theorems 3 and 4: The first Theorem shows that $\mathcal{O}\mathrm{Ind}(n)$ has tree-like resolution proofs of size $O(n^2)$, whereas the second one shows that a resolution proof of this statement must have height $\Omega(n)$ and hence is unprovable in polylogarithmic-height resolution.

Theorems 3 and 4 can also be used to obtain a separation between $2_m\left(\left(\log^{(m+1)} n\right)^{O(1)}\right)$-height resolution and $2_{m+1}\left(\left(\log^{(m+2)} n\right)^{O(1)}\right)$-height resolution: By the first theorem, the formulas $\mathcal{O}\mathrm{Ind}\left(2_{m+1}\left(\left(\log^{(m+2)} n\right)^{2}\right)\right)$, for m fixed, have resolution proofs of height $2_{m+1}\left(\left(\log^{(m+2)} n\right)^{O(1)}\right)$, whereas the second theorem can be used to show that resolution proofs of these statements must have height $\Omega\left(2_{m+1}\left(\left(\log^{(m+2)} n\right)^{2}\right)\right)$, again for m fixed, and, therefore, are unprovable in $2_m\left(\left(\log^{(m+1)} n\right)^{O(1)}\right)$-height resolution.

By Theorem 17 and Theorem 18 we obtain translations of provability in $\Sigma^b_m(\alpha)$-L^{m}IND into two propositional proof systems which seem to be incomparable (for $m \geq 2$). We have visualized this for the case $m = 2$ in Fig. 3. Note that in general $2_m\left(\left(\log^{(m+1)} n\right)^{O(1)}\right)$-height resolution proofs have size super-quasi-polynomial in n.

$$\begin{tikzcd}
 & & 2^{(\log\log n)^{O(1)}}\text{-height resolution} \\
sR^2_2(\alpha) \arrow[r, hook] & \vdash^{(\log\log n)^{O(1)}}_{\Sigma_1^{\mathrm{poly}(n)}} \arrow[ur] \arrow[dr] & \\
 & & \text{quasi-polynomial-size } R(\log)^*
\end{tikzcd}$$

Fig. 3. Differences of translations of derivations

4 Cut Introduction and Simulation

In this section we investigate converses to cut-elimination. Krajíček has used ideas from Spira ([11, 4.3.10]) to reduce the number of cuts on any path through a tree-like proof by adding a special-$\bigwedge$-rule to LK and raising the depth of formulas in the proof.

Here we will study how the height of proofs can be shrinked by raising the depth of cut-formulas. We will obtain the following converse to the Cut Elimination Theorem from Section 3. Recall that $|\Gamma|$ denotes the number of formulas in the cedent Γ.

Theorem 19. *1. Assume* $\vdash^{\gamma}_{\Sigma^{s,t}_d} \Gamma$ *for* $\Gamma \subset \Pi^{s,t}_{d+1}$ *such that* $|\Gamma| \leq \log\gamma$ *and* $d > 0$. *Then* $\vdash^{O((\log\gamma)^2)}_{\Sigma^{s_\gamma,t}_{d+1}} \Gamma$ *for* $s_\gamma := s^{\gamma^{O(1)}}$.

2. Assume $\vdash^{\gamma}_{Var} \Gamma$ *for* $\Gamma \subset \Pi^{s,t}_1$ *such that* $|\Gamma| \leq \log\gamma$. *Then* $\vdash^{O(\log\gamma)}_{\Sigma_1^{2^{\gamma},O(t\cdot\gamma)}} \Gamma$.

The proof of this Theorem needs some lemmas. Let ${}^m n$ denote the set of all number-theoretic functions from $\{0,\ldots,m{-}1\}$ to $\{0,\ldots,n{-}1\}$. The first lemma reduces heights by introducing intermediate cut formulas from the set $\Sigma_{d+1}^{s,t,\delta}$ given by formulas of the form $\bigvee_s \left(\bigwedge_\delta (\Sigma_d^{s,t} \cup \Pi_d^{s,t})\right)$. We understand $\Sigma_{d+1}^{s,t} \subset \Sigma_{d+1}^{s,t,\delta}$.

Lemma 20. *1. Let $\Gamma \subset \Pi_{d+1}^{s,t}$ and assume $\vdash^{\gamma}_{\Sigma_d^{s,t}} \Gamma$. Then $\vdash^{O(\log\gamma)+|\Gamma|}_{\Sigma_{d+1}^{s^\gamma,t,\gamma+|\Gamma|}} \Gamma$.*

2. In case of $d = 0$ let $\Gamma \subset \Pi_1^{s,t}$ and assume $\vdash^{\gamma}_{Var} \Gamma$. Then $\vdash^{O(\log\gamma)+|\Gamma|}_{\Sigma_1^{2^\gamma,\gamma+t\cdot|\Gamma|}} \Gamma$.

The proof of this lemma is postponed to Appendix A. The second part of the previous Lemma already proves the second part of Theorem 19.

The next Lemma is a propositional variant of sharply bounded collection [11, Def. 5.2.11].

Lemma 21. *Let $\varphi_{ij} \in \Pi_{d-1}^{s,t}$ and assume $d, s, \alpha \geq 2$, then*

$$\vdash^{\gamma}_{\Sigma_d^{s^\alpha,t}} \Gamma, \bigwedge_{i<\alpha} \bigvee_{j<s} \varphi_{ij} \qquad \Rightarrow \qquad \vdash^{\gamma+\log\alpha+O(d)}_{\Sigma_d^{s^\alpha,t}} \Gamma, \bigvee_{f\in{}^\alpha s} \bigwedge_{i<\alpha} \varphi_{i\,f(i)} \ .$$

Proof. Assume that $\vdash^{\gamma}_{\Sigma_d^{s^\alpha,t}} \Gamma, \bigwedge_{i<\alpha} \bigvee_{j<s} \varphi_{ij}$ and the other assumptions of the Lemma hold. For all $0 \leq a \leq b \leq \alpha$ and $k \leq \lceil \log\alpha \rceil$ it is not hard to show that

$$\vdash^{\gamma+N(k)}_{\Sigma_d^{s^\alpha,t}} \Gamma, \neg \bigvee_{f\in{}^\alpha s} \bigwedge_{a\leq i<b} \varphi_{i\,f(i)}, \bigvee_{f\in{}^\alpha s} \bigwedge_{a\leq i<b+2^k, i<\alpha} \varphi_{i\,f(i)}$$

holds for $N(k) = k + O(d)$. Then the assertion follows for $k = \lceil \log\alpha \rceil$ and $a = b = 0$. □

Finally we can remove the special cut formulas from Lemma 20.

Lemma 22. *Assume $\alpha \geq 2$, $d \geq 1$ and $t \leq s$. Then*

$$\vdash^{\gamma}_{\Sigma_{d+1}^{s,t,\alpha}} \Gamma \qquad \Rightarrow \qquad \vdash^{(\gamma+1)\cdot 2\cdot\log\alpha}_{\Sigma_{d+1}^{s^{\alpha+1},t}} \Gamma \ .$$

The proof of this lemma is postponed to Appendix A.

Proof (of Theorem 19.1). Assume $\vdash^{\gamma}_{\Sigma_d^{s,t}} \Gamma$ for $\Gamma \subset \Pi_{d+1}^{s,t}$ such that $|\Gamma| \leq \log\gamma$ and $d \geq 1$. By Lemma 20 we obtain $\vdash^{O(\log\gamma)}_{\Sigma_{d+1}^{s^\gamma,t,2\cdot\gamma}} \Gamma$. Now Lemma 22 produces $\vdash^{O(\log\gamma)\cdot 2\cdot\log(2\cdot\gamma)}_{\Sigma_{d+1}^{s^{\gamma\cdot(2\cdot\gamma)},t}} \Gamma$. Hence $\vdash^{O((\log\gamma)^2)}_{\Sigma_{d+1}^{s^{\gamma^{O(1)}},t}} \Gamma$. □

Applying Theorem 19, and the Cut Elimination Theorem and the Bounded-Cut Elimination from Section 3 we can draw the following Corollary:

Corollary 23 (Simulation). *Let $(\Gamma_n)_n$ be included in $\Pi_{d+1}^{\mathrm{poly}(n)}$ and the length of Γ_n, $|\Gamma_n|$, be bounded by a constant for all $n \in \mathbb{N}$.*

1. *Assume* $d > 0$ *and* $2_{i+1}((\log^{(j)} n)^{O(1)})$ *grows polylogarithmic in* n, *i.e.* $i+3 \leq j$. *Then*

$$\vdash^{2_{i+1}((\log^{(j)} n)^{O(1)})}_{\Sigma_d^{\mathrm{poly}(n)}} (\Gamma_n)_n \qquad \Leftrightarrow \qquad \vdash^{2_i((\log^{(j)} n)^{O(1)})}_{\Sigma_{d+1}^{\mathrm{poly}(n)}} (\Gamma_n)_n \enspace .$$

2. *For* $d = 0$ *assume* $2_{i+1}(O(\log^{(j)} n))$ *grows polylogarithmic in* n, *i.e.* $i+2 \leq j$. *Then*

$$\vdash^{2_{i+1}(O(\log^{(j)} n))}_{Var} (\Gamma_n)_n \qquad \Leftrightarrow \qquad \vdash^{2_i(O(\log^{(j)} n))}_{\Sigma_1^{\mathrm{poly}(n)}} (\Gamma_n)_n \enspace .$$

In particular, for $i = 0$ *and* $j = 2$ *this shows*

$$\vdash^{(\log n)^{O(1)}}_{Var} (\Gamma_n)_n \qquad \Leftrightarrow \qquad \vdash^{O(\log\log n)}_{\Sigma_1^{\mathrm{poly}(n)}} (\Gamma_n)_n \enspace .$$

□

Final Remarks and Open Problems

We have shown (and represented in Fig. 1) that provability in $S^1_2(\alpha)$ translates to polylogarithmic-height resolution, and provability in $T^1_2(\alpha)$ translates to quasi-polynomial size sequence-like resolution. Is there a system of bounded arithmetic which corresponds to quasi-polynomial size tree-like resolution?

The simulation given by Corollary 23 is unsatisfying in the following aspects: First, it does not hold for super-polylogarithmic height resolution which comes from $\Sigma^b_i(\alpha)$-L^{i}IND for $i \geq 2$. And second, for polylogarithmic-height resolution we have established the simulation only for provability of $\Pi_1^{\mathrm{poly}(n)}$-sequents which does not include $\mathcal{O}\mathrm{Ind}(n)$. This leads to the following questions:
1. What is the “right” propositional proof system corresponding to e.g. $sR^2_2(\alpha)$ (which is the same as $\Sigma^b_2(\alpha)$-L^{2}IND)? Remember that we have the two translations, represented in Fig. 3, that $sR^2_2(\alpha)$-proofs translate on the one side to $2^{(\log\log n)^{O(1)}}$-height resolution, and on the other side to quasi-polynomial-size $R(\log)^*$. Is the “right” system given by combining both proof systems, i.e. by $\vdash^{2^{(\log\log n)^{O(1)}},2^{(\log n)^{O(1)}}}_{\Sigma_0^{\mathrm{poly}(n)}}$ which is the same as quasi-polynomial-size $2^{(\log\log n)^{O(1)}}$-height $R(\log)^*$?
2. Can the simulation between $\vdash^{O(\log\log n)}_{\Sigma_1^{\mathrm{poly}(n)}}$ (which corresponds to provability in $S^1_2(\alpha)$) and polylogarithmic-height resolution be extended to formulas of the same kind as $\mathcal{O}\mathrm{Ind}(n)$, e.g. $\Sigma_2^{\mathrm{poly}(n)}$? Or, is there another version of resolution which allows this correspondence?

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 and Wolfram Pohlers. Applications of cut-free infinitary derivations to generalized recursion theory. *Ann. Pure Appl. Logic*, 94:7–19, 1998.
5. Eli Ben-Sasson, Russell Impagliazzo, and Avi Wigderson. Near-optimal separation of tree-like and general resolution. ECCC TR00-005, 2000.
6. Samuel R. Buss. *Bounded arithmetic*, volume 3 of *Stud. Proof Theory, Lect. Notes.* Bibliopolis, Naples, 1986.
7. Samuel R. Buss. Relating the bounded arithmetic and the polynomial time hierarchies. *Ann. Pure Appl. Logic*, 75:67–77, 1995.
8. Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symbolic Logic*, 44:36–50, 1979.
9. Johan Håstad. *Computational Limitations of Small Depth Circuits.* MIT Press, Cambridge, MA, 1987.
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.

Appendix A. Proofs of Lemma 20 and of Lemma 22

Proof (of Lemma 20). For $\mathcal{A}$ a set of cedents let $\bigvee\mathcal{A}$ be the set of all $\bigvee\Gamma$ for $\Gamma\in\mathcal{A}$. Let $\Gamma\subset\Sigma^{s,t}_d\cup\Pi^{s,t}_d$. We can show

$$\mathcal{A}\vdash^{2^\gamma}_{\Sigma^{s,t}_d}\Gamma\qquad\Rightarrow\qquad\bigvee\mathcal{A}\vdash^{O(\gamma)}_{\Sigma^{s^{2^\gamma},t,2^\gamma+|\Gamma|}_{d+1}}\bigvee\Gamma$$

by induction on γ. Then we obtain 1. by the following argument: Let Γ be the set $\{\bigwedge_{j<s}\varphi_{ij} : i<I\}$ with $\varphi_{ij}\in\Sigma^{s,t}_d$. For $f\in{}^I s$ let Γ_f be the set $\{\varphi_{if(i)} : i<I\}$ of inversions, then by ($\bigwedge$)-Inversion from Section 3 $\vdash^{\gamma}_{\Sigma^{s,t}_d}\Gamma_f$. From the assertion we obtain $\vdash^{O(\log\gamma)}_{\Sigma^{s^\gamma,t,\gamma+|\Gamma|}_{d+1}}\Gamma_f$ for all $f\in{}^I s$, hence by $|\Gamma|$ many ($\bigwedge$) inferences $\vdash^{O(\log\gamma)+|\Gamma|}_{\Sigma^{s^\gamma,t,\gamma+|\Gamma|}_{d+1}}\Gamma$.

The idea for proving the induction step of the assertion goes as follows: Given $\mathcal{A} \vdash^{2^{\gamma+1}}_{\Sigma^{s,t}_d} \Gamma$ we can find some set of cedents Γ_i for $i \in I$ such that $\mathcal{A} \vdash^{2^\gamma}_{\Sigma^{s,t}_d} \Gamma_i$ for all $i \in I$ and $\{\Gamma_i : i \in I\} \vdash^{2^\gamma}_{\Sigma^{s,t}_d} \Gamma$. Now we can apply the induction hypothesis to all these derivations, and putting them together suitably yields the assertion. The additional cuts are of the form $\bigwedge_{i\in I} \bigvee \Gamma_i$.

In case of $d = 0$ the same strategy even shows

$$\mathcal{A} \vdash^{2^\gamma}_{Var} \Gamma \quad \text{and} \quad \Gamma \subset Var \qquad \Rightarrow \qquad \bigvee \mathcal{A} \vdash^{O(\gamma)}_{\Sigma_1^{2^{2^\gamma}, 2^\gamma+|\Gamma|}} \bigvee \Gamma \ .$$

Then we obtain 2. in the following way: Let Γ be the set $\{\bigwedge_{j<s} \bigvee_{k<t} \varphi_{ijk} : i < I\}$ with $\varphi_{ijk} \in Var$. For $f \in {}^I s$ let Γ_f be the set $\bigcup_{i<I} \{\varphi_{i,f(i),0}, \ldots, \varphi_{i,f(i),(t-1)}\}$ of inversions, then by ($\bigwedge$)-Inversion and ($\bigvee$)-Exportation from Section 3 $\vdash^{\gamma}_{Var} \Gamma_f$ for all $f \in {}^I s$. The assertion now shows $\vdash^{O(\log\gamma)}_{\Sigma_1^{2^\gamma, \gamma+t\cdot|\Gamma|}} \bigvee \Gamma_f$. From this we obtain by a direct argument $\vdash^{O(\log\gamma)}_{\Sigma_1^{2^\gamma, \gamma+t\cdot|\Gamma|}} \bigvee_{k<t} \varphi_{0,f(0),k}\ , \ldots, \bigvee_{k<t} \varphi_{(I-1),f(I-1),k}$ for all $f \in {}^I s$, hence by $|\Gamma|$ many ($\bigwedge$) inferences $\vdash^{O(\log\gamma)+|\Gamma|}_{\Sigma_1^{2^\gamma, \gamma+t\cdot|\Gamma|}} \Gamma$. □

Proof (of Lemma 22). Again we have to make our assertion a little bit more general. W.l.o.g. let $\varphi \in \Sigma^{s,t,\alpha}_{d+1}$ be of the form

$$\varphi = \bigvee_{i<s} [\bigwedge_{j<\alpha_i} \bigvee_{k<s} \varphi_{ijk} \wedge \bigwedge_{\alpha_i \le j < \alpha} \varphi_{ij}]$$

with $\varphi_{ijk} \in \Pi^{s,t}_{d-1}$ and $\varphi_{ij} \in \Pi^{s,t}_d$. Then let

$$\varphi^* := \bigvee_{i<s} \bigvee_{f \in {}^{(\alpha_i)}s} [\bigwedge_{j<\alpha_i} \varphi_{ijf(j)} \wedge \bigwedge_{\alpha_i \le j < \alpha} \varphi_{ij}] \ .$$

Dually for $\Pi^{s,t,\alpha}_{d+1}$. Observe that $\left(\Sigma^{s,t,\alpha}_{d+1}\right)^* \subset \Sigma^{s^{\alpha+1},t}_{d+1}$ and $\left(\Pi^{s,t,\alpha}_{d+1}\right)^* \subset \Pi^{s^{\alpha+1},t}_{d+1}$
We can prove

$$\vdash^{\gamma}_{\Sigma^{s,t,\alpha}_{d+1}} \Gamma, \Xi \quad \text{and} \quad \Xi \subset \Sigma^{s,t,\alpha}_{d+1} \cup \Pi^{s,t,\alpha}_{d+1} \qquad \Rightarrow \qquad \vdash^{(\gamma+1)\cdot 2\cdot\log\alpha}_{\Sigma^{s^{\alpha+1},t}_{d+1}} \Gamma, \Xi^*$$

by induction on γ which implies the Lemma for $\Xi = \emptyset$. In the induction step we use the previous Lemma 21. □