From positive and intuitionistic bounded arithmetic to monotone proof complexity

Anupam Das

▶ To cite this version:

Anupam Das. From positive and intuitionistic bounded arithmetic to monotone proof complexity. 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'16), Jul 2016, New York, United States. pp.126-135, 10.1145/2933575.2934570 . hal-01494106

HAL Id: hal-01494106
https://hal.science/hal-01494106

Submitted on 22 Mar 2017

Preprint of extended abstract appearing in proceedings of *LICS '16*

From positive and intuitionistic bounded arithmetic to monotone proof complexity

Anupam Das
LIP, Université de Lyon, CNRS, ENS de Lyon, Université Claude-Bernard Lyon 1, Milyon
anupam.das@ens-lyon.fr

Abstract

We study versions of second-order bounded arithmetic where induction and comprehension formulae are positive or where the underlying logic is intuitionistic, examining their relationships to monotone and deep inference proof systems for propositional logic.

In the positive setting a restriction of a Paris-Wilkie (PW) style translation yields quasipolynomial-size monotone propositional proofs from Π^0_1 arithmetic theorems, as expected. We further show that, when only polynomial induction is used, quasipolynomial-size normal deep inference proofs may be obtained, via a graph-rewriting normalisation procedure from earlier work.

For the intuitionistic setting we calibrate the PW translation with the Brouwer-Heyting-Kolmogorov interpretation of intuitionistic implication to recover a transformation to monotone proofs. By restricting type level we are able to identify an intuitionistic theory, $I_1U^1_2$, for which the transformation yields quasipolynomial-size monotone proofs. Conversely, we show that $I_1U^1_2$ is powerful enough to prove the soundness of monotone proofs, thereby establishing a full correspondence.

1. Introduction

Bounded arithmetic has been a fruitful way to relate complexity classes with logical theories and propositional proof systems. For example Paris and Wilkie showed that proofs of Π^0_1-sentences in the theory $I\Delta_0$[1] translate to classes of polynomial-size Hilbert-Frege (HF) proofs of bounded depth [27]; conversely, the soundness of bounded-depth HF systems can be proved in such theories.[2]

In this work we identify theories of bounded arithmetic for *monotone* and *deep inference* proof systems, via positive and intuitionistic versions of well-known theories in the literature.

Deep inference proof complexity has received much attention in recent years, and the complexity of the minimal system, KS, is considered as yet unresolved [7] [22] [15]. While an extension of it, KS$^+$, is known to quasipolynomially[3] simulate HF systems[4] [22] [8], there is neither such a simulation known for KS nor some nontrivial lower bound separating the two systems.

These systems can be viewed as subclasses of tree-like monotone proofs (exemplified in e.g. [5] and [22]), i.e. sequent calculus proofs free of negation steps (MLK), studied in e.g. [28], [4] and [2].[5] We exploit this correspondence in the present work and, for simplicity of exposition, work with rewriting systems Mon and Nor instead of KS$^+$ and KS, respectively [16].

The starting point of this work is the second-order framework due to Buss [9], as developed by Krajícek in [25]. [6] In Sect. 3 we consider 'positive' versions of the theories U^i_j and V^i_j, where set variables may not occur in negative context in non-logical rules. We address some proof-theoretic issues and give a deep inference style presentation of the Paris-Wilkie (PW) translation to Mon in Dfn. 24. The main result of this section is Thm. 27, that proofs in the image of a certain theory $\underline{MU^1_2}$ can be transformed to Nor-proofs in quasipolynomial time, via graph-rewriting normalisation procedures from [19] and analysis of their complexity from [17].

In Sect. 4, in order to obtain converse statements to these translations, we turn to *intuitionistic* variants of these theories, allowing us to recover the ability to conduct some metalogical reasoning. The two main contributions of this section are Lemma 39, a sort of *witnessing theorem* that eliminates the presence of second-order existential quantifiers in a proof, and Dfn. 44, an adaptation of the PW translation by the Brouwer-Heyting-Kolmogorov interpretation of intuitionistic logic, ultimately yielding monotone proofs. For a certain theory, $I_1U^1_2$, we obtain in Cor. 46 that proofs in the image of the translation can be made tree-like (i.e. in Mon) efficiently.

In Sect. 5 we consider *reflection* principles: formal statements of the soundness of a system. The main result of this section is Thm. 49, that $I_1U^1_2$ proves the soundness of Mon, thereby establishing a full correspondence between $I_1U^1_2$ and Mon.

Finally, in Sect. 6 we present some further discussion and results, and in Sect. 7 we give some concluding remarks.

Acknowledgements I would like to thank Arnold Beckmann for many helpful conversations on this line of research. I would also like to thank Paola Bruscoli, Alessio Guglielmi, Tom Gundersen, Lutz Straßburger and others in the deep inference community for their feedback on early versions of this work. This work has been partially supported by the ANR-14-CE25-0005 Elica project.

[1] This is the fragment of Peano Arithmetic with induction is restricted to Δ_0-formulae.

[2] Strictly speaking, we also require the 'Ω_1 axiom', to allow simple manipulation of sequences.

[3] A quasipolynomial is a function $2^{\log^{O(1)} n}$.

[4] In fact, it is widely believed that a polynomial simulation holds, cf. [23].

[5] Indeed, it was in this setting that the aforementioned quasipolynomial simulation was first proved [2].

[6] We choose not to work in the framework developed by Cook and Nguyen [13] since many relevant distinctions, e.g. polynomial induction vs. regular induction, seem to collapse in that setting.

2. Preliminaries

We generally follow the notations and conventions from [25], and occasionally [13] as well. Throughout this paper we adopt quasipolynomial-time, i.e. $2^{\log^{O(1)} n}$-time, as our model of feasible computation. A polylogarithm is a function $\log^{O(1)} n$.

2.1 Propositional and second-order logic

We formulate propositional logic (PL) with connectives $\bot$, $\top$, $\vee$, $\wedge$, $\supset$ and countably many propositional variables, e.g. p, q etc. We may use other common connectives as abbreviations for their usual definitions in this basis. Namely, we write $\neg\varphi$ for $\varphi \supset \bot$ and $\varphi \equiv \psi$ for $(\varphi \supset \psi) \wedge (\psi \supset \varphi)$. We often omit brackets for long conjunctions and disjunctions for readability, and also for long implications when the right-most bracketing is assumed.

For arithmetic theories, we work in a two-sorted first-order logic, which we refer to as *second-order logic* (SOL) in line with the literature. SOL extends PL by variables x, y, z etc. for individuals, X, Y, Z etc. for sets (or strings), symbols $=_1, =_2$ for individual and set equality, respectively, and quantifiers $\exists^1, \forall^1$ and $\exists^2, \forall^2$ for individual and set quantification respectively. There is also a non-logical binary infix symbol $\in$ expressing membership of an individual in a set. There may be further non-logical symbols, in which case we use metavariables s, t and S, T to range over individual and set terms respectively.

We sometimes write Xx or $X(x)$ instead of $x \in X$. In all settings, we denote formulae by Greek letters φ, ψ etc., possibly indicating free variables within parentheses, e.g. $\varphi(x, y)$.

Definition 1 (Contexts and polarity)**.** A context $\varphi[\cdot]$ is a formula with a hole in place of a subformula. We say that a context $\varphi[\cdot]$ is *positive* if its hole is under the left-scope of an even number of $\supset$ symbols; otherwise it is *negative*. E.g. the context $([\cdot] \supset \varphi) \supset \psi$ is positive, while the context $[\cdot] \supset (\varphi \supset \psi)$ is negative.

A formula is *positive* or *monotone* if no set symbol occurs in negative context.

Convention 2 (Sequent calculus)**.** We work with a usual sequent calculus LK^2 over our basis of connectives, with multiplicative formulations of branching logical rules and additive versions of non-branching logical rules,[7] e.g. as presented in [9]. In all cases cedents are multisets of formulae and the symbol $\rightarrow$ delimits the two sides of a sequent, e.g. a typical sequent is written $\Gamma \rightarrow \Delta$. We write LK for the propositional fragment of LK^2.

A sequent is *positive* if it contains only positive formulae. The *monotone (propositional) sequent calculus MLK* is obtained from the propositional calculus LK by removing the $\supset$ rules.

The intuitionistic caclulus LJ^2 is obtained from LK^2 by insisting that the RHS of each sequent in a proof consists of at most one formula. For this we must also alter the $\vee$-l rule slightly as follows:

$$\vee\text{-l}\ \frac{\Gamma, \varphi \rightarrow \Delta \quad \Sigma, \psi \rightarrow \Delta}{\Gamma, \Sigma, \varphi \vee \psi \rightarrow \Delta}$$

A (dag-like) *proof* is a list of sequents such that each one follows from previous ones by a rule of LK^2. We call a proof *tree-like* if its dependency graph is a tree, i.e. each sequent is used at most once as the premiss of an inference step.

2.2 Bounded arithmetic and the Paris-Wilkie translation

We work in the setting of [25] (itself based on [9]), and refer the reader to those works for comprehensive preliminary material on bounded arithmetic.

We consider second-order theories over the vocabulary,

$$\mathcal{L}_2 = \{0, 1, +, \times, |\cdot|, \#, \lfloor \tfrac{\cdot}{2} \rfloor, <\}$$

with the usual interpretation of symbols, as construed in [25]. As usual, set symbols are now equipped with bounding terms and associated axioms. We will write $X \leq t$ for the positive atomic formula $s \leq t$, where s is the bounding term of X.[8] We will write Σ_i^B and Π_i^B for the classes of formulae *strict*-$\Sigma_i^{1,b}$ and -$\Pi_i^{1,b}$ resp.

Remark 3. While we are borrowing some notation from [13] for readability, we do not formally follow their framework. They include a length term for sets, which makes it difficult to distinguish the forms of induction $PIND$ and IND we consider later on. However we do assume that set symbols are equipped with a bounding term as in [25], when necessary.

We assume that all our theories contain some appropriate set $BASIC$ of basic axioms (including extensionality and boundedness of sets), which can be found in [25].

Definition 4 (Induction and comprehension)**.** We define the following axioms:

$$\begin{array}{rcl}
CA & : & \exists X \leq y. \forall x < y. (Xx \equiv \varphi(x)) \\
IND & : & \varphi(0) \supset \forall x. (\varphi(x) \supset \varphi(x+1)) \supset \forall x. \varphi(x) \\
PIND & : & \varphi(0) \supset \forall x. (\varphi(\lfloor \frac{x}{2} \rfloor) \supset \varphi(x)) \supset \forall x. \varphi(x)
\end{array}$$

For any of these axioms AX and a set of formulae Φ, we denote by Φ-AX the set of axiom instances when the formula φ is in Φ.

Henceforth we assume the calculus LK^2 is enriched with initial sequents for (all instantiations by terms of) any axioms under consideration and also the usual designated rules for the bounded quantifiers. If we are working in theories containing IND or $PIND$, then we assume proofs are formulated with their associated inference rules, cf. [25]. We will also have a proof-theoretic treatment of comprehension in the form of *witnessing theorems*, which we will present in Sects. 3.2 and 4.3.

The following result is, in fact, a corollary of what is usually called 'free-cut elimination' introduced by Takeuti in [30], which is discussed in detail in [12], although we state essentially the version from [13].

Theorem 5 (Free-cut elimination)**.** *Let $\mathcal{S}$ be a sequent system containing LK^2 and possibly containing non-logical initial sequents and induction rules that are closed under substitution of terms for free variables. Every $\mathcal{S}$-theorem φ has an $\mathcal{S}$-proof where each formula occurring is (a substitutional instance of) a subformula of φ, an induction formula, or a formula in an initial sequent.*

An important point is that the above statement also holds for *intuitionistic* theories (e.g. as stated in [12]).

Definition 6. The theory U_2^i is axiomatised by $BASIC$, Σ_0^B-CA and Σ_i^B-$PIND$. V_2^i is the same but with IND in place of $PIND$.

We now present a translation $\langle \cdot \rangle$ of closed Σ_0^B-formulae to quasipolynomial-size propositional formulae, where set symbols are associated with propositional variables, essentially from [27].

Let $v(t)$ denote the numerical value of a closed term t.

Definition 7 (PW for closed formulae)**.** We define a translation $\langle \cdot \rangle$ of closed Σ_0^B-formulae as follows,

$$\begin{array}{rclrcl}
\langle \top \rangle & := & \top & \langle \varphi \star \psi \rangle & := & \langle \varphi \rangle \star \langle \psi \rangle \\
\langle \bot \rangle & := & \bot & \langle \exists x \leq t. \varphi(x) \rangle & := & \bigvee\limits_{k=0}^{v(t)} \langle \varphi(k) \rangle \\
\langle X(t) \rangle & := & p^X_{v(t)} & & & \\
\langle s \bowtie t \rangle & := & \ddagger & \langle \forall x \leq t. \varphi(x) \rangle & := & \bigwedge\limits_{k=0}^{v(t)} \langle \varphi(k) \rangle
\end{array}$$

for $\bowtie \in \{\leq, =\}$ and $\star \in \{\vee, \wedge, \supset\}$, where $\ddagger$ is $\top$ if $v(s) \bowtie v(t)$ and $\bot$ otherwise.

[7] Here, we mean 'additive' and 'multiplicative' in the sense of linear logic.

[8] Such an X would formally have s in superscript, i.e. written X^s, in [25].

The following result can essentially be found in, e.g. [25] or [13], but the initial idea was due to Paris and Wilkie [27].

Theorem 8 (PW for proofs)**.** *A V_2^0 (or U_2^0) proof of a Π_1-sentence $\forall \vec{x}.\varphi(\vec{x})$ can be translated to quasipolynomial-size bounded-depth LK-proofs of $\langle \varphi(\vec{n}) \rangle_{\vec{n} \in \mathbb{N}^{|\vec{x}|}}$.*

In this paper we will be interested in adapting an extension of this result due to Krajícek, for U_2^1.

2.3 Monotone and normal proofs in deep inference

The setting we use is due to Brünnler and McKinley [5] [26], and independently Jeřábek [22]: tree-like MLK proofs can be represented as term rewriting derivations in the following system,[9]

$$\begin{array}{ll} w{\uparrow} : \varphi \to \top & c{\uparrow} : \varphi \to \varphi \wedge \varphi \\ w{\downarrow} : \bot \to \varphi & c{\downarrow} : \varphi \vee \varphi \to \varphi \\ \multicolumn{2}{c}{s : \varphi \wedge (\psi \vee \chi) \to (\varphi \wedge \psi) \vee \chi} \end{array} \tag{1}$$

modulo associativity and commutativity of $\wedge$ and $\vee$ and the equations $A \wedge \top = A = A \vee \bot$, $\top \vee \top = \top$ and $\bot \wedge \bot = \bot$.

Definition 9 (Normal proofs)**.** A *normal* monotone proof is one where all $\uparrow$-steps occur before all $\downarrow$-steps.

Notation 10. We denote by MON the rewriting system in (1) above and by NOR the set of all normal monotone proofs.

For the sake of reducing prerequisites, we deal with MON and NOR in this paper rather than explicitly defining the associated deep inference proof systems, KS^+ and KS respectively.

In what follows we give a deep inference style presentation of rewriting derivations, first appearing in [20], in order to aid the analysis of normalisation complexity later on, e.g. in Sect. 3.

Definition 11 (Derivations)**.** We define *derivations* (or *proofs*), and *premiss* and *conclusion* functions, pr and cn resp., inductively:

- Each formula φ is a derivation with premiss and conclusion φ.
- For derivations π_1, π_2 and $\star \in \{\wedge, \vee\}$, $\pi_1 \star \pi_2$ is a derivation with premiss $\mathsf{pr}(\pi_1) \star \mathsf{pr}(\pi_2)$ and conclusion $\mathsf{cn}(\pi_1) \star \mathsf{cn}(\pi_2)$.
- If $\mathsf{cn}(\pi_1) \to \mathsf{pr}(\pi_2)$ an instance of a rule ρ then $\rho\,\dfrac{\pi_1}{\pi_2}$ is a derivation with premiss $\mathsf{pr}(\pi_1)$ and conclusion $\mathsf{cn}(\pi_2)$.

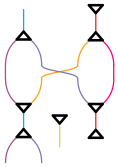
If π is a derivation where all inference steps are instances of rules in a system P with premiss φ, conclusion ψ, we write $\begin{array}{c}\varphi\\ \pi \,\|\, P\\ \psi\end{array}$.

We now introduce a certain geometric abstraction of derivations, called atomic flows. They were first introduced in [19], and the complexity of certain transformations were studied in [15]. They can be thought of as specialised versions of Buss' flow graphs [11].

Definition 12 (Atomic flows)**.** The *(atomic) flow* of a MON derivation is the (directed) graph obtained by tracing the paths of all atoms, designating nodes at $w{\downarrow}$, $w{\uparrow}$, $c{\downarrow}$ and $c{\uparrow}$ steps.

Below we give an example of a MON-derivation and its associated flow,[10] using colours to associate variable occurrences in the proof with edges in the flow:

$$s\,\dfrac{m\,\dfrac{c{\uparrow}\dfrac{p}{p \wedge p} \vee w{\uparrow}\dfrac{\bot}{c{\uparrow}\dfrac{p}{p \wedge p}}}{=\dfrac{c{\downarrow}\dfrac{p \vee p}{p}}{p \vee w{\downarrow}\dfrac{\bot}{q}} \wedge c{\downarrow}\dfrac{p \vee p}{p}}}{c{\uparrow}\dfrac{p}{p \wedge p} \vee \; = \dfrac{q \wedge w{\uparrow}\dfrac{p}{\top}}{q}}$$



(2)

Using flows, normalisation of monotone proofs can be conducted in an entirely 'syntax-free' way [19]. In particular we have the following complexity bound from [15].

Theorem 13. *A* MON *proof π can be transformed into a* NOR *proof with the same premiss and conclusion in time polynomial in the number of maximal paths in the flow of π.*

In this work it will suffice to estimate the number of paths by the following very simple upper bound:

Fact 14. *The number of maximal paths in a flow of length l is $\leq 2^l$.*

3. Monotone theories and translations

We first define some simple positive versions of the theories U_2^i and V_2^i, before considering certain extensions later, cf. [9].

Definition 15 (Positive classes and theories)**.** $\Sigma_i^{B,+}, \Pi_i^{B,+}$ are the classes of positive Σ_i^B and Π_i^B formulae, resp. The theories MU_2^i and MV_2^i are defined as U_2^i and V_2^i, resp., but with induction and comprehension formulae required to be positive.

An important observation is that the usual argument proving $U_2^0 = V_2^0$, i.e. that Σ_0^B-*PIND* can simulate Σ_0^B-*IND*, cf. [9], cannot be carried out in the monotone setting due to the use of $\supset$ symbols in that argument.

3.1 Strengthening by generalisations of comprehension

A problem with the theories defined above is that they are rather weak. Usually, the presence of induction in, say, U_2^1 allows one to 'iterate' comprehension to express more predicates. However, to prove this, we require a certain amount of negation, even if the final predicates are themselves positive. We address this problem by introducing the iterated comprehension axiom, and this will be later justified by a converse result from Sect. 4.3.

In the definition below, we assume we the presence of a *pairing* function allowing us to express sets of tuples [25] [13]. Here, we write $(a, b) \leq (a', b')$ for $a \leq a' \wedge b \leq b'$.

Definition 16 (Iterated comprehension)**.** *Length iterated comprehension*, denoted $CA_{|\omega|}$, is the following axiom schema:[11]

$$\begin{array}{l} \exists X \leq (\vec{a}, b). \forall (\vec{x}, y) < (\vec{a}, b). \\ y > 0 \supset \left[X(\vec{x}, y) \equiv \varphi\left(\vec{x}, y, X\left(-, \lfloor \frac{y}{2} \rfloor\right)\right)\right] \end{array} \tag{3}$$

CA_ω is defined as $CA_{|\omega|}$ but with $(y-1)$ in place of $\lfloor \frac{y}{2} \rfloor$.

As we mentioned, this form of comprehension is already available in the presence of Σ_1^B-*PIND*:

Proposition 17. *Σ_1^B-$CA_{|\omega|}$ is provable in U_2^1.*

[9] Strictly speaking, this is not a term rewriting system (TRS) due to the fact that the LHS of $c{\uparrow}$ and $w{\uparrow}$ is just a variable, but the notions of reduction, derivation etc. otherwise remain the same as for a TRS.

[10] In this derivation we also make use of the *medial* rule, given by $m : (\varphi_1 \wedge \varphi_2) \vee (\psi_1 \wedge \psi_2) \to (\varphi_1 \vee \psi_1) \wedge (\varphi_2 \vee \psi_2)$, to show how $c{\uparrow}$ and $c{\downarrow}$ steps can be reduced to atomic form.

[11] The notation $\varphi(X(-))$ formally corresponds to the formula $\varphi(\lambda\vec{x}.X\vec{x})$, where the meta-level λ binder is used for formal abstraction.

Proof. Let us denote (3) as $IH(b)$ and proceed by induction on b. For the inductive step, proving $IH(2b)$ from $IH(b)$, we introduce a set $X' \leq (\vec{a}, 2b)$ by Σ^B_0-CA such that:

$$\forall (\vec{x}, y) < (\vec{a}, 2b).[X'(\vec{x}, y) \equiv \varphi(\vec{x}, y, X(-, \lfloor \tfrac{y}{2} \rfloor))] \qquad (4)$$

Now, suppose $y < b$. We have that,

$$\begin{array}{rl} & X'(x, 2y) \\ \longleftrightarrow & \varphi(\vec{x}, 2y, X(\vec{t_1}, y), \dots, X(\vec{t_n}, y)) \\ \longleftrightarrow & \varphi(\vec{x}, 2y, \varphi(\vec{t_1}, y, X(-, \lfloor \frac{y}{2} \rfloor)), \dots, \varphi(\vec{t_n}, y, X(-, \lfloor \frac{y}{2} \rfloor))) \\ \longleftrightarrow & \varphi(\vec{x}, 2y, X'(\vec{t_1}, y), \dots, X'(\vec{t_n}, y)) \end{array}$$

where every occurrence of X in φ is indicated in the second line. The equivalences follow by (4), $IH(b)$ and (4) respectively, and this finishes the proof of $IH(2b)$. The proof of $IH(2b + 1)$ is similar, and the base case follows from a single application of CA. □

Notice that the above proof is constructive, a useful observation for when we consider intuitionistic theories in Sect. 4.3.

If φ is positive in (3), then we will see that the Paris-Wilkie translation can be adapted to find monotone propositional formulae witnessing this existential. Consequently, we consider theories obtained by adding $\Sigma^{B,+}_0$-$CA_{|\omega|}$ to MU^1_2 and MV^1_2.

Notation 18. We write $\underline{MU^1_2}$ for $MU^0_2 + \Sigma^{B,+}_0$-$CA_{|\omega|}$, $\underline{MV^{0.5}_2}$ for $MV^0_2 + \Sigma^{B,+}_0$-$CA_{|\omega|}$ and $\underline{MV^1_2}$ for $MV^0_2 + \Sigma^{B,+}_0$-CA_ω.

These theories are *not* conservative extensions, but we justify this notation by Prop. 17 above and the converse results in Sect. 4.3.

3.2 Witnessing set existentials by SO terms: part I

Second-order theories are often hasslesome for the Paris-Wilkie translation since it is not clear how to handle set quantifiers. They are often translated by *extension* variables, e.g. in [25], although these may introduce negation in the propositional translation.[12]

For this reason we develop an appropriate term language for comprehension and thus eliminate occurrences of existential set quantifiers altogether. This result scales up to our intuitionistic theories later on, albeit with additional complications, which is helpful since notions of quantifier complexity beyond Σ^B_0 are not well-defined in intuitionistic versions of arithmetic.

Definition 19 (Comprehension terms)**.** We extend $\mathcal{L}_2$ by SO terms,

$$\{\vec{a} < \vec{t} : \varphi\} \quad \text{and} \quad T_{\varphi, \vec{t}}$$

parametrised by FO terms $\vec{t}$, variables $\vec{a}$ and formulae φ.

Φ-CT is the set of initial double-sequents,

$$\vec{x} \in \{\vec{a} < \vec{t} : \varphi(\vec{a})\} \longleftrightarrow \vec{x} < \vec{t} \wedge \varphi(\vec{x})$$

for each $\varphi \in \Phi$, and Φ-$CT_{|\omega|}$ is the set of initial double-sequents,

$$T_{\varphi, \vec{s}, t}(\vec{x}, y) \longleftrightarrow y > 0 \wedge (\vec{x}, y) < (\vec{s}, t) \wedge \varphi(T_{\varphi, \vec{s}, t}(-, \lfloor \tfrac{y}{2} \rfloor))$$

Intuitively, the initial sequents for $CT_{|\omega|}$ evaluates the fixed point defined by the comprehension formula. It is not difficult to see that, over any SO theory, we have the following results:

Lemma 20. *Φ-CT, Φ-$CT_{|\omega|}$ and Φ-CT_ω conservatively extend Φ-CA, Φ-$CA_{|\omega|}$ and Φ-CA_ω resp.*

Theorem 21. *$\Sigma^{B,+}_0$ theorems of $\underline{MU^1_2}$, $\underline{MV^{0.5}_2}$ and $\underline{MV^1_2}$ have proofs containing only $\Sigma^{B,+}_0$-formulae, using $CT_{|\omega|}$, $CT_{|\omega|}$ and CT_ω resp. instead of CA.*

Proof. Follows from free-cut elimination, Thm. 5, and Lemma 20 above, replacing existentially quantified set variables by terms. □

Finally, we can extend the Paris-Wilkie translation of closed formulae to account for comprehension terms.

Definition 22 (PW for comprehension terms)**.** We define:

$$\begin{array}{rcl} \langle \vec{s} \in \{\vec{a} < \vec{t} : \varphi\} \rangle & := & \langle \vec{s} < \vec{t} \rangle \wedge \langle \varphi(\vec{s}) \rangle \\ \langle T_{\varphi, \vec{s}, t}(\vec{r}, u) \rangle & := & \langle \vec{r} \leq \vec{s} \rangle \wedge \langle u < t \rangle \wedge \langle \varphi(T_{\varphi, \vec{s}, t}(-, \lfloor \frac{u}{2} \rfloor)) \rangle \end{array}$$

Notice that the case of $CT_{|\omega|}$ computes the fixed point of φ by a monotone propositional formula of low complexity:

Fact 23. *$\langle T_{\varphi, \vec{a}, b}(\vec{s}, t) \rangle$ has polylogarithmic depth and quasipolynomial size in $v(\vec{s})$, $v(t)$, for $CT_{|\omega|}$.*

Using $CT_{|\omega|}$ we can, for example, express the *threshold functions* from [1], [2] [8] [16]:

$$\begin{array}{rcl} \mathrm{th}(x, a, 0) & \longleftrightarrow & x = 0 \vee (x = 1 \wedge a \in X) \\ \mathrm{th}(x, a, b) & \longleftrightarrow & \exists y \leq x. \left(\begin{array}{rl} & \mathrm{th}(y, a, \lfloor \frac{b}{2} \rfloor) \\ \wedge & \mathrm{th}(x - y, a + \lfloor \frac{b}{2} \rfloor, \lceil \frac{b}{2} \rceil) \end{array} \right) \end{array}$$

Clearly, there are simple propositional proofs of the PW translations of the initial sequents from CT and $CT_{|\omega|}$.

3.3 Paris-Wilkie translation for monotone theories

We present a version of the Paris-Wilkie translation from our monotone theories to deep inference derivations, focussing on the length of the atomic flows obtained to derive complexity bounds for NOR later on. A minor contribution to the literature here is our presentation of the Paris-Wilkie translation in deep inference style, thanks in large part to insights from previous works, e.g. [5] [22] [16].

First, let us extend $\langle \cdot \rangle$ to the LHS and RHS of sequents. We define $\langle \Gamma \rangle_l$ as $\bigwedge\limits_{\varphi \in \Gamma} \langle \varphi \rangle$ and $\langle \Gamma \rangle_r$ as $\bigvee\limits_{\varphi \in \Gamma} \langle \varphi \rangle$.

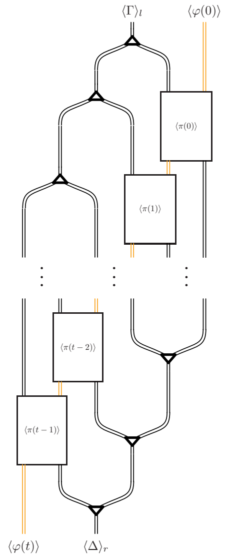
Definition 24 (PW for proofs)**.** We extend the translation $\langle \cdot \rangle$ to proofs $\pi(\vec{x})$ in $\underline{MV^{0.5}_2}$ or $\underline{MU^1_2}$ of a $\Sigma^{B,+}_0$ sequent $\Gamma(\vec{x}) \rightarrow \Delta(\vec{x})$, mapping to derivations $\begin{array}{c} \langle \Gamma(\vec{n}) \rangle_l \\ {\scriptstyle \langle \pi(\vec{n}) \rangle} \Big\Vert {\scriptstyle \mathrm{MON}} \\ \langle \Delta(\vec{n}) \rangle_r \end{array}$ for $\vec{n} \in \mathbb{N}^{|\vec{x}|}$, by induction on the number of inference steps in $\pi(\vec{x})$.

The most significant step, from the point of view of complexity is if a proof $\pi(a)$ extended by an induction step:

$$IND \, \frac{\Gamma, \varphi(a) \rightarrow \varphi(a + 1), \Delta}{\Gamma, \varphi(0) \rightarrow \varphi(t), \Delta}$$

This is translated to the following derivation:

$$\begin{array}{rc}
 & c{\uparrow}\dfrac{\langle \Gamma \rangle_l}{\langle \Gamma \rangle_l \wedge \langle \Gamma \rangle_l} \wedge \langle \varphi(0) \rangle \\ \hline
= & c{\uparrow}\dfrac{\langle \Gamma \rangle_l}{\langle \Gamma \rangle_l \wedge \langle \Gamma \rangle_l} \wedge \begin{array}{c} \langle \Gamma \rangle_l \wedge \langle \varphi(0) \rangle \\ {\scriptstyle \langle \pi(0) \rangle} \Big\Vert \\ \langle \varphi(1) \rangle \vee \langle \Delta \rangle_r \end{array} \\ \hline
s & c{\uparrow}\dfrac{\langle \Gamma \rangle_l}{\langle \Gamma \rangle_l \wedge \langle \Gamma \rangle_l} \wedge \left[\begin{array}{c} \langle \Gamma \rangle_l \wedge \langle \varphi(1) \rangle \\ {\scriptstyle \langle \pi(1) \rangle} \Big\Vert \\ \langle \varphi(2) \rangle \vee \langle \Delta \rangle_r \end{array} \vee \langle \Delta \rangle_r \right] \\ \hline
s & \vdots \qquad \vdots \qquad \vdots \\ \hline
s & \langle \Gamma \rangle_l \wedge \left[\begin{array}{c} \langle \Gamma \rangle_l \wedge \langle \varphi(t-2) \rangle \\ {\scriptstyle \langle \pi(t-2) \rangle} \Big\Vert \\ \langle \varphi(t-1) \rangle \vee \langle \Delta \rangle_r \end{array} \vee c{\downarrow}\dfrac{\langle \Delta \rangle_r \vee \langle \Delta \rangle_r}{\langle \Delta \rangle_r} \right] \\ \hline
s & \begin{array}{c} \langle \Gamma \rangle_l \wedge \langle \varphi(t-1) \rangle \\ {\scriptstyle \langle \pi(t-1) \rangle} \Big\Vert \\ \langle \varphi(t) \rangle \vee \langle \Delta \rangle_r \end{array} \vee c{\downarrow}\dfrac{\langle \Delta \rangle_r \vee \langle \Delta \rangle_r}{\langle \Delta \rangle_r} \\ \hline
= & \langle \varphi(t) \rangle \vee c{\downarrow}\dfrac{\langle \Delta \rangle_r \vee \langle \Delta \rangle_r}{\langle \Delta \rangle_r}
\end{array}$$



[12] Intuitively, one expects that this negation can be eliminated, but existing versions of free-cut elimination, e.g. from [13], do not quite yield this.

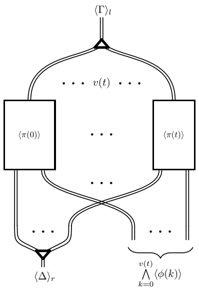
By following the path of the induction formula (in orange), notice that this multiplies the length of flow by $v(t)$, a possibly quasipolynomial factor. The case for $PIND$ is analogous to IND, but crucially the length of flow is only multiplied by $\lceil \log v(t) \rceil$, a logarithmic factor.

A proof $\pi(a)$ extended by a ∀-r step,

$$\forall\text{-r}\ \frac{\Gamma, a \le t \to \Delta, \varphi(a)}{\Gamma \to \Delta, \forall x \le t.\varphi(x)}$$

is translated to the derivation below,

$$\begin{array}{c} = \dfrac{c\uparrow \dfrac{\langle\Gamma\rangle_l}{\langle\Gamma\rangle_l \wedge \cdots \wedge \langle\Gamma\rangle_l} \wedge = \dfrac{\top}{\top \wedge \cdots \wedge \top}}{\langle\Gamma\rangle_l \wedge \langle 0 \le t\rangle \qquad\qquad \langle\Gamma\rangle_l \wedge \langle v(t) \le t\rangle} \\ \langle\pi(0)\rangle \Big\| \qquad \wedge \ \cdots \wedge \qquad \langle\pi(t)\rangle \Big\| \\ s\ \dfrac{\langle\Delta\rangle_r \vee \langle\varphi(0)\rangle \qquad\qquad \langle\Delta\rangle_r \vee \langle\varphi(t)\rangle}{c\downarrow \dfrac{\langle\Delta\rangle_r \vee \cdots \vee \langle\Delta\rangle_r}{\langle\Delta\rangle_r} \vee \bigwedge\limits_{k=0}^{v(t)} \langle\varphi(k)\rangle} \end{array}$$



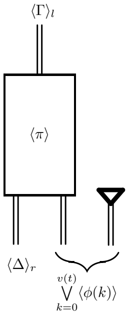
where we notice that $\langle n \le t\rangle$ is $\top$ for all $n \le v(t)$. With regards to the length of the flow, besides that inherited from each $\pi(i)$, notice that the $v(t)$ $c\uparrow$ nodes at the top (for each atom occurrence in $\langle\Gamma\rangle_l$) can be implemented by a complete (almost) balanced tree of depth $\lceil \log v(t) \rceil$, and similarly for the $c\downarrow$ nodes corresponding to $\langle\Delta\rangle_r$.

A proof π extended by a ∃-r step,

$$\exists\text{-r}\ \frac{\Gamma \to \Delta, \varphi(s)}{\Gamma, s \le t \to \Delta, \exists x \le t.\varphi(x)}$$

is translated to the derivation below,

$$\begin{array}{c} = \dfrac{\langle\Gamma\rangle_l \wedge \top}{\langle\Gamma\rangle_l} \\ \langle\pi\rangle \Big\| \\ \left[\langle\Delta\rangle_r \vee\ w\downarrow \dfrac{\langle\varphi(s)\rangle}{\bigvee\limits_{k=0}^{v(t)} \langle\varphi(k)\rangle} \right] \end{array}$$



assuming $v(s) \le v(t)$, and so $\langle s \le t\rangle$ is $\top$. Otherwise $\langle s \le t\rangle$ is $\bot$ and the derivation is just composed of several $w\uparrow$ and $w\downarrow$ steps.

The composition of two proofs by cut is translated as follows:

$$cut\ \frac{\begin{array}{c}\pi_1 \\ \Gamma \to \Delta, \varphi\end{array} \quad \begin{array}{c}\pi_2 \\ \Sigma, \varphi \to \Pi\end{array}}{\Gamma, \Sigma \to \Delta, \Pi} \qquad \rightsquigarrow \qquad \begin{array}{c} \langle\Gamma\rangle_l \\ \langle\pi_1\rangle \| \qquad \wedge \langle\Sigma\rangle_l \\ s\ \dfrac{\langle\Delta\rangle_r \vee \langle\varphi\rangle}{\langle\varphi\rangle \wedge \langle\Sigma\rangle_l} \\ \langle\Delta\rangle_r \vee \quad \langle\pi_2\rangle \| \\ \langle\Pi\rangle_r \end{array}$$

This can be seen as a simpler version of the translation of an induction step, where the length of flows is increased by only a constant factor rather than a logarithmic factor.

In a similar way, the translations of ∨ and ∧ steps are simpler versions of ∃ and ∀ steps, respectively, increasing flow length by at most addition of a constant rather than addition of a logarithm.

Finally, the translation of structural steps affect length of a flow by at most addition of a constant. The case for weakening, w-l and w-r, can also be seen as a simpler version of the case for ∃-r above. For instance, a proof π extended by a c-r step is translated as follows,

$$c\text{-r}\ \frac{\begin{array}{c}\pi \\ \Gamma \to \Delta, \varphi, \varphi\end{array}}{\Gamma \to \Delta, \varphi} \qquad \rightsquigarrow \qquad \begin{array}{c} \langle\Gamma\rangle_l \\ \langle\pi\rangle \| \\ \langle\Delta\rangle_r \vee c\downarrow \dfrac{\langle\varphi\rangle \vee \langle\varphi\rangle}{\langle\varphi\rangle} \end{array}$$

whence the case for c-l is dual.

A routine complexity analysis gives us the following:

Theorem 25. *If $\underline{MV}_2^{0.5}$ proves a $\Sigma_0^{B,+}$ sequent $\Gamma(\vec{x}) \to \Delta(\vec{x})$, there are derivations* $\begin{array}{c}\langle\Gamma(\vec{n})\rangle_l \\ \| \textsc{Mon} \\ \langle\Delta(\vec{n})\rangle_r\end{array}$ *of size quasipolynomial in $\vec{n} \in \mathbb{N}^{|\vec{x}|}$.*

3.4 $\langle\cdot\rangle$ on $\underline{MU}_2^1$ normalises in quasipolynomial time

As we mentioned, $\langle\cdot\rangle$ on $PIND$-steps multiplies the length of a flow by a polylogarithmic factor, due to the divide-and-conquer format of the induction.

Lemma 26. *$\langle\cdot\rangle$ on $\underline{MU}_2^1$ proofs induces atomic flows of polylogarithmic length.*

We can now apply the normalisation result, Thm. 13, and Fact 14 to obtain one of our main results:

Theorem 27. *If $\underline{MU}_2^1$ proves a $\Sigma_0^{B,+}$ sequent $\Gamma(\vec{x}) \to \Delta(\vec{x})$, there are derivations* $\begin{array}{c}\langle\Gamma(\vec{n})\rangle_l \\ \| \textsc{Nor} \\ \langle\Delta(\vec{n})\rangle_r\end{array}$ *of size quasipolynomial in $\vec{n} \in \mathbb{N}^{|\vec{x}|}$.*

4. Intuitionistic theories and translations

Unfortunately, the monotone setting in arithmetic does not allow us to readily conduct metalogical reasoning, and so it does not seem possible to prove soundness results (or 'reflection' principles).

Therefore we introduce an *intuitionistic* hierarchy of theories in which to conduct such reasoning. The idea here is to view intuitionistic implication under the Brouwer-Heyting-Kolmogorov interpretation, as a "transformation of proofs". In this way we can extend the PW-translation to deal with implication without breaking monotonicity.[13]

Remark 28. Previous work on intuitionistic bounded arithmetic has included only positive induction for versions of Buss' theory S_2 [10] [14], in order to conduct realizability arguments. In those settings one can, in fact, simulate the full power of non-positive induction, but it is not possible in our setting due to the presence of set symbols.

4.1 The hierarchy of type levels in intuitionistic logic

In order to simplify the definition of a higher type Paris-Wilkie translation later on, here we only work with formulae that are $(\forall, \wedge, \supset)$-combinations of $\Sigma_0^{B,+}$-formulae, as is common in realizability and Dialectica style interpretations. Disjunction and existentials, as expected, cause genuine difficulties that are cumbersome to deal with, cf. Sect. 6.4. Nonetheless, we point out that this fragment suffices to prove the various results in the converse direction that we seek, in particular Thm. 49, and so we still attain the required correspondence for this theory of arithmetic.

Definition 29 (Levels)**.** Define L_0 to be the set of positive formulae (of 'type level 0'). For $j > 0$ we define L_j as follows:

- If $\varphi \in L_{j-1}$ then $\varphi \in L_j$.

[13] Such an approach is not generally available in classical logic due to De Morgan laws, which induce a collapse of negation to the atoms.

- If $\varphi \in L_{j-1}$ and $\psi \in L_j$ then $\varphi \supset \psi \in L_j$.
- If $\varphi \in L_j$ and $\psi \in L_j$ then $\varphi \wedge \psi \in L_j$.
- If $\varphi \in L_j$ then $\forall x \leq t.\varphi \in L_j$.

The set of bounded formulae of level j, $L_j \cap \Sigma_0^B$, is denoted Σ_0^{B,L_j}. We write Σ_1^{B,L_j} for the set of formulae $\exists \vec{X} \leq \vec{t}.\varphi$, for $\varphi \in \Sigma_0^{B,L_j}$.

We write $L_j J$ and $L_j K$ to denote the fragments of LJ and LK, respectively, consisting of only (propositional) L_j formulae.

Henceforth, let us assume that theories are based over intuitionistic logic, unless otherwise mentioned.

Definition 30 (Intuitionistic theories)**.** For $i = 0, 1$ define the theory $I_j U_2^i$ as U_2^i but with induction formulae in Σ_i^{B,L_j} and comprehension formulae in $\Sigma_0^{B,+}$.

Remark 31 (Quantifiers in intuitionistic logic)**.** There is no canonical notion of quantifier hierarchy in intuitionistic logic, namely due to the lack of a general prenex normal form for formulae. Various hierarchies have been proposed for intuitionistic versions of bounded arithmetic, e.g. in [10] [21] in order to mimic associated complexity hierarchies, but this is beyond the scope of this work.

We point out that the notion of bounded formulae, Σ_0^B, remains the same in both the classical setting and the intuitionistic setting. Our notion of Σ_1^{B,L_j} is in the 'strict' sense of [13], and we will later eliminate these existentials altogether in favour of a formulation using set terms, as in Sect. 3.2, allowing us to remain amongst Σ_0^B formulae where quantifier behaviour is more robust.

4.2 On the relative strength of theories

In this section we address the relative strength of our intuitionistic theories with the positive theories defined earlier, as well as their more well known classical versions.

From [10] we have that the law of excluded middle holds for all quantifier-free formulae free of set symbols already in IS_2, and so also $I_0 U_2^0$, which helps prove some of the results here:

Proposition 32 (Classical reasoning)**.** *If $U_2^0 \vdash \varphi$ and φ is free of quantifiers and set symbols then $I_0 U_2^0 \vdash \varphi$.*

By inspection of the rules, or by alluding to a *multiple conclusion* version of the intuitionistic calculus (e.g. from [18]), notice that there are only two rules of LK^2 that cannot be simulated by LJ^2: $\supset$-r and $\forall$-r. In particular this yields the following, which was observed in [4]:

Proposition 33. *The positive propositional fragments MLJ and MLK of LJ and LK resp. polynomially simulate each other.*

Both $\supset$-r and $\forall$-r require restriction of one formula on the right to be intuitionistically valid. While the former is an inherently non-constructive principle, the latter, which is freely available in MU_2^i and MV_2^i, can be simulated by an induction argument:

Proposition 34. *$I_1 U_2^1 \vdash \forall x \leq t.(\varphi(x) \vee \psi) \to (\forall x \leq t.\varphi(x) \vee \psi)$, where φ and ψ are $\Sigma_0^{B,+}$ and x does not occur free in ψ.*

Proof. We reason inside the theory $I_1 U_2^1$ and prove the following L_1 formula by polynomial induction on y:

$$\forall y.\forall x \leq (t-y).\left[\begin{array}{cc} & \forall z \in [x, x+y).(\varphi(z) \vee \psi) \\ \supset & \forall z \in [x, x+y).\varphi(z) \vee \psi) \end{array}\right] \quad (5)$$

Let $\chi(x,y)$ be such that the formula (5) is $\forall y.\forall x \leq (t-y).\chi(x,y)$. The base case, when $y = 0$, is simple since the quantifiers in $\chi(x,y)$ collapse to enforcing $z = x$, whence $\chi(x,y)$ is equivalent to the identity formula $(\varphi(x) \vee \psi) \supset (\varphi(x) \vee \psi)$.

Now assume, for some b, we have that $\forall x \leq (t-b).\chi(x,b)$, and let $a \leq (t-2b)$. We will attempt to show that $\chi(a, 2b)$. Notice that from $a \leq (t-2b)$ we have that $a \leq (t-b)$ and $(a+b) \leq (t-b)$, by classical reasoning and Prop. 32 above. Therefore, by the inductive hypothesis we have that $\chi(a,b)$ and $\chi(a+b,b)$.

Now, let us assume the antecedent, say $\chi_1(a,2b)$, of $\chi(a,2b)$, i.e. $\forall z \in [a, a+2b).(\varphi(z) \vee \psi)$, and attempt to deduce the succedent, say $\chi_2(a,2b)$, i.e. $\forall z \in [a, a+2b).\varphi(z) \vee \psi$. Notice that, due to the intuitionistic setting, we cannot at this point query the universal quantifier occurring in the succedent since it is underneath a disjunction. Instead, again by Prop. 32, we have:

$$c \in [a, a+2b) \equiv c \in [a, a+b) \vee c \in [a+b, a+2b) \quad (6)$$

Consequently, by the right-left direction of 6 above, from $\chi_1(a,2b)$ we can deduce $\forall z \in [a, a+b).(\varphi(z) \vee \psi)$ and $\forall z \in [a+b, a+2b)$, i.e. $\chi_1(a,b)$ and $\chi_1(a+b,b).(\varphi(z) \vee \psi)$.

Finally, since we already have $\chi(a,b)$ and $\chi(a+b,b)$ from the inductive hypothesis, we can conclude $\chi_2(a,b)$ and $\chi_2(a+b,b)$. From here we can apply the left-right direction of (6) along with basic logical manipulations to obtain $\chi_2(a,2b)$ as required.

The inductive step for $y = 2b+1$ is similar. The theorem now follows from (5) by setting $y = t$ and conducting basic logical manipulations. □

From here we arrive at a useful normal form for our higher-type Paris-Wilkie translation later on:

Corollary 35. *Every $\Sigma_0^{B,+}$-formula is equivalent in $I_1 U_2^1$ to one in prenex normal form.*

The usual simulation of propositional MLK in propositional LJ, i.e. Prop. 33, is carried over by converting the succedents of MLK-sequents to disjunctions of their formulae. We just showed, in Prop. 34 above, that this approach also admits simulation of the $\forall$-r rule once L_1-$PIND$ is available.

The intuitionistic formulations of induction rules, with no side-formulae on the right, turn out to have equal strength to their classical formulations, by a routine argument. Furthermore, we can observe that the usual argument simulating IND from $PIND$, e.g. from [12] or [9], is constructive and requires only an increase by 1 in the type-level of induction formulae:

Proposition 36. *$\Sigma_0^{B,L_{j+1}}$-$PIND$ proves Σ_0^{B,L_j}-IND, for $j \geq 0$.*

Finally, since the proof of Prop. 17 is constructive, we have:

Proposition 37. *Σ_1^B-$CA_{|\omega|}$ is provable in $I_1 U_2^1$.*

Proof. Only Σ_1^{B,L_1}-$PIND$ is used in the proof of Prop. 17. □

We can now conclude the following.

Theorem 38 (Inclusions)**.** *$I_0 U_2^1 \subseteq \underline{MU_2^1} \subseteq \underline{MV_2^{0.5}} \subseteq I_1 U_2^1$.*

Proof. The first two inclusions are routine. The final inclusion follows from Props. 33, 34, 36 and 37. □

4.3 Witnessing set existentials by SO terms: part II

For the same reasons as Sect. 3.2, and the difficulty of handling quantifiers in intuitionistic logic, we wish to eliminate occurrences of second-order quantification in our intuitionistic theories. The arguments are a little more involved now that we have access to induction on more complex formulae, but we are nonetheless able to work with the same comprehension terms and rules as before.

We will assume that every Σ_1^{B,L_j} formula has just one second-order existential quantifier.[14] Our main witnessing lemma is the following:

[14] This can be achieved by the usual trick of string interleaving, cf. [13].

Lemma 39. *Suppose $j > 0$ and $I_jU^1_2 \vdash \Gamma(\vec{a}, \vec{A}) \to \exists X.\varphi(X, \vec{a}, \vec{A})$, where all free variables are indicated. Then there is a $\Sigma^{B,+}_0$-$CT_{|\omega|}$ term $T(\vec{a}, \vec{A})$ such that $I_jU^1_2 \vdash \Gamma(\vec{a}, \vec{A}) \to \varphi(T(\vec{a}, \vec{A}), \vec{a}, \vec{A})$.*

Proof sketch. By induction on the number of inference steps in a free-cut free proof π. The only problematic case is when π consists of a subproof π' followed by a $PIND$ step,

$$_{PIND}\,\frac{\Gamma, \exists X \leq s.\varphi(X, \lfloor \frac{a}{2} \rfloor) \to \exists X \leq s.\varphi(X, a)}{\Gamma, \exists X \leq s.\varphi(X, 0) \to \exists X \leq s.\varphi(X, t)}$$

with free variables amongst $\vec{a}, \vec{A}$. We then have a proof of,

$$\Gamma, A \leq s, \varphi(A, \lfloor \tfrac{a}{2} \rfloor) \to \exists X.\varphi(X, a)$$

from which we have a term $R(A)$ (with free variables from $\vec{a}, \vec{A}$), by the inductive hypothesis, and a proof $\pi'(A)$ of:

$$\Gamma, A \leq s, \varphi(A, \lfloor \tfrac{a}{2} \rfloor) \to R(A) \leq s \wedge \varphi(R(A), a)$$

Now, by $\Sigma^{B,+}_0$-$CT_{|\omega|}$, we have a term $T_{R,s,a}$ and initial sequents:

$$T_{R,s,a}(x, y) \longleftrightarrow y > 0 \wedge (x, y) < (s, a) \wedge R(T_{R,s,a}(-, \lfloor \tfrac{y}{2} \rfloor))(x)$$

Finally, we can apply $PIND$ after $\pi'(T_{R,s,a})$ to obtain a proof of the required format. □

From here we can obtain our quantifier-elimination result:

Theorem 40. *For $j > 0$, $I_jU^1_2$ is equivalent to $I_jU^0_2 + \Sigma^{B,+}_0$-$CT_{|\omega|}$ over $\Sigma^{B,+}_0$-theorems.*

Proof. Since the proof of Prop. 17 can be made constructive in $I_1U^1_2$, and so the theorem follows from Lemma 39 above. □

Notation 41. Following the shorthands from Sect. 3, we will write $\underline{I}_j\underline{U}^1_2$ for $I_jU^0_2 + \Sigma^{B,+}_0$-$CT_{|\omega|}$, $\underline{I}_j\underline{V}^{0.5}_2$ for $I_jV^0_2 + \Sigma^{B,+}_0$-$CT_{|\omega|}$ and $\underline{I}_j\underline{V}^1_2$ for $I_jV^0_2 + \Sigma^{B,+}_0$-$CT_\omega$.

4.4 Paris-Wilkie translation for $I_jU^1_2$ and $I_jV^1_2$

For convenience we will switch back to the sequent calculus presentation of monotone proofs, MLK, whose tree-like variant is polynomially equivalent to MON [22]. It is just as simple to conduct the translation to MON, but already existing concepts and terminology for the sequent calculus makes it slightly easier to explain the translation; in particular, the existence of a sequent arrow ($\to$) at the meta-level makes it simple to translate implications between monotone formulae to monotone sequents.

This way, it will also be clearer from our translation how to obtain a correspondence for dag-like MLK, for which there is no standard definition of a corresponding system based on MON.

As expected for realizability-style translations, it is contractive behaviour that generates complexity, this time in the dependency graph of a dag-like MLK proof. However, the length of this graph is tamed just like in Sect. 3.4, by relying on $PIND$.

Definition 42 (Formula and sequent translation)**.** Set $\langle\!\langle \cdot \rangle\!\rangle^0 = \langle \cdot \rangle$, and for $j > 0$, we define a translation $\langle\!\langle \cdot \rangle\!\rangle^j$ from closed bounded L_j formulae to multisets of propositional L_{j-1} sequents as follows:

- If $\varphi \in L_{j-1}$ then, $\langle\!\langle \varphi \rangle\!\rangle^j := \{ \ \ \to \langle \varphi \rangle \}$
- If $\varphi \in L_{j-1}$ and $\psi \in L_j$ then:
$$\langle\!\langle \varphi \supset \psi \rangle\!\rangle^j \quad := \quad \left\{ \langle \varphi \rangle, \Gamma \to \Delta \quad : \quad \Gamma \to \Delta \ \in \ \langle\!\langle \psi \rangle\!\rangle^j \right\}$$
- If $\varphi, \psi \in L_j$ then $\langle\!\langle \varphi \wedge \psi \rangle\!\rangle^j := \langle\!\langle \varphi \rangle\!\rangle^j \cup \langle\!\langle \psi \rangle\!\rangle^j$.
- If $\varphi \in L_j$ then $\langle\!\langle \forall x \leq t.\varphi(x) \rangle\!\rangle^j := \bigcup\limits_{k=0}^{v(t)} \langle\!\langle \varphi(k) \rangle\!\rangle^j$.
- For a cedent Γ of L_j formulae, $\langle\!\langle \Gamma \rangle\!\rangle := \bigcup\limits_{\varphi \in \Gamma} \langle\!\langle \varphi \rangle\!\rangle^j$.

In what follows, we will use S and its decorations to vary over sequents, and we write $\begin{array}{c} \vec{S} \\ \mid_{\pi} \\ S \end{array}$ for a (dag-like) sequent derivation called π with premisses the (multi)set or list $\vec{S}$ and conclusion S.

Before proceeding to give the generalised Paris-Wilkie translation of $I_jU^1_2$ proofs, we first give a version of the *deduction theorem* that will be useful, e.g. for the $\supset$-r case in our translation.

Lemma 43 (Deduction)**.** *An L_jJ derivation $\begin{array}{c} \to \varphi \\ \mid_{\pi} \\ \to \psi \end{array}$ can be polynomially transformed to an L_jJ proof π' of $\varphi \to \psi$, and vice-versa.*

Proof. The right-left direction is simply obtained by cutting $\to \varphi$ against the conclusion $\varphi \to \psi$ of π'. For the left-right direction, we append the cedent φ to the left-hand side of all sequents occurring in the derivation π: $\begin{array}{c} \varphi \to \varphi \\ \mid_{\varphi, \pi} \\ \varphi \to \psi \end{array}$. It is not difficult to see that the derivation remains valid in L_jJ and, moreover, begins with a correct initial sequent. □

Definition 44 (Translation of proofs)**.** For $j > 0$, an $\underline{I}_j\underline{U}^1_2$ or $\underline{I}_j\underline{V}^{0.5}_2$ proof π of a sequent $\Sigma \to \varphi$ is translated by $\langle\!\langle \cdot \rangle\!\rangle^j$ to a multiset of (dag-like) $L_{j-1}J$ derivations of the following format:

$$\left\{ \begin{array}{c} \langle\!\langle \Sigma \rangle\!\rangle^j \\ \mid_{\langle\!\langle \pi \rangle\!\rangle^j_S} \\ S \end{array} \quad : \quad S \ \in \ \langle\!\langle \varphi \rangle\!\rangle^j \right\}$$

The translation is again by induction on the structure of an arithmetic proof π. We give some key steps in the translation below, henceforth fixing j and suppressing it in superscripts.

If π consists of subproofs π_1 and π_2 followed by a cut step,

$$_{cut}\,\frac{\Sigma \to \varphi \quad \Pi, \varphi \to \psi}{\Pi, \Sigma \to \psi}$$

then by the inductive hypothesis we have derivations $\begin{array}{c} \langle\!\langle \Sigma \rangle\!\rangle \\ \mid_{\langle\!\langle \pi_1 \rangle\!\rangle_S} \\ S \end{array}$ for each $S \in \langle\!\langle \varphi \rangle\!\rangle$, and derivations $\begin{array}{c} \langle\!\langle \Pi \rangle\!\rangle \\ \langle\!\langle \varphi \rangle\!\rangle \\ \mid_{\langle\!\langle \pi_2 \rangle\!\rangle_{S'}} \\ S' \end{array}$ for each $S' \in \langle\!\langle \psi \rangle\!\rangle$. Let $\langle\!\langle \varphi \rangle\!\rangle = \{S_i \ : \ i \leq n\}$ and, for each $S' \in \langle\!\langle \psi \rangle\!\rangle$, we define,

$$\langle\!\langle \pi \rangle\!\rangle_{S'} \quad := \quad \begin{array}{c} \langle\!\langle \Pi \rangle\!\rangle \\ \langle\!\langle \Sigma \rangle\!\rangle \\ \mid_{\langle\!\langle \pi_1 \rangle\!\rangle_{S_0}} \\ S_0 \\ \mid_{\langle\!\langle \pi_1 \rangle\!\rangle_{S_1}} \\ \vdots \\ \mid_{\langle\!\langle \pi_1 \rangle\!\rangle_{S_n}} \\ S_n \\ \mid_{\langle\!\langle \pi_2 \rangle\!\rangle_{S'}} \\ S' \end{array}$$

where $\langle\!\langle \Sigma \rangle\!\rangle$ is used once for each $\langle\!\langle \pi_1 \rangle\!\rangle_{S_i}$.

If π consists of a subproof π' followed by a c-l step,

$$_{c\text{-l}}\,\frac{\Gamma, \varphi, \varphi \to \psi}{\Gamma, \varphi \to \psi}$$

then, for $S \in \langle\!\langle \psi \rangle\!\rangle$, $\langle\!\langle \pi \rangle\!\rangle_S$ is defined as $\langle\!\langle \pi' \rangle\!\rangle_S$, deleting one of the occurrences of each formula χ in $\langle\!\langle \varphi \rangle\!\rangle$; from the point of view of the dependency graph, any later sequents previously relying on the deleted occurrence now rely on the remaining occurrence of χ.

If a proof π consists of a subproof π' followed by a $\supset$-r step,

$$\supset\!\text{r}\ \frac{\Sigma, \varphi \to \psi}{\Sigma \to \varphi \supset \psi}$$

then, again, notice that φ must be in L_{j-1}, since $\varphi \supset \psi$ must be in L_j. Therefore, by the inductive hypothesis, we have derivations $\begin{array}{l}\langle\!\langle\Sigma\rangle\!\rangle\\ \ \to\langle\varphi\rangle\\ \ \big|\,{\scriptstyle\langle\!\langle\pi'\rangle\!\rangle_S}\\ \ S\end{array}$ for each $S \in \langle\!\langle\psi\rangle\!\rangle$. From here, we can obtain a definition of $\langle\!\langle\pi\rangle\!\rangle_S$ of the appropriate format by simply applying the deduction theorem, Lemma 43.

If π consists of subproofs π_1 and π_2 followed by a $\supset$-l step,

$$\supset\!\text{l}\ \frac{\Sigma \to \varphi \quad \Pi, \psi \to \chi}{\Pi, \varphi \supset \psi, \Sigma \to \chi}$$

then notice that φ must be L_{j-1}, since $\varphi \supset \psi$ must be in L_j. Therefore, by the inductive hypothesis, we have a derivation $\begin{array}{l}\langle\!\langle\Sigma\rangle\!\rangle\\ \ \big|\,{\scriptstyle\langle\!\langle\pi_1\rangle\!\rangle_\varphi}\\ \to\langle\varphi\rangle\end{array}$ and derivations $\begin{array}{l}\langle\!\langle\Pi\rangle\!\rangle\\ \langle\!\langle\psi\rangle\!\rangle\\ \ \big|\,{\scriptstyle\langle\!\langle\pi_2\rangle\!\rangle_S}\\ \ S\end{array}$ for each $S \in \langle\!\langle\chi\rangle\!\rangle$.

Let $\langle\!\langle\psi\rangle\!\rangle = \{\Gamma_i \to \Delta_i \,:\, i \leq n\}$ and, for $S \in \langle\!\langle\chi\rangle\!\rangle$, we define,

$$\langle\!\langle\pi\rangle\!\rangle_S \quad := \quad \begin{array}{c}\langle\!\langle\Pi\rangle\!\rangle\\ \langle\varphi\rangle, \Gamma_0 \to \Delta_0\\ \big|\,{\scriptstyle\langle\!\langle\varphi\supset\psi\rangle\!\rangle}\\ \langle\varphi\rangle, \Gamma_n \to \Delta_n\\ \langle\!\langle\Sigma\rangle\!\rangle\\ \big|\,{\scriptstyle\langle\!\langle\pi_1\rangle\!\rangle_\varphi}\\ \to\langle\varphi\rangle\\ \Gamma_0 \to \Delta_0\\ {\scriptstyle cut}\,\big|\\ \Gamma_n \to \Delta_n\\ \big|\,{\scriptstyle\langle\!\langle\pi_2\rangle\!\rangle_S}\\ S\end{array}$$

where the sequence of formulae marked *cut* is obtained by cutting the sequent $\to \langle\varphi\rangle$ against each $\langle\varphi\rangle, \Gamma_i \to \Delta_i$ in $\langle\!\langle\varphi \supset \psi\rangle\!\rangle$.

The $\forall$ rules are rather simple. The rule $\forall$-l amounts to adding further premisses to an existing derivation, while $\forall$-r essentially follows from expanding out the definition of $\langle\!\langle\cdot\rangle\!\rangle$ on universally quantified formulae.

For the extension of a proof by an induction step, the definition of $\langle\!\langle\cdot\rangle\!\rangle$ is obtained by first converting the induction into finitely many instances of *cut* (the number determined by the value of the closed term in the succedent of the lower sequent), like in the definition of $\langle\cdot\rangle$, and then applying the definition of $\langle\!\langle\cdot\rangle\!\rangle$ for the case of *cut* steps. This may increase the length of the dependency graph by a logarithmic factor in the case of $\underline{I}_j\underline{U}_2^1$, and by a quasipolynomial factor in the case of $\underline{I}_j\underline{V}_2^{0.5}$.

It turns out that the image of $\underline{I}_j\underline{U}_2^1$ proofs can be made tree-like in quasipolynomial time. We omit a complexity analysis here, for brevity, but remark that the argument is not dissimilar to that for $\langle\cdot\rangle$ on MU_2^0 and its variations. Essentially, the length of the dependency graph of an $L_{j-1}J$ proof in the image of $\langle\!\langle\cdot\rangle\!\rangle^j$ is bounded by a polylogarithm in the size of the arguments in the conclusion, due to the use of only polynomial induction steps, and so 'unwinding' the proof to tree-like form takes quasipolynomial-time. The argument also bears semblance to that used in [25] for the theory U_1^1 (or equivalently U_2^1), where it is extension variables rather than dagness that needs to be unwound in a proof.

Theorem 45 (Complexity of $\langle\!\langle\cdot\rangle\!\rangle$). *If $\underline{I}_j\underline{V}_2^{0.5}$ proves an L_j sequent $\Sigma(\vec{x}) \to \varphi(\vec{x})$, there are $L_{j-1}J$ derivations $\begin{array}{c}\langle\!\langle\Sigma(\vec{n})\rangle\!\rangle\\ \big|\,{\scriptstyle\pi}\\ S\end{array}$ for each $S \in \langle\!\langle A(\vec{n})\rangle\!\rangle$ of size quasipolynomial in $\vec{n}$ and, if it is a $\underline{I}_j\underline{U}_2^1$ theorem, π has a dependency graph of length polylogarithmic in $\vec{n}$.*

Finally, by considering the special case when $j = 1$ and the aforementioned correspondence between tree-like MLK and MON, we arrive at one of our main results:

Corollary 46. *If $I_1U_2^1$ proves a $\Sigma_0^{B,+}$ sequent $\Gamma \to \Delta$ then there are quasipolynomial-size* MON *proofs $\begin{array}{c}\langle\Gamma\rangle_l\\ \|\\ \langle\Delta\rangle_r\end{array}$, or equivalently tree-like MLK proofs of $\langle\Gamma\rangle_l \to \langle\Delta\rangle_r$.*

5. Reflection principles

The *reflection* principle for a propositional proof system (PPS) is a formal statement of its soundness. Proofs in arithmetic theories of such principles serve as converses of propositional translations (e.g. Paris-Wilkie), since they guarantee that the theory is amongst the strongest for which such a translation could exist.

Due to the criteria of positivity and level we must be careful about how to formalise sequences and data structures. Therefore we take a mixed approach, using individual variables (on which negation may occur) to code formulae and proofs, as often done in subsystems of Buss' S_2^i and T_2^i, using set variables to code the truth of the formula, as is usually done for subsystems of U_2^i and V_2^i [25]. This is also the reason why we include the # symbol in all our theories, since it is required to carry out such a coding.[15]

We do not present the full formalisation here, but assume we have access to the following $\Sigma_0^{B,+}$-formulae free of set variables:

- $\mathrm{Fla}^+(x)$: "x codes a positive formula".
- $\mathrm{Der}_P(x, y, z)$: $\mathrm{Fla}^+(y) \wedge \mathrm{Fla}^+(z) \wedge$ "x codes a P-derivation from y to z".

We assume that their basic properties are provable in U_2^0 (and so $I_0U_2^0$ and MU_2^0) cf. [25].

We also need a formula,

$$\mathrm{Tr}^+(x) \ : \quad \mathrm{Fla}^+(x) \ \wedge \ \text{"the formula coded by } x \text{ is true"}$$

obtained by $\Sigma_0^{B,+}\text{-}CA_{|\omega|}$ and so containing set variables. In order to do this we need to use a monotone variation of *Spira's theorem*, stating that every formula can be polyomially transformed into an equivalent one that is *balanced*, i.e. has logarithmic depth.

The exposition follows that in [25], taking care to preserve monotonicity. For brevity, let us suppose we have such formulae, and that $\langle\mathrm{Tr}^+(x)\rangle$ is logically equivalent to the propositional formula coded by x, witnessed by short proofs in NOR.

Definition 47 (Positive reflection). For a PPS P, we define:

$$\mathrm{Rfn}_P^+ := \forall x, y, z.(\mathrm{Der}_P(x, y, z) \supset (\mathrm{Tr}^+(y) \supset \mathrm{Tr}^+(z))) \quad (7)$$

Recall that a (propositional) monotone implication is a propositional formula $\varphi \supset \psi$ where φ and ψ are free of $\supset$ symbols.

Proposition 48 (Quasipolynomial simulation). *For a PPS P:*

1. *If $\underline{MU}_2^1 \vdash \mathrm{Rfn}_P^+$ then* NOR *quasipolynomially simulates P over monotone implications.*
2. *If $\underline{MV}_2^{0.5} \vdash \mathrm{Rfn}_P^+$ or $I_1U_2^1 \vdash \mathrm{Rfn}_P^+$ then* MON *quasipolynomially simulates P over monotone implications.*

[15] We do not lose much, however, since quasipolynomials pop up from various locations in the propositional translations presented, not just #.

Proof. Let us consider 1, whence the case for 2 is analogous. Applying Thm. 25[16] we arrive at quasipolynomial-size families of propositional derivations:

$$\begin{array}{c}\langle \mathrm{Der}_P(l,m,n) \wedge \langle \mathrm{Tr}^+(m)\rangle\rangle \\ {\scriptstyle \pi(l,m,n)}\Big\| {\scriptstyle \textsc{Nor}} \\ \langle \mathrm{Tr}^+(n)\rangle\end{array}$$

for $l, m, n \in \mathbb{N}$. Consider a P-proof $\pi_{\varphi,\psi}$ of a monotone implication $\varphi \supset \psi$, and let us write $\ulcorner\alpha\urcorner$ for the code of some (finite) object. Notice that $\mathrm{Der}_P(\ulcorner\pi_{\varphi,\psi}\urcorner, \ulcorner\varphi\urcorner, \ulcorner\psi\urcorner)$ is true and contains no set symbols, so its image under $\langle\cdot\rangle$ is simply a Boolean combination of constant symbols, which can be evaluated even in Nor. Finally, recall that $\langle \mathrm{Tr}^+(\ulcorner\chi\urcorner)\rangle$ is provably equivalent to χ by short proofs in Nor, for any positive propositional formula χ, and so we can construct from $\pi(\ulcorner\pi_{\varphi,\psi}\urcorner, \ulcorner\varphi\urcorner, \ulcorner\psi\urcorner)$ quasipolynomial-size derivations of the format $\begin{array}{c}\varphi \\ \| {\scriptstyle \textsc{Nor}} \\ \psi\end{array}$ as required. □

Finally we give the following result which, in light of Prop. 48 above, provides a form of converse to Cor. 46.

Theorem 49. *$I_1U_2^1$ proves $\mathrm{Rfn}^+_{\textsc{Mon}}$.*

Proof sketch. We prove the following Σ_0^{B,L_1}-formula,

$$\forall x, y, z < w.(\mathrm{Der}_{\textsc{Mon}}(x, y, z) \supset (\mathrm{Tr}^+(y) \supset \mathrm{Tr}^+(z)))$$

by polynomial induction on w, whence the result follows by $BASIC$. In the inductive step we apply the inductive hypothesis to the first half and second half of a Mon rewriting derivation, thence applying cuts to derive the inductive step. In order to construct divide-and-conquer style arguments on Mon proofs, we may represent them as usual rewriting derivations that are simply lists of formulae (i.e. 'Calculus of Structures' style [6]).[17]

□

6. Further remarks

We briefly present some further points related to this work and discuss some ongoing research.

6.1 Variants of V_2^1

We have discussed mostly the monotone and intuitionistic versions of U_2^1 and the versions of V_2^1 with only Σ_0^{B,L_1}-$PIND$ rather than Σ_0^{B,L_1}-IND, our so-called '$V_2^{0.5}$' theories. We believe that all the expected results for $\underline{MV_2^1}$ and $I_1V_2^1$ go through, namely that both translate to dag-like MLK derivations with *extension* variables, cf. [24], and the latter is able to prove its soundness.

In a recent line of work by Straßburger et al., variants of KS (or Nor) with extension have been studied [29], so it would be interesting to see what blend of rules corresponds to those systems. The answer does not seem obvious since, as soon as we add Σ_0^{B,L_1}-IND we inherit $\Sigma_0^{B,+}$-IND, and so cannot distinguish normal proofs from monotone proofs.

6.2 Counting arguments and further reflection principles

It is known that tree-like MLK can quasipolynomially simulate LK over monotone sequents [1], and this (along with [1] [16] etc.) is one of the main sources of inspiration for this work.

The proof relies crucially on monotone formulae computing the *threshold function*, for which we constructed SO terms at the end of Sect. 3.2. In all these works, the crucial point is to find short proofs witnessing the *symmetry* of threshold functions. While Atserias et al. achieved this for tree-like MLK (or Mon), this is also achievable for Nor, albeit via a more complicated proof, and this was used in [16] to construct quasipolynomial-size proofs of the propositional pigeonhole principle in Nor.

To show the usefulness of our monotone theories, in ongoing work we show that $\underline{MU_2^1}$ proves the correctness of merge-sort, and so can prove the symmetry of threshold functions, subsuming the results of [16]. We would be interested in taking this further, finding new upper bounds and separations via these natural theories.

Can we reproduce Atserias et al.'s result using purely logical tools, instead of complex counting arguments? A corollary of their result is that the intuitionistic calculus LJ quasipolynomially simulates LK over monotone sequents. Can we perhaps reproduce this result or something in between, say for $I_jU_2^1$ for some large but finite j? A potentially fruitful idea is given in the next subsection; an answer to this question might have ramifications for more general questions in monotone proof complexity.

6.3 $(\forall, \supset)$-classical logic and Pierce's law

There are several difficulties with attempting to extend some of our results to the classical setting, but such results could provide a purely logical analogue to results in, say, [2], which rely on complex combinatorial arguments.

Over the $(\forall, \supset)$-fragment of the language we can recover classical reasoning by what is known as *Pierce's law*:

$$((\varphi \supset \psi) \supset \varphi) \supset \varphi \quad \text{or the rule} \quad \frac{\Sigma, \varphi \supset \psi \to \varphi}{\Sigma \to \varphi}$$

In fact, when dealing with only L_1-proofs, we can actually *realize* this law by (tree-like) MLK derivations,

$$\left\langle\!\!\left\langle \frac{\Sigma, \varphi \supset \psi \to \varphi}{\Sigma \to \varphi} \right\rangle\!\!\right\rangle : \quad \begin{array}{c} \langle\!\langle \Sigma \rangle\!\rangle \\ \langle\varphi\rangle, \Gamma_1 \to \Delta_1 \\ \big| {\scriptstyle \langle\!\langle \varphi \supset \psi \rangle\!\rangle} \\ \langle\varphi\rangle, \Gamma_n \to \Delta_n \\ \big| {\scriptstyle \langle\!\langle \pi \rangle\!\rangle_\varphi} \\ \to \langle\varphi\rangle \end{array} \quad \mapsto \quad \begin{array}{c} \langle\!\langle \Sigma \rangle\!\rangle \\ \langle\varphi\rangle \to \langle\varphi\rangle \\ \langle\varphi\rangle, \Gamma_1 \to \Delta_1, \langle\varphi\rangle \\ \big| {\scriptstyle w} \\ \langle\varphi\rangle, \Gamma_n \to \Delta_n, \langle\varphi\rangle \\ \big| {\scriptstyle \langle\!\langle \pi \rangle\!\rangle_\varphi, \langle\varphi\rangle} \\ \to \langle\varphi\rangle, \langle\varphi\rangle \\ \to \langle\varphi\rangle \end{array}$$

where $\langle\!\langle \pi \rangle\!\rangle_\varphi, \langle\varphi\rangle$ is obtained by appending $\langle\varphi\rangle$ to the succedent of every sequent in $\langle\!\langle \pi \rangle\!\rangle_\varphi$. Notice that, while this transformation is valid in MLK it is not, in general, valid for L_jJ due to the restriction on the $\supset$-r rule.

The problem with implementing this is the fact that we do not have much control on the logical complexity of ψ. Nonetheless, in ongoing work we are exploring fragments of classical U_2^1 for which a translation to MLK may still be attained.

6.4 Disjunction in the intuitionistic setting

We have not dealt with disjunction in the intuitionistic setting in favour of easing the translation. As one might expect, things become very cumbersome, with particular complications arising since our base type includes *all* monotone formulae. One might extend the class L_j by taking advantage of *Harrop* or *hereditarily Harrop* formulae, cf. [12], which allows us to preserve the disjunction property of intuitionistic logic in the presence of contexts. This approach bears semblance with the V^1-$HORN$ theory presented in [13] which limits induction to a generalisation of *Horn* clauses.

Another approach might be to use a variant of the deep inference medial rule [6] to manipulate disjunctions of implications:

$$(\varphi \supset \psi) \vee (\varphi' \supset \psi') \to (\varphi \wedge \varphi') \supset (\psi \vee \psi')$$

[16] In the case of 2 we should apply 27 or Cor. 46, as appropriate.

[17] This representation is at most quadratically larger than the deep inference representation of Sect. 2.3.

6.5 Towards a theory for NOR

We do not yet have a full correspondence for NOR, and this reflects the difficulty in deep inference proof complexity of conducting any metalogical reasoning at all in NOR, or KS. One approach might be to incorporate structural restrictions from *linear logic*, e.g. that induction formulae must be free of modalities, like in [3]. This could also allow us to complete the higher-types version of the PW-translation by allowing recursive application of $\langle\!\langle \cdot \rangle\!\rangle$, using linearity to control resource usage. While this might not be desirable from the point of view of reasoning, it might allow us to conduct one-off proofs of soundness of various systems, thereby settling certain proof complexity questions.

7. Conclusions

We gave uniform versions of monotone and analytic deep inference proof systems, in the setting of bounded arithmetic. This constituted an application of a characterisation of certain provable fixed points, deep inference proof normalisation and intuitionistic bounded arithmetic to propositional proof complexity. In the case of monotone proofs we were able to also prove a converse result.

This work further brings research in deep inference in line with the standards of mainstream proof complexity. By studying restrictions of monotone systems we also contribute to 'bridging the gap' between weak systems and Hilbert-Frege systems (for which no nontrivial lower bounds are known), providing finer granularity of the various subproblems.

References

[1] Albert Atserias, Nicola Galesi, and Ricard Gavaldà. Monotone proofs of the pigeon hole principle. *Electronic Colloquium on Computational Complexity (ECCC)*, 7(8), 2000.

[2] Albert Atserias, Nicola Galesi, and Pavel Pudlák. Monotone simulations of non-monotone proofs. *Journal of Computer and System Sciences*, 65(4):626–638, 2002.

[3] Stephen Bellantoni and Martin Hofmann. A new "feasible" arithmetic. *Journal of Symbolic Logic*, 67(1):104–116, 2002.

[4] Marta Bílková. Monotone sequent calculus and resolution. *Commentationes Mathematicae Universitatis Carolinae*, 42(3):575–582, 2001.

[5] Kai Brünnler. Deep inference and its normal form of derivations. In *Computability in Europe 2006*, volume 3988 of *Lecture Notes in Computer Science*, pages 65–74. Springer-Verlag, July 2006.

[6] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In *LPAR 2001*, volume 2250 of *Lecture Notes in Computer Science*, pages 347–361. Springer-Verlag, 2001.

[7] Paola Bruscoli and Alessio Guglielmi. On the proof complexity of deep inference. *ACM Transactions on Computational Logic*, 10(2):1–34, 2009.

[8] Paola Bruscoli, Alessio Guglielmi, Tom Gundersen, and Michel Parigot. A quasipolynomial cut-elimination procedure in deep inference via atomic flows and threshold formulae. In *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR '16)*, volume 6355 of *Lecture Notes in Computer Science*, pages 136–153. Springer-Verlag, 2010.

[9] Samuel R. Buss. *Bounded arithmetic*, volume 1 of *Studies in Proof Theory*. Bibliopolis, Naples, 1986.

[10] Samuel R. Buss. The polynomial hierarchy and intuitionistic bounded arithmetic. In *Structure in Complexity Theory, Proceedings of the Conference hold at the University of California, Berkeley, California, June 2-5, 1986*, pages 77–103, 1986.

[11] Samuel R. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53(1):75–102, 1991.

[12] Samuel R. Buss, editor. *Handbook of proof theory*. Elsevier, Amsterdam, 1998.

[13] Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge University Press, New York, NY, USA, 1st edition, 2010.

[14] Stephen Cook and Alasdair Urquhart. Functional interpretations of feasibly constructive arithmetic. In *Proceedings of the Twenty-First annual ACM Symposium on Theory of Computing*, STOC '89, pages 107–112. ACM, 1989.

[15] Anupam Das. Complexity of deep inference via atomic flows. In *Computability in Europe*, volume 7318 of *Lecture Notes in Computer Science*, pages 139–150. Springer-Verlag, 2012.

[16] Anupam Das. On the pigeonhole and related principles in deep inference and monotone systems. In *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, CSL-LICS '14, pages 36:1–36:10, New York, NY, USA, 2014. ACM.

[17] Anupam Das. On the relative proof complexity of deep inference via atomic flows. *Logical Methods in Computer Science*, 11(1):4:1–27, 2015.

[18] Michael Dummett. *Elements of intuitionism*. Oxford University Press, 2000.

[19] Alessio Guglielmi and Tom Gundersen. Normalisation control in deep inference via atomic flows. *Logical Methods in Computer Science*, 4(1:9):1–36, 2008.

[20] Alessio Guglielmi, Tom Gundersen, and Michel Parigot. A proof calculus which reduces syntactic bureaucracy. In Christopher Lynch, editor, *21st International Conference on Rewriting Techniques and Applications (RTA '10)*, volume 6 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 135–150. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2010.

[21] Victor Harnik. Provably total functions of intuitionistic bounded arithmetic. *Journal of Symbolic Logic*, 57(2):466–477, 1992.

[22] Emil Jeřábek. Proof complexity of the cut-free calculus of structures. *Journal of Logic and Computation*, 19(2):323–339, 2009.

[23] Emil Jeřábek. A sorting network in bounded arithmetic. *Annals of Pure and Applied Logic*, 162(4):341–355, 2011.

[24] Emil Jeřábek. Proofs with monotone cuts. *Mathematical Logic Quarterly*, 58(3):177–187, 2012.

[25] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*. Cambridge University Press, New York, NY, USA, 1995.

[26] Richard McKinley. Classical categories and deep inference. In *Structures and Deduction*, pages 19–33. Technische Universität Dresden, 2005. ICALP Workshop. ISSN 1430-211X.

[27] J.B. Paris and A.J. Wilkie. Δ_0 sets and induction. *Open Days in Model Theory and Set Theory, W. Guzicki, W. Marek, A. Pelc, and C. Rauszer, eds*, pages 237–248, 1981.

[28] Pavel Pudlák. On the complexity of the propositional calculus. *London Mathematical Society Lecture Note Series*, pages 197–218, 1999.

[29] Lutz Straßburger. Extension without cut. *Annals of Pure and Applied Logic*, 163(12):1995–2007, 2012.

[30] Gaisi Takeuti. *Proof Theory*, volume 81 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, 1975.