Characterising Definable Search Problems in Bounded Arithmetic via Proof Notations

Arnold Beckmann[*]
Department of Computer Science
Swansea University
Swansea SA2 8PP, UK
a.beckmann@swansea.ac.uk

Samuel R. Buss[†]
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112, USA
sbuss@math.ucsd.edu

October 25, 2009

Abstract

The complexity class of Π^{p}_k-Polynomial Local Search (PLS) problems with Π^{p}_ℓ-goal is introduced, and is used to give new characterisations of definable search problems in fragments of Bounded Arithmetic. The characterisations are established via notations for propositional proofs obtained by translating Bounded Arithmetic proofs using the Paris-Wilkie-translation. For $\ell \leq k$, the $\Sigma^{\mathrm{b}}_{\ell+1}$-definable search problems of T^{k+1}_2 are exactly characterised by Π^{p}_k-PLS problems with Π^{p}_ℓ-goals. These Π^{p}_k-PLS problems can be defined in a weak base theory such as S^1_2, and proved to be total in T^{k+1}_2. Furthermore, the Π^{p}_k-PLS definitions can be Skolemised with simple polynomial time functions. The Skolemised Π^{p}_k-PLS definitions give rise to a new $\forall\Sigma^{\mathrm{b}}_1(\alpha)$ principle conjectured to separate $\mathrm{T}^k_2(\alpha)$ from $\mathrm{T}^{k+1}_2(\alpha)$.

1 Introduction

Bounded Arithmetic in the form introduced by the second author [Bus86] denotes a collection of theories of arithmetic which have a strong connection to computational complexity. An important goal in Bounded Arithmetic is to give good descriptions of the functions that are definable in a certain theory by a certain class of formulas. For the sake of simplicity of this introduction, we will concentrate only on the Bounded Arithmetic theories S^i_2. These theories are given as first order theories of arithmetic in a language which suitably extends that of Peano Arithmetic, where induction is restricted in two ways. First, logarithmic induction is considered which only

[*]Supported in part by EPSRC grant EP/D03809X/1.
[†]Supported in part by NSF grant DMS-0700533.

inducts over a logarithmic part of the universe of discourse.

$$\varphi(0) \ \wedge\ (\forall x)(\varphi(x) \ \rightarrow\ \varphi(x+1)) \ \rightarrow\ (\forall x)\varphi(|x|) \ .$$

Here, $|x|$ denotes the length of the binary representation of the natural number x, which defines a kind of logarithm on natural numbers. As in these theories exponentiation will not be a total function, this is a proper restriction. Second, the properties which can be inducted on, must be described by a suitably restricted ("bounded") formula. The class of formulas used here are the Σ^{b}_i-formulas which exactly characterise Σ^{p}_i, that is, properties of the i-th level of the polynomial time hierarchy of predicates. The main axioms of the theory S^i_2 are the instances of logarithmic induction for Σ^{b}_i formulas.

Let a (multi-)function f be called Σ^{b}_j-definable in S^i_2, if its graph can be expressed by a Σ^{b}_j-formula φ, such that the totality of f, which renders as $(\forall x)(\exists y)\varphi(x, y)$, is provable from the S^i_2-axioms in first-order logic. The main results characterising definable (multi-)functions in Bounded Arithmetic are the following.

- Buss [Bus86] characterised the Σ^{b}_i-definable functions of S^i_2 as $\mathrm{FP}^{\Sigma^{\mathrm{p}}_{i-1}}$, the i-th level of the polynomial time hierarchy of functions.

- Krajíček [Kra93] characterised the $\Sigma^{\mathrm{b}}_{i+1}$-definable multi-functions of S^i_2 as the class $\mathrm{FP}^{\Sigma^{\mathrm{p}}_i}[wit, O(\log n)]$ of multi-functions which can be computed in polynomial time using a witness oracle from Σ^{p}_i, where the number of oracle queries is restricted to $O(\log n)$ many (n being the length of the input).

- Buss and Krajíček [BK94] characterised the Σ^{b}_1-definable multi-functions of S^2_2 as projections of solutions to polynomial local search problems. This result extends to higher levels as well: the $\Sigma^{\mathrm{b}}_{i-1}$-definable multi-functions of S^i_2 are exactly the projections of solutions to problems from $\mathrm{PLS}^{\Sigma^{\mathrm{p}}_{i-2}}$, which is the class of polynomial local search problems relativised to $\Sigma^{\mathrm{p}}_{i-2}$-oracles.

- Pollett [Pol99] showed that the $\Sigma^{\mathrm{b}}_{j+1}$-definable multi-functions in S^i_2 for $j > i$ are exactly $\mathrm{FP}^{\Sigma^{\mathrm{p}}_j}[wit, O(1)]$.

The characterisation of the Σ^{b}_i-definable functions of S^{k+1}_2 for $0 < i < k$ turned out to be more difficult, but recently some advances have been made. Krajíček, Skelley, and Thapen [KST07] characterised the Σ^{b}_1-definable functions of S^3_2 in terms of coloured PLS problems, and the Σ^{b}_1-definable functions of S^4_2 in terms of a kind of reflection principle, and also in terms of a kind of recursion called *verifiable recursion.* Subsequently, Skelley and Thapen [ST07] characterised the Σ^{b}_1-definable functions of S^{k+1}_2, for all

$k \geq 2$, in terms of a combinatorial principle for k-turn games. An earlier, more complex, game characterisation of the same functions was given by Pudlák [Pud06] using a combinatorial analysis of Herbrand disjunctions, which has been improved later by the same author [Pud07].

In this article we will provide characterisations for all pairs of bounded formula class $\Sigma^{\mathrm{b}}_{\ell+1}$ and theory S^{k+2}_2, for $\ell < k$, in terms of generalisations of PLS problems which we call Π^{b}_k-*PLS problems with* Π^{b}_ℓ-*goals*. We will define the new complexity classes in Section 3. An instance of a Π^{b}_k-PLS problems with Π^{b}_ℓ-goals will consist, on input a, of a polynomially bounded set of feasible solutions of complexity Π^{b}_k and a goal set of complexity Π^{b}_ℓ, an initial value function computing a feasible solution, a cost function computing the cost of a feasible solution, and a neighbourhood function computing from a given feasible solution another feasible solution (its neighbour), such that either the computed neighbour is identical to the original solution, or the neighbour is of lower cost — these functions have to be polynomial time computable. The goal set has to satisfy that it consists of exactly those feasible solutions for which the neighbourhood function is the identity. An important requirement will be that these conditions are provable in a weak theory like S^1_2, as without such requirements we can easily construct for any total function f given by $(\forall x)\varphi(x, f(x))$ with φ polynomial time computable and polynomially bounded (that is, for any (x, y) with $\varphi(x, y)$, $|y|$ is polynomial in $|x|$), a Π^{b}_1-PLS problem with goal φ — some of the requirements will then depend on the totality of the function and can thus only be proved in a theory which already proves the totality of the function.

The new characterisations have been obtained during a research visit of the first author at the second author's institution in autumn 2007. Prior to this visit, these new characterisations had been partially guessed based on recent results about obtaining the above-mentioned known characterisations of definable functions via notations for propositional proofs and cut-reduction [AB09]. Then, during the research visit, two different proofs for the new characterisations have been obtained, one extending the idea of notations for propositional proofs, and the other based on witnessing arguments.

Witnessing arguments form the dominant method for characterising definable (multi-)functions in Bounded Arithmetic. For example, the above-mentioned known characterisation of definable (multi-)functions in Bounded Arithmetic all have been proven by specially tailored witnessing arguments. The new characterisation based on witnessing arguments will be reported in a different place [BB08].

In this article, we present the new characterisations based on proof notations, that is, via notations for propositional proofs which are obtained by translating first order proofs and applying cut-reduction. We will compare this approach with the above-mentioned witnessing argument at the end of this introduction after we have given an idea of how the new characterisations based on proof notations work. First, we briefly describe the general idea of proof notations as presented in [AB09], which will also be one half of the idea for the new characterisations. Suppose $(\forall x)(\exists y)\varphi(x, y)$, describing the totality of some multi-function, is provable in some Bounded Arithmetic theory. Fix a particularly nice formal proof P of this. Given $a \in \mathbb{N}$ we want to describe a procedure which finds some b such that $\varphi(\underline{a}, \underline{b})$ is true ($\underline{a}$ is some canonical term in the language of Bounded Arithmetic with value a.) Invert the proof P of $(\forall x)(\exists y)\varphi(x, y)$ to a proof of $(\exists y)\varphi(x, y)$, where x is now a free variable of the proof, then substitute $\underline{a}$ for all occurrences of x. This yields a proof of $(\exists y)\varphi(\underline{a}, y)$. Now we want to translate this proof to propositional logic. The propositional translation used here is well-known in proof-theoretic investigations; the translation has been described by Tait [Tai68], and later was independently discovered by Paris and Wilkie [PW85]. In the Bounded Arithmetic world it is known as the *Paris-Wilkie translation.* As these translations in general produce exponential size formulas and proofs, we cannot directly work with the resulting objects, but have to use notations for them. Applying cut-reduction appropriately to notations of propositional proofs, we obtain a proof with all cut-formulas of (at most) the same logical complexity as φ. It should be noted that a notation $h(a)$ for this proof can be computed in time polynomial in $|a|$ (cf. [AB09].)

The general local search problem which finds a witness for $(\exists y)\varphi(\underline{a}, y)$ can now be characterised as follows. Its instance is given by a. The set of possible solutions are those notations of a suitable size which denote derivations of a suitable cut-rank (cut-rank is the maximal level of cut-formulas occurring in the derivation). Furthermore, they must satisfy that the formula which they derive is equivalent to $(\exists y)\varphi(\underline{a}, y) \ \vee \ \psi_1 \ \vee \ \cdots \ \vee \ \psi_l$, where all ψ_i are of low complexity and false. An initial solution is given by $h(a)$. A neighbour to a solution h is a solution which denotes an immediate subderivation of the derivation denoted by h, if this exists, and h otherwise. The cost of a notation is the height of the proof-tree represented by the notation. The search task is to find a notation in the set of solutions which is a fixed point of the neighbourhood function. Obviously, a solution to the search task must exist. In fact, any solution of minimal cost has this property. Now consider any solution to the search problem. It must have the property that none of the immediate subderivations is in the solution space. This can only happen if the last inference derives $(\exists y)\varphi(\underline{a}, y)$ from a true statement $\varphi(\underline{a}, \underline{b})$ for some $b \in \mathbb{N}$. Thus b is a witness to $(\exists y)\varphi(\underline{a}, y)$, and we can output b as a solution to our original witnessing problem.

This approach works fine if the difference between the complexity of induction and the level of definability we are interested in is not too big. For the known characterisations mentioned above, things can be arranged such that, depending on the complexity of logarithmic induction present in the Bounded Arithmetic theory we started with, and the level of definability, we obtain local search problems *defined by functions of some level of the polynomial time hierarchy,* and different bounds to the cost function [AB09]. For example, if we start with the Σ^{b}_i-definable functions of S^i_2, we obtain a local search problem defined by properties in $\mathrm{FP}^{\Sigma^{\mathrm{b}}_{i-1}}$, where the cost function is bounded by $|a|^{O(1)}$. Thus, by following the canonical path through the search problem which starts at the initial value and iterates the neighbourhood function until reaching a solution, we obtain a path of polynomial length, which describes a procedure in $\mathrm{FP}^{\Sigma^{\mathrm{b}}_{i-1}}$ to compute a witness.

For the new characterisations however, the complexity of induction is much bigger than the level of definability, Σ^{b}_j versus Σ^{b}_i with $j >> i$ say. The above-described strategy would deal with this difference by applying an appropriate number of cut-reductions $(j + 1 - i)$. But if $j + 1 - i$ is too big, too many cut-reductions would have to be applied, resulting in a search space which explodes: the search space would contain too many objects as well as objects of too big size (iterated exponentiation in input length.) In such a situation the solution will be to apply a maximal number of cut-reductions such that the search space does not explode, and then change the above-described local search problem so that a feasible solution still contains a notation for derivation as above, but now the complexity of ψ_j does not necessarily match that of φ but can be bigger. This is compensated by accompanying the notation with an auxiliary search problem for determining the truth of ψ_j. In other words, a feasible solution in the overall search problem contains a notation h and a position $\mathfrak{s}$ in an auxiliary search problem for a formula ψ which is related to h. A solution to the auxiliary search problem for ψ will determine the truth of ψ, and allow us to choose an appropriate immediate subderivation of h to continue the overall search problem. Overall, we end up with search problems where the set of feasible solutions has high computational complexity (due to the assertion that all ψ_j are false) but, e.g., the neighbourhood function is still of low computational complexity (due to the use of the auxiliary search problems.) For example, we obtain for the Σ^{b}_1-definable multi-functions of S^{k+2}_2 that the set of feasible solutions has complexity Π^{p}_k, but the neighbourhood function, cost function and initial value function are polynomial time computable — this defines an instance of the above-mentioned Π^{b}_k-PLS problems.

An important property of our characterisation is that the Π^{b}_k-PLS conditions that the functions and predicates have to satisfy, are provable in S^1_2. Furthermore, these conditions can be written in a prenex form which can be Skolemised with simple polynomial time computable functions, such that the resulting conditions are still provable in S^1_2. This has several consequences: First, we obtain a much stronger algorithmic description of the $\Sigma^{\mathrm{b}}_{\ell+1}$-definable functions, as Π^{b}_k-PLS problems with Π^{b}_ℓ-goals in Skolem form, in which all conditions are given as $\forall\Pi^{\mathrm{b}}_1$ conditions. Second, using the description in Skolem form we can define search principles classes based on some generic principle (involving second order symbols representing the functions and predicates that make up a Π^{b}_k-PLS problem with Π^{b}_ℓ-goal in Skolem form) which can be seen to characterise the $\forall\Sigma^{\mathrm{b}}_{\ell+1}$-consequences of T^{k+1}_2. This, third, leads to the conjecture that the generic principle separates relativised theories, i.e. $\mathrm{T}^{k+1}_2(\alpha)$ from $\mathrm{T}^k_2(\alpha)$.

It is worth mentioning at this point that there are connections between the approach described here and the approach considered in [ST07]. The main similarity is that [ST07] also makes use of a translation of T^{k+1}_2 proofs into exponential sized propositional proofs of some special purpose propositional proof systems which are described by polynomial time relations.

To come back to a comparison between the proof notation approach to the new characterisations presented here, and the witnessing arguments given in [BB08], the difference between them goes beyond obtaining the same results with two different methods. The layout of the witnessing argument is such that its inductive formulation has to incorporate the cut-reduction part of the proof notation argument. This in particular means that the witnessing argument directly deals with sequents of formulas as complex as induction formulas, where the notation argument directly deals with sequents of formulas of one level below that. So, on one hand the witnessing argument is direct but more involved, whereas for the notation argument it takes a while to set up the necessary machinery (mainly by repeating parts of [AB09]), but after that is pretty straightforward. Both approaches have in common that they use auxiliary search problems to determine the truth of formulas. The difference between the two approaches becomes even more visible when it comes to refinements of the results by Skolemising properties of the resulting search problems. While this is a technical but straightforward task for proof notations, it is more involved for the witnessing argument which needs to prove a stronger Skolemisation result due to its inductive layout and higher formula complexities.

The next section will briefly introduce Bounded Arithmetic in a way suitable for our proof-theoretic investigations. Section 3 defines the search problem classes of Π^{b}_k-polynomial local search, and their generalisations. Sections 4 and 5 review necessary definitions and results on notations and cut-reduction in general, and for Bounded Arithmetic in particular, from [AB09]. Section 6 then introduces the auxiliary search problems to determine the truth of formulas. This is followed by the section defining the search problems which come from proofs in Bounded Arithmetic, and stating our main result concerning the characterisation of definable multi-functions in terms of Π^{b}_k-PLS. The next two sections deal with a strengthening of our main results by showing that the conditions for Π^{b}_k-PLS problems extracted from Bounded Arithmetic proofs can be Skolemised with simple, polynomial time computable Skolem-functions. In the final section we will use the Skolemised Π^{b}_k-PLS problems to define $\forall\Sigma^{\mathrm{b}}_1(\alpha)$-sentences which we conjecture to separate relativised Bounded Arithmetic theories $\mathrm{S}_2^{k+1}(\alpha)$ from $\mathrm{S}_2^{k+2}(\alpha)$.

2 Bounded Arithmetic

We introduce Bounded Arithmetic very briefly, and in a slightly nonstandard way which better suits our proof-theoretic investigations. The reader interested in the general theory of Bounded Arithmetic is kindly referred to the literature [Bus86].

The standard model for Bounded Arithmetic is $\mathbb{N}$, the set of natural numbers. For $a \in \mathbb{N}$ let $|a|$ denote the length of the binary representation of a.

Definition 2.1 (Language of Bounded Arithmetic)**.** We define the *language* $\mathcal{L}_{\mathrm{BA}}$ *of Bounded Arithmetic* as in [Bus86] with a few additional symbols for polynomial time computable functions:

$$\mathcal{L}_{\mathrm{BA}} = \{\mathrm{S}, +, \times, |\cdot|, \#, =, \leq\} \cup \{c_a \colon a{\in}\mathbb{N}\} \cup \{2^{|\cdot|}, \dot{-}, \min, \mathrm{pair}, (\cdot)_1, (\cdot)_2\}$$

To explain the meaning of these symbols we briefly indicate their interpretation in the standard model $\mathbb{N}$: $\{=, \leq\}$ denote the binary relations "equality" and "less than or equal". c_a for $a{\in}\mathbb{N}$ denotes a constant with standard interpretation $c_a^{\mathbb{N}} = a$. We will often write $\underline{a}$ instead of c_a, and 0 for c_0. S, $|\cdot|$ and $2^{|\cdot|}$ are unary function symbols whose standard interpretations are given by the successor function, $|\cdot|^{\mathbb{N}} \colon a \mapsto |a|$, and $2^{|\cdot|^{\mathbb{N}}} \colon a \mapsto 2^{|a|}$. $+$, $\times$, $\dot{-}$, min and $\#$ are binary function symbols whose standard interpretation are addition, multiplication, $\dot{-}^{\mathbb{N}} \colon a, b \mapsto \max(a{-}b, 0)$, minimisation, and $\#^{\mathbb{N}} \colon a, b \mapsto 2^{|a|\cdot|b|}$. pair, $(\cdot)_1$, $(\cdot)_2$ define some feasible pairing function like the Cantor pairing function with corresponding projections.

Atomic formulas are of the form $s = t$ or $s \leq t$ where s and t are terms. *Literals* are expressions of the form A or $\neg A$ where A is an atomic formula. Formulas are built up from literals by means of $\wedge$, $\vee$, $(\forall x)$, $(\exists x)$. The *negation* $\neg C$ *for a formula* C is defined via de Morgan's laws. Negation extends to sets of formulas in the usual way by applying it to their members individually. $A \rightarrow B$ is an abbreviation of $\neg A \vee B$.

Let $\mathrm{FV}(A)$ denote the free variables occurring in formula A. With $A_x(t)$ we denote the result of replacing all free occurrences of the variable x in A by t. Similar definitions are used for substitution into terms.

Definition 2.2 ($\overline{\mathrm{BASIC}}$)**.** With a *valid disjunction of literals* we mean a disjunction A of literals such that A is true in $\mathbb{N}$ under any assignment. Let $\overline{\mathrm{BASIC}}$ denote a set of valid disjunctions of literals which is sufficient to define the non-logical symbols in $\mathcal{L}_{\mathrm{BA}}$. More precisely, we consider the set $\overline{\mathrm{BASIC}}$ to be the natural reformulation of the axioms BASIC from [Bus86] into a set of disjunctions of literals, extended by suitable axioms defining the new symbols. We assume that the following axioms are included:

$$\begin{array}{cc}
(\mathrm{pair}(a,b))_1 = a & (\mathrm{pair}(a,b))_2 = b \\
(c)_1 \le c & (c)_2 \le c \\
\multicolumn{2}{c}{a,b \le t \ \rightarrow\ \mathrm{pair}(a,b) \le B(t) \text{ for some } \mathcal{L}_{\mathrm{BA}}\text{-term } B} \\
\min(a,b) = a \ \vee\ \min(a,b) = b & \min(a,b) = \min(b,a) \\
a \le b \ \rightarrow\ \min(a,b) = a & \min(a,b) = a \ \rightarrow\ a \le b \\
a \dot- a = 0 & (\mathrm{S}\,a) \dot- (\mathrm{S}\,b) = a \dot- b \\
a \le b \ \rightarrow\ a \dot- b = 0 & a \dot- b = 0 \ \rightarrow\ a \le b
\end{array}$$

Definition 2.3 (Bounded Quantification)**.** Bounded quantifiers are introduced as follows: $(\forall x \le t)A$ denotes $(\forall x)A_x(\min(x,t))$, $(\exists x \le t)A$ denotes $(\exists x)A_x(\min(x,t))$, where x may not occur in t.

Our introduction of bounded quantifiers is a bit nonstandard. It has the advantage that already the usual cut-reduction procedure gives optimal results. The more standard abbreviation of bounded quantification, where e.g. $(\exists x \le t)A$ denotes $(\exists x)(x \le t \ \wedge\ A)$, would need a modification of cut-reduction to produce optimal bounds, as two logical connectives are to be removed for one bounded quantifier. Nevertheless, the two kind of abbreviations are equivalent over a weak base theory like Buss' BASIC (c.f. [Bus86]) assuming that this base theory includes some standard axiomatisation of min using $\le$ like $a \le b \ \rightarrow\ \min(x,y) = x$ and $\min(a,b) = \min(b,a)$. Also, either way makes use of a nonlogical symbol ("$\le$" versus "min").

Another approach to formalise bounded quantifiers is followed in [Bus86], where bounded quantifiers are treated as new logical symbols, not as abbreviations, and have their own, new kind of inference rules.

Definition 2.4 (Bounded Formulas)**.** The set Δ_0 of *bounded* $\mathcal{L}_{\mathrm{BA}}$*-formulas* is the set of $\mathcal{L}_{\mathrm{BA}}$-formulas consisting of literals and being closed under $\wedge$, $\vee$, $(\forall x \le t)$, $(\exists x \le t)$.

We now define a delineation of bounded formulas. The literature sometimes distinguishes between "strict" or "prenex" versions versus more liberal ones. We do not want to make such a distinction here to keep the focus on our proof-theoretic investigations, and define the classes only in their restricted form.

Definition 2.5. The set $\mathrm{s}\Sigma^{\mathrm{b}}_i$ is the smallest subset of bounded $\mathcal{L}_{\mathrm{BA}}$-formulas that is closed under taking subformulas and that contains all formulas of the form

$$(\exists x_1 \le t_1)(\forall x_2 \le t_2) \cdots (Q x_i \le t_i)(\overline{Q} x_{i+1} \le |t_{i+1}|)A(\vec{x}) \ ,$$

with Q and $\overline{Q}$ being of the corresponding alternating quantifier shape and A being quantifier free. A and the t_i's may involve variables not mentioned here.

Let $\mathrm{s}\Pi^{\mathrm{b}}_i$ be the set $\{\neg\varphi \colon \varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_i\}$, and let $\mathrm{s}\Sigma^{\mathrm{b}}_\infty$ be $\bigcup_{d<\infty} \mathrm{s}\Sigma^{\mathrm{b}}_d$.

Definition 2.6 (Rank)**.** The *rank of a formula* φ, $\mathrm{rk}(\varphi)$, is defined as the minimal k such that $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_k \cup \mathrm{s}\Pi^{\mathrm{b}}_k$, if such a k exists, and ∞ otherwise.

Definition 2.7. Let $\mathrm{Ind}(A, z, t)$ denote the expression

$$A_z(0) \ \wedge\ (\forall z \le t)(A \ \rightarrow\ A_z(z+1)) \ \rightarrow\ A_z(t) \ .$$

We will base our definition of Bounded Arithmetic theories on a different normal form of induction than usually considered in the literature.

Definition 2.8. Let T^i_2 denote the theory consisting of (universal closures of) formulas in $\overline{\mathrm{BASIC}}$ and of (universal closures of) formulas of the form $\mathrm{Ind}(A, z, 2^{|t|})$ with $A \in \mathrm{s}\Sigma^{\mathrm{b}}_i$, z a variable, and t an $\mathcal{L}_{\mathrm{BA}}$-term.

Let S^1_2 denote the theory consisting (of universal closures) of formulas in $\overline{\mathrm{BASIC}}$ and (of universal closures) of formulas of the form $\mathrm{Ind}(A, z, |t|)$ with $A \in \mathrm{s}\Sigma^{\mathrm{b}}_1$, z a variable and t an $\mathcal{L}_{\mathrm{BA}}$-term.

Our versions of T^i_2 and S^1_2 are different from the standard versions as for example defined in [Bus86]. They are adapted to suit the proof-theoretic investigations we want to pursue. Nevertheless, they are equivalent in that the sets of consequences are the same. This follows from the fact that the restricted form of induction as defined in Definition 2.7 implies the usual form, because the following can be proven from $\overline{\mathrm{BASIC}}$ alone:

$$\mathrm{Ind}(A(\min(t,z)), z, 2^{|t|}) \ \rightarrow\ \mathrm{Ind}(A(z), z, t) \ .$$

Definition 2.9. Let Σ^{b}_i (Π^{b}_i) be the set of formulas φ such that there exist $\psi \in \mathrm{s}\Sigma^{\mathrm{b}}_i$ (resp. $\psi \in \mathrm{s}\Pi^{\mathrm{b}}_i$) with $\mathrm{S}^1_2 \vdash \varphi \ \leftrightarrow\ \psi$.

Let Δ^{b}_1 be the set of formulas φ such that there exist formulas $\sigma \in \mathrm{s}\Sigma^{\mathrm{b}}_1$ and $\pi \in \mathrm{s}\Pi^{\mathrm{b}}_1$ with $\mathrm{S}^1_2 \vdash (\varphi \ \leftrightarrow\ \sigma) \ \wedge\ (\varphi \ \leftrightarrow\ \pi)$.

3 Π^{p}_k-Polynomial Local Search

A binary relation $R \subseteq \mathbb{N} \times \mathbb{N}$ is called *polynomially bounded* iff there is a polynomial p such that $(x, y) \in R$ implies $|y| \le p(|x|)$. R is called *total* if for all x there exists a y with $(x, y) \in R$.

Definition 3.1 (Total and Definable Search Problems)**.** Let $R \subseteq \mathbb{N} \times \mathbb{N}$ be a polynomially bounded, total relation. The *(total) search problem* associated with R is this: Given input $x \in \mathbb{N}$, return a $y \in \mathbb{N}$ such that $(x, y) \in R$. R is called $\Sigma^{\mathrm{b}}_{\ell+1}$*-definable in* T^{k+1}_2 if there exists a Π^{b}_ℓ-formula $\varphi(x, y)$ (Δ^{b}_1 if $\ell = 0$) and an $\mathcal{L}_{\mathrm{BA}}$-term $t(x)$, both with all free variables shown, such that $(x, y) \in R$ iff $\mathbb{N} \vDash \varphi(x, y)$, and such that $\mathrm{T}^{k+1}_2 \vdash (\forall x)(\exists y \le t(x))\varphi(x, y)$.

Definition 3.2 (Π^{p}_k-PLS Problems with Π^{p}_ℓ-Goal)**.** A Π^{p}_k-*Polynomial Local Search (PLS) problem with* Π^{p}_ℓ*-goal*, for $k \geq \ell \geq 0$, is a tuple $L = (F, G, N, c, i)$ consisting of, for a given input x, a set $F(x)$ of *feasible solutions* with a polynomial bound d, a *goal set* $G(x)$, a *neighbourhood function* $N(x, s)$ mapping a configuration s to another configuration, a function $c(x, s)$ computing the *cost of a configuration* s, and a function $i(x)$ computing an *initial feasible solution*, such that the following properties are satisfied: the functions N, c and i are polynomial time computable, $F \in \Pi^{\mathrm{p}}_k$ and $G \in \Pi^{\mathrm{p}}_\ell$, and the following five conditions are satisfied:

$$(\forall x, s)(s \in F(x) \;\rightarrow\; |s| \leq d(|x|)) \tag{3.1}$$

$$(\forall x)(i(x) \in F(x)) \tag{3.2}$$

$$(\forall x, s)(s \in F(x) \;\rightarrow\; N(x, s) \in F(x)) \tag{3.3}$$

$$(\forall x, s)(N(x, s) = s \;\vee\; c(x, N(x, s)) < c(x, s)) \tag{3.4}$$

$$(\forall x, s)(s \in G(x) \;\leftrightarrow\; (N(x, s) = s \;\wedge\; s \in F(x))) \tag{3.5}$$

The search task is, for a given input x, to find some s with $s \in G(x)$.

Usually, the polynomial bound to F, d, is thought to be understood from the context and not explicitely mentioned. If we want to make it explicit we sometimes write $L = (d, F, G, N, c, i)$. We have introduced F and G as sets. When we focus on their complexity or their definability in Bounded Arithmetic, we treat "$s \in F(a)$" etc. as relations in s, a.

Without any further requirements, Π^{p}_k-PLS problems with Π^{p}_ℓ-goals do not say much about the complexity of the underlying search task. For example, let R be a polynomial time computable, total relation with polynomial bound p, defining a total search problem. Then we can define a Π^{p}_1-PLS problem with goal R as follows: Let $T(x)$ be $2^{p(|x|)}$. A feasible solution $s{\in}F(x)$ is given if $s{<}T(x) \;\wedge\; R(x, s)$, or, in case $s{=}T(x){+}s'$, if $|s'|{\leq}p(|x|) \;\wedge\; (\forall y{<}s')(x, y){\notin}R$; the initial value is $T(x)$; the neighbourhood function takes an s and outputs s if $s < T(x)$, or, in case $s{=}T(x){+}s'$, produces $T(x){+}s'{+}1$ if $|s'{+}1|{\leq}p(|x|) \;\wedge\; (x, s'){\notin}R$, and s' otherwise; and the cost of an s is computed as $2T(x){\dot-}s$ for $s \geq T(x)$, and 0 otherwise. The problem with this definition is that its condition (3.3) cannot be proven only if one can already prove that R defines a *total* search problem.

To formulate a Π^{p}_k-PLS local search principle so as to guarantee the totality of a search problem without actually presupposing it, we have to ensure that the conditions (3.1)–(3.5) have "simple" proofs. We make this precise in the next definition by requiring that they are provable in S^1_2.

Definition 3.3 (Formalised Π^{p}_k-PLS Problems with Π^{p}_ℓ-Goals)**.** A Π^{p}_k-PLS problem with Π^{p}_ℓ-goal is *formalised in* S^1_2 provided the functions N, c, and i are Σ^{b}_1-definable in S^1_2, the predicate F is given by a Π^{b}_k-formula, the predicate G is given by a Π^{b}_ℓ-formula (Δ^{b}_1 if $\ell = 0$), and the defining conditions (3.1)–(3.5) are provable in S^1_2.

A Π^{p}_k-PLS problem with Π^{p}_ℓ-goal which is formalised in S^1_2 will be called a Π^{b}_k*-PLS problem with* Π^{b}_ℓ*-goal* (with superscript "b" instead of "p".)

The direction "←" in condition (3.5) of a Π^{b}_k-PLS problem with Π^{b}_ℓ-goal is inessential, dropping it would result in an equivalent class of search problems. To make this more precise, let us denote with Π^{b}_k*-PLS' problems with* Π^{b}_ℓ*-goals* the class of search problems which are defined similar to Π^{b}_k-PLS problems with Π^{b}_ℓ-goals, with the only difference that in (3.5) equivalence "↔" is replaced by implication "→". To see that Π^{b}_k-PLS' problems with Π^{b}_ℓ-goals are equivalent to Π^{b}_k-PLS problems with Π^{b}_ℓ-goals, first observe that any Π^{b}_k-PLS problem with Π^{b}_ℓ-goal is also a Π^{b}_k-PLS' problem with Π^{b}_ℓ-goal. Secondly, we can transform any Π^{b}_k-PLS' problem with Π^{b}_ℓ-goal $L' = (d', F', G', N', c', i')$ into a Π^{b}_k-PLS problem with Π^{b}_ℓ-goal $L = (d, F, G, N, c, i)$ which solves L', in the following way: Let $T(x)$ be $2^{d'(|x|)}$. We set d to $2d'$, and $i(x)$ as $T(x){+}i'(x)$. Let $s{\in}F(x)$ if either $s{<}T(x) \wedge s{\in}G(x)$, or, in case $s{=}T(x){+}s'$, if $s'{\in}F'(x)$. Set $N(x, s)$ to be s if $s{<}T(x)$, or, in case $s{=}T(x){+}s'$, to be $T(x){+}N'(x, s')$ if $N'(x, s'){\neq}s'$, and s' otherwise. Finally, define $c(x, s)$ to be 0 if $s{<}T(x)$, and $1{+}c'(x, s')$ in case $s{=}T(x){+}s'$.

Theorem 3.4. *Let $k \geq \ell \geq 0$. The* Π^{b}_k*-PLS problems with* Π^{b}_ℓ*-goals are* $\Sigma^{\mathrm{b}}_{\ell+1}$*-definable search problems in* T^{k+1}_2.

Proof. Let $L = (F, G, N, c, i)$ be a Π^{b}_k-PLS problem with Π^{b}_ℓ-goal. Let x be given. The set $A := \{c(x, s) \colon s \in F(x)\}$ is non-empty by (3.2), and can be expressed by a $\Sigma^{\mathrm{b}}_{k+1}$ formula. T^{k+1}_2 proves minimisation for $\Sigma^{\mathrm{b}}_{k+1}$-formulas, thus, arguing in T^{k+1}_2, we can choose some minimal $c \in A$. Pick $s \in F(x)$ with $c(x, s) = c$, and let $s' := N(x, s)$. Then $s' \in F(x)$ by (3.3). By construction $c(x, s') \geq c(x, s)$, hence (3.4) shows $s' = N(x, s) = s$. Hence, (3.5) shows $s \in G(x)$.

That $\{(x, s) \colon s \in G(x)\}$ can be described by some Π^{b}_ℓ formula is clear by definition. □

The converse of the last theorem is also true and forms one of our main results in this article. It will be proven in Section 7.2.

Theorem 3.5. *Let $0 \leq \ell \leq k$. The* $\Sigma^{\mathrm{b}}_{\ell+1}$*-definable total search problems in* T^{k+1}_2 *can be characterised by* Π^{b}_k*-PLS problems with* Π^{b}_ℓ*-goals. This characterisation satisfies in addition that the goal formula is syntactically identical to the* Π^{b}_ℓ*-subformula of the original* $\Sigma^{\mathrm{b}}_{\ell+1}$*-formula.*

3.1 Search Problem Classes

Definition 3.2 gives rise to search principles expressed by one formula $\mathrm{PiPLS}(d, F, G, N, c, i)$ in second order parameters d, F, G, N, c, i, which is defined as

$$(3.1) \ \wedge \ (3.2) \ \wedge \ (3.3) \ \wedge \ (3.4) \ \wedge \ (3.5) \ \rightarrow \ (\forall x)(\exists y)G(x,y) \ .$$

By choosing appropriate substitutions for the parameters, this generic formula can be used to define syntactic search problem classes which characterise the $\forall\Sigma^{\mathrm{b}}_{\ell+1}$-consequences of T^{k+1}_2: Let $\mathrm{PiPLS}(k,\ell)$ be the set of all formulas obtained by replacing in $\mathrm{PiPLS}(d,F,G,N,c,i)$, d by some polynomial, N,c,i by polynomial time computable functions (represented by their Σ^{b}_1-definition in S^1_2), F by some formula in Π^{b}_k, and G by some formula in Π^{b}_ℓ. The proof of Theorem 3.4 shows that each formula in $\mathrm{PiPLS}(k,l)$ is provable in T^{k+1}_2. A converse is also true and can be shown using Theorem 3.5.

Corollary 3.6. *Over* S^1_2*, the theories* $\mathrm{PiPLS}(k,l)$ *and* T^{k+1}_2 *have the same* $\forall\Sigma^{\mathrm{b}}_{\ell+1}$*-consequences.*

Proof. We already argued for one inclusion. We still have to show that if T^{k+1}_2 proves $(\forall x)\varphi(x)$ with $\varphi \in \Sigma^{\mathrm{b}}_{\ell+1}$, then this formula also follows from a formula in $\mathrm{PiPLS}(k,l)$ over S^1_2.

Applying Theorem 3.5 we obtain a formalised Π^{p}_k-PLS problem with goal formula identical to φ. Consider the formula $\mathrm{PiPLS}(d,F,G,N,c,i)$ in $\mathrm{PiPLS}(k,l)$ coming from this characterisation. The conditions (3.1)–(3.5) are now provable in S^1_2, so over S^1_2 we immediately obtain $(\forall x)\varphi(x)$ from $\mathrm{PiPLS}(d,F,G,N,c,i)$. □

In Sections 8 and 9, we will see that a strengthening of Theorem 3.5 can also be proven, in which the conditions (3.1)–(3.5) will be transformed into some canonical Skolem form, see Corollary 9.8. This will reduce the complexity of the search principle class to match the complexity of the goal formulas. In particular we will obtain a set of $\forall\Sigma^{\mathrm{b}}_1$ formulas characterising the $\forall\Sigma^{\mathrm{b}}_1$-consequences of the theories T^{k+1}_2, for $k \geq 0$, see Corollary 10.2.

4 Notation Systems for Formulas and Proofs

In this section we review notation systems for propositional formulas and proofs, and cut-reduction for them from [AB09]. They provide the basic machinery for dealing with search problems based on proof notations.

4.1 Proof Systems

We begin with an abstract definition of proof systems, which will be at the heart of several derivation systems considered later.

Definition 4.1 (Notation System for Formulas)**.** A *notation system for formulas* is a triple $\langle \mathcal{F}, \approx, \mathrm{rk}\rangle$ where $\mathcal{F}$ is a set (of *formulas*), $\approx$ an equivalence relation on $\mathcal{F}$ (*identity between formulas*), and $\mathrm{rk}\colon \mathfrak{P}(\mathcal{F}) \times \mathcal{F} \rightarrow \mathbb{N}$ a function (*rank*). Here, $\mathfrak{P}(\mathcal{F})$ denotes the power set of $\mathcal{F}$.

We always write $\mathcal{C}$-rk(A) instead of rk$(\mathcal{C}, A)$. With $\approx\Gamma$ we denote the set $\{G\colon (\exists F \in \Gamma)(G \approx F)\}$.

Definition 4.2. A *proof system* $\mathfrak{S}$ *over* $\langle \mathcal{F}, \approx, \mathrm{rk}\rangle$ is given by a set of formal expressions called *inference symbols* (syntactic variable $\mathcal{I}$), and for each inference symbol $\mathcal{I}$ an ordinal $|\mathcal{I}| \leq \omega$, a sequent $\Delta(\mathcal{I})$ and a family of sequents $(\Delta_\iota(\mathcal{I}))_{\iota<|\mathcal{I}|}$.

Proof systems may have inference symbols of the form Cut_C for $C \in \mathcal{F}$; these are called "cut inference symbols" and their use will (in Definition 4.4) be measured by the $\mathcal{C}$-cut-rank.

Notation 4.3. By writing $(\mathcal{I})\ \dfrac{\ldots\Delta_\iota\ldots(\iota < I)}{\Delta}$ we declare $\mathcal{I}$ as an inference symbol with $|\mathcal{I}| = I$ many hypotheses, with conclusion $\Delta(\mathcal{I}) = \Delta$, and ι-th hypothesis $\Delta_\iota(\mathcal{I}) = \Delta_\iota$ for $\iota < I$. If $|\mathcal{I}| = n$ we write $\dfrac{\Delta_0\ \Delta_1\ \ldots\ \Delta_{n-1}}{\Delta}$ instead of $\dfrac{\ldots\Delta_\iota\ldots(\iota < I)}{\Delta}$.

$\mathfrak{S}$-quasi derivations, to be defined next, are (infinite) terms built up from inference symbols. An $\mathfrak{S}$-quasi derivation will always have the form of an inference symbol $\mathcal{I}$, followed by "(", followed by a sequence of length $|\mathcal{I}|$ of $\mathfrak{S}$-quasi derivations, followed by ")". For example, the simplest $\mathfrak{S}$-quasi derivations are given as $\mathcal{I}()$ in case $\mathcal{I}$ is an inference symbol with $|\mathcal{I}| = 0$. We will write a sequence of the form $(d_0, \ldots, d_{n-1})$ as $(d_\iota)_{\iota<n}$.

Definition 4.4 (Inductive definition of $\mathfrak{S}$-quasi derivations)**.** If $\mathcal{I}$ is an inference symbol of $\mathfrak{S}$, and $(d_\iota)_{\iota<|\mathcal{I}|}$ is a sequence of $\mathfrak{S}$-quasi derivations, then $d := \mathcal{I}(d_\iota)_{\iota<|\mathcal{I}|}$ is an $\mathfrak{S}$-*quasi derivation* with *end-sequent*

$$\Gamma(d) := \Delta(\mathcal{I}) \cup \bigcup_{\iota<|\mathcal{I}|} (\Gamma(d_\iota) \setminus \approx\Delta_\iota(\mathcal{I}))\ ,$$

last inference last$(d) := \mathcal{I}$, *subderivations* $d(\iota) := d_\iota$ for $\iota < |\mathcal{I}|$, *height*

$$\mathrm{hgt}(d) := \sup\{\mathrm{hgt}(d_\iota) + 1\colon \iota < |\mathcal{I}|\}\ ,$$

size (provided $\mathfrak{S}$ has inference symbols of finite arity only)

$$\mathrm{sz}(d) := (\sum_{\iota<|\mathcal{I}|} \mathrm{sz}(d_\iota)) + 1\ ,$$

and *cut-rank*

$$\mathcal{C}\text{-crk}(d) := \sup(\{\mathcal{C}\text{-rk}(\mathcal{I})\} \cup \{\mathcal{C}\text{-crk}(d_\iota)\colon \iota < |\mathcal{I}|\})\ .$$

Here we define $\mathcal{C}$-rk$(\mathcal{I})$, the *cut-rank of* $\mathcal{I}$, to be $\mathcal{C}$-rk$(C) + 1$ if $\mathcal{I}$ is of the form $\mathcal{I} = \mathrm{Cut}_C$ with $C \notin \mathcal{C}$, and to be 0 otherwise.

Definition 4.5. $d \vdash_{\approx} \Gamma$ is defined as $\Gamma(d) \subseteq {\approx}\Gamma$.

A translation of first order proofs into propositional ones, like the Paris-Wilkie translation, usually comes in two steps: First, first order formulas are translated into propositional ones; Second, first order proofs are translated into propositional proofs. In the next subsection, we introduce notation systems for propositional formulas of the type obtained by the Paris-Wilkie translation of first order formulas. The subsequent section defines our propositional proof system. Then, Subsection 4.4 describes polynomial-size notations for exponential-size propositional proofs that are obtained by the translation of first order proofs.

4.2 Notations for Propositional Formulas

Translating first order formulas into propositional ones via the Paris-Wilkie translation ${}^{\mathrm{PW}}$ transforms a bounded quantifier of the form $(\forall x \leq t(a))\varphi(x)$ into the propositional formula $\bigwedge_{i \leq t(a)^{\mathbb{N}}} \varphi(i)^{\mathrm{PW}}$. The length of this propositional formula is exponential in $|a|$, thus we need notation systems for such propositional formulas which allow us to deal with them in a feasible way. The next definition collects all necessary ingredients and properties of notation systems for propositional formulas.

Definition 4.6. We define $\neg$ as a function on the symbols $\{\top, \bot, \bigwedge, \bigvee\}$ in the following way: $\neg(\top) = \bot$, $\neg(\bot) = \top$, $\neg(\bigwedge) = \bigvee$, and $\neg(\bigvee) = \bigwedge$.

Definition 4.7. A *notation system* $\langle \mathcal{F}, \mathrm{tp}, \cdot[\cdot], \neg, \mathrm{rk}, \approx \rangle$ *for (infinitary) propositional formulas* is a notation system $\langle \mathcal{F}, \approx, \mathrm{rk} \rangle$ for formulas together with functions $\mathrm{tp}\colon \mathcal{F} \to \{\top, \bot, \bigwedge, \bigvee\}$, $\cdot[\cdot]\colon \mathcal{F} \times \mathbb{N} \to \mathcal{F}$, and $\neg\colon \mathcal{F} \to \mathcal{F}$, called *outermost connective*, *subformula*, and *negation*, respectively, such that $\mathrm{tp}(\neg(f)) = \neg(\mathrm{tp}(f))$, $\neg(f)[n] = \neg(f[n])$, $\mathcal{C}\text{-rk}(f) = \mathcal{C}\text{-rk}(\neg f)$, $\mathcal{C}\text{-rk}(f[n]) < \mathcal{C}\text{-rk}(f)$ for $f \notin \mathcal{C}$ and $n < |\mathrm{tp}(f)|$, and $f \approx g$ implies $\mathrm{tp}(f) = \mathrm{tp}(g)$, $f[n] \approx g[n]$, $\neg(f) \approx \neg(g)$ and $\mathcal{C}\text{-rk}(f) = \mathcal{C}\text{-rk}(g)$.

In the previous definition, the obvious idea behind $f[n]$ for $f \in \mathcal{F}$ and $n \in \mathbb{N}$ is that it denotes the n-th subformula of f. But observe that the situation we are describing is a bit more general. It does not exclude non-wellfounded notation systems, which may contain a notation f for which $0 < |\mathrm{tp}(f)|$ continues to hold for $f[0]$, $f[0][0]$, etc. ad infinitum. The cut-elimination results summarised in the following are still valid also in such a situation.

4.3 Propositional Proofs

The propositional proof system we are concerned with is directly based on notation systems for propositional formulas. There is of course a propositional proof system for (usual) propositional formulas in the background which is obtained by unfolding notations for propositional formulas into (usual) propositional formulas. This background proof system is not necessary for our technical developments, therefore we omit it. The interested reader will find a more detailed discussion in [AB09].

Definition 4.8. Let $\mathcal{F} = \langle \mathcal{F}, \mathrm{tp}, \cdot[\cdot], \neg, \mathrm{rk}, \approx \rangle$ be a notation system for propositional formulas. The *(propositional) proof system* $\mathfrak{S}_{\mathcal{F}}$ *over* $\mathcal{F}$ is the proof system over $\mathcal{F}$ which is given by the following set of inference symbols.

(Ax_A) $\quad \dfrac{}{A}$ for $A \in \mathcal{F}$ with $\mathrm{tp}(A) = \top$

$(\bigwedge_C)$ $\quad \dfrac{\dots \quad C[n] \quad \dots \quad (n \in \mathbb{N})}{C}$ for $C \in \mathcal{F}$ with $\mathrm{tp}(C) = \bigwedge$

$(\bigvee_C^i)$ $\quad \dfrac{C[i]}{C}$ for $C \in \mathcal{F}$ with $\mathrm{tp}(C) = \bigvee$ and $i \in \mathbb{N}$

(Cut_C) $\quad \dfrac{C \qquad \neg C}{\emptyset}$ for $C \in \mathcal{F}$ with $\mathrm{tp}(C) \in \{\top, \bigwedge\}$

(Rep) $\quad \dfrac{\emptyset}{\emptyset}$

Abbreviations
For $\mathrm{tp}(C) \in \{\bot, \bigvee\}$ let (Cut_C) $\dfrac{C \qquad \neg C}{\emptyset}$ denote $(\mathrm{Cut}_{\neg C})$ $\dfrac{\neg C \qquad C}{\emptyset}$

4.4 Notations for Propositional Proofs and Cut-Elimination

The translation of first order proofs in Bounded Arithmetic into the propositional proof system defined in Definition 4.8 may generate proofs of exponential size. E.g., an application of $(\forall)$ $\dfrac{\varphi(\min(x, t(a)))}{(\forall x \leq t(a))\varphi(x)}$ is translated into $(\bigwedge)$ $\dfrac{\varphi(0)^{\mathrm{PW}} \quad \dots \quad \varphi(t(a)^{\mathbb{N}})^{\mathrm{PW}}}{(\forall x \leq t(a))\varphi(x)^{\mathrm{PW}}}$ which may have exponentially in $|a|$ many premises. Thus, besides notations for propositional formulas, we also need notations for propositional proofs obtained by translation in order to be able to deal with them in a feasible way. The necessary ingredients for this are collected in the next definition.

Definition 4.9. Let $\mathcal{F}$ be a notation system for formulas, and $\mathfrak{S}_{\mathcal{F}}$ the propositional proof system over $\mathcal{F}$ from Definition 4.8.

A *notation system* $\mathcal{H} = \langle \mathcal{H}, \mathrm{tp}, \cdot[\cdot], \Gamma, \mathrm{crk}, \mathrm{o}, |\cdot| \rangle$ *for* $\mathfrak{S}_{\mathcal{F}}$ is a set $\mathcal{H}$ of *notations* and functions $\mathrm{tp}\colon \mathcal{H} \to \mathfrak{S}_{\mathcal{F}}$, $\cdot[\cdot]\colon \mathcal{H} \times \mathbb{N} \to \mathcal{H}$, $\Gamma\colon \mathcal{H} \to \mathfrak{P}_{\mathrm{fin}}(\mathcal{F})$, $\mathrm{crk}\colon \mathfrak{P}(\mathcal{F}) \times \mathcal{H} \to \mathbb{N}$, and $\mathrm{o}, |\cdot|\colon \mathcal{H} \to \mathbb{N} \setminus \{0\}$ called *denoted last inference*, *denoted subderivation*, *denoted end-sequent*, *denoted cut-rank*, *denoted height* and *size*, such that $\mathcal{C}$-$\mathrm{crk}(h[n]) \leq \mathcal{C}$-$\mathrm{crk}(h)$, $\mathrm{tp}(h) = \mathrm{Cut}_C$ implies $\mathcal{C}$-$\mathrm{rk}(C) < \mathcal{C}$-$\mathrm{crk}(h)$ for $C \notin \mathcal{C}$, $\mathrm{o}(h[n]) < \mathrm{o}(h)$ for $n < |\,\mathrm{tp}(h)|$, and the following local faithfulness property holds for $h \in \mathcal{H}$:

$$\Delta(\mathrm{tp}(h)) \subseteq {\approx}\Gamma(h) \quad \text{and} \quad \forall \iota < |\,\mathrm{tp}(h)|\ h[\iota] \vdash_{\approx} \Gamma(h), \Delta_\iota(\mathrm{tp}(h)) \ .$$

We observe that the size function in the last definition is not denoted. The idea is that it measures the size of the notation, not of the denoted proof. The size function will be important later when we try to measure the effect which cut-elimination has on notations, to identify those cases where the effect is feasible, i.e. does not lead to an exponential blow-up typical for cut-elimination on (regular) proofs.

The next definition gives the canonical propositional translation of proof notations into propositional proofs. The observation following this definition states the connection between key structural functions for notations and for connected propositional derivations.

Definition 4.10. Let $\mathcal{H} = \langle \mathcal{H}, \mathrm{tp}, \cdot[\cdot], \Gamma, \mathrm{crk}, \mathrm{o}, |\cdot| \rangle$ be a notation system for $\mathfrak{S}_{\mathcal{F}}$. The *interpretation* $[\![h]\!]$ *of* $h \in \mathcal{H}$ is inductively defined as the following $\mathfrak{S}_{\mathcal{F}}$-derivation:

$$[\![h]\!] := \mathrm{tp}(h)([\![h[\iota]]\!])_{\iota < |\,\mathrm{tp}(h)|}$$

Observation 4.11. *We make use of the functions defined in Definition 4.4. For $h \in \mathcal{H}$ we have*

$$\begin{aligned} \mathrm{last}([\![h]\!]) &= \mathrm{tp}(h) \\ [\![h]\!](\iota) &= [\![h[\iota]]\!] \qquad \textit{for } \iota < |\,\mathrm{tp}(h)| \\ \Gamma([\![h]\!]) &\subseteq {\approx}\Gamma(h) \end{aligned}$$

We explained in the introduction of this paper that our characterisation of definable search problems in Bounded Arithmetic will be based on translating Bounded Arithmetic proofs into propositional ones, and applying cut-reduction to the resulting propositional proofs. Thus, we also have to add to our notation system for propositional logic some notations for cut-reduction on propositional proofs. This can be done very uniformly, as presented in the next definition. Our approach following [AB09] is based on Mints' continuous cut-elimination procedure [Min78] in its technical smooth presentation by Buchholz [Buc91, Buc97] and utilises notations for certain operators of propositional proofs. Readers interested in a fuller account of this situation are kindly referred to [AB09]. The intuition behind the notations for operators for cut-reduction are as follows:

- The symbol I^k_C denotes an *inversion operator* which satisfies: If $h \vdash_{\approx} \Gamma, C$ and $\mathrm{tp}(C) = \bigwedge$ then $\mathsf{I}^k_C h \vdash_{\approx} \Gamma, C[k]$, $\mathcal{C}$-$\mathrm{crk}(\mathsf{I}^k_C h) \leq \mathcal{C}$-$\mathrm{crk}(h)$ and $\mathrm{o}(\mathsf{I}^k_C h) \leq \mathrm{o}(h)$.

- The symbol R_C denotes a *one-cut-reduction operator* which satisfies: If $h_0 \vdash_{\approx} \Gamma, C$, $h_1 \vdash_{\approx} \Gamma, \neg C$ and $\mathrm{tp}(C) \in \{\top, \bigwedge\}$, then $\mathsf{R}_C h_0 h_1 \vdash_{\approx} \Gamma$, $\mathcal{C}\text{-crk}(\mathsf{R}_C h_0 h_1) \leq \max\{\mathcal{C}\text{-crk}(h_0), \mathcal{C}\text{-crk}(h_1), \mathcal{C}\text{-rk}(C)\}$ and $\mathrm{o}(\mathsf{R}_C h_0 h_1) \leq \mathrm{o}(h_0) + \mathrm{o}(h_1)$.

- The symbol E denotes a *highest-cut-elimination operator* which satisfies: If $h \vdash_{\approx} \Gamma$ then $\mathsf{E}h \vdash_{\approx} \Gamma$ and $\mathcal{C}\text{-crk}(\mathsf{E}h) \leq \mathcal{C}\text{-crk}(h) \dot{-} 1$ and $\mathrm{o}(\mathsf{E}h) < 2^{\mathrm{o}(h)}$.

Definition 4.12. The *notation system $\mathcal{CH}$ for cut-elimination on $\mathcal{H}$* is given by the set of terms $\mathcal{CH}$ which are inductively defined by

- $\mathcal{H} \subset \mathcal{CH}$,

- $h \in \mathcal{CH}$, $C \in \mathcal{F}$ with $\mathrm{tp}(C) = \bigwedge$, $k < \omega \quad \Rightarrow \quad \mathsf{I}_C^k h \in \mathcal{CH}$,

- $h_0, h_1 \in \mathcal{CH}$, $C \in \mathcal{F}$ with $\mathrm{tp}(C) \in \{\top, \bigwedge\} \quad \Rightarrow \quad \mathsf{R}_C h_0 h_1 \in \mathcal{CH}$,

- $h \in \mathcal{CH} \quad \Rightarrow \quad \mathsf{E}h \in \mathcal{CH}$,

where $\mathsf{I}, \mathsf{R}, \mathsf{E}$ are new symbols, and functions $\mathrm{tp}\colon \mathcal{CH} \to \mathfrak{S}_{\mathcal{F}}$, $\cdot[\cdot]\colon \mathcal{CH} \times \mathbb{N} \to \mathcal{CH}$, $\Gamma\colon \mathcal{CH} \to \mathfrak{P}_{\mathrm{fin}}(\mathcal{F})$, $\mathrm{crk}\colon \mathfrak{P}(\mathcal{F}) \times \mathcal{CH} \to \mathbb{N}$, $\mathrm{o}\colon \mathcal{CH} \to \mathbb{N} \setminus \{0\}$ and $|\cdot|\colon \mathcal{CH} \to \mathbb{N}$ defined by recursion on the complexity of $h \in \mathcal{CH}$:

- If $h \in \mathcal{H}$ then all functions are inherited from $\mathcal{H}$.

- $h = \mathsf{I}_C^k h_0$: Let $\Gamma(h) := \{C[k]\} \cup (\Gamma(h_0) \setminus \approx\{C\})$, $\mathcal{C}\text{-crk}(h) := \mathcal{C}\text{-crk}(h_0)$, $\mathrm{o}(h) := \mathrm{o}(h_0)$, and $|h| := |h_0| + 1$.

  Case 1. $\mathrm{tp}(h_0) \in \{\bigwedge_D \colon D \approx C\}$. Then let $\mathrm{tp}(h) := \mathrm{Rep}$, and $h[0] := \mathsf{I}_C^k h_0[k]$.

  Case 2. Otherwise, let $\mathrm{tp}(h) := \mathrm{tp}(h_0)$, and $h[i] := \mathsf{I}_C^k h_0[i]$.

- $h = \mathsf{R}_C h_0 h_1$: Let $\mathcal{I} := \mathrm{tp}(h_1)$. We define $\Gamma(h) := (\Gamma(h_0) \setminus \approx\{C\}) \cup (\Gamma(h_1) \setminus \approx\{\neg C\})$, $\mathcal{C}\text{-crk}(h) := \max\{\mathcal{C}\text{-crk}(h_0), \mathcal{C}\text{-crk}(h_1), \mathcal{C}\text{-rk}(C)\}$, $\mathrm{o}(h) := \mathrm{o}(h_0) + \mathrm{o}(h_1)$, and $|h| := |h_0| + |h_1| + 1$. For $\mathrm{tp}(h)$ and $h[i]$ we consider the following two cases:

  Case 1. $\Delta(\mathcal{I}) \cap \approx\{\neg C\} = \emptyset$: Then let $\mathrm{tp}(h) := \mathcal{I}$, and $h[i] := \mathsf{R}_C h_0 h_1[i]$.

  Case 2. Otherwise, $\Delta(\mathcal{I}) \cap \approx\{\neg C\} \neq \emptyset$. Since $\mathrm{tp}(C) \in \{\top, \bigwedge\}$ and no inference symbol $\mathcal{I}'$ of $\mathfrak{S}_{\mathcal{F}}$ has $D \in \Delta(\mathcal{I}')$ with $\mathrm{tp}(D) = \bot$, we must have $\mathrm{tp}(C) = \bigwedge$. Thus $\mathcal{I} = \bigvee_D^k$ for some $k \in \mathbb{N}$ and $D \approx \neg C$. Then let $\mathrm{tp}(h) := \mathrm{Cut}_{C[k]}$ and $h[0] := \mathsf{I}_C^k h_0$, $h[1] := \mathsf{R}_C h_0 h_1[0]$.

- $h = \mathsf{E}h_0$: Let $\Gamma(h) := \Gamma(h_0)$, $\mathcal{C}\text{-crk}(h) := \mathcal{C}\text{-crk}(h_0) \dot{-} 1$, $\mathrm{o}(h) := 2^{\mathrm{o}(h_0)} - 1$, and $|h| := |h_0| + 1$.

Case 1. $\mathrm{tp}(h_0) = \mathrm{Cut}_C$: Then let $\mathrm{tp}(h) := \mathrm{Rep}$ and
let $h[0] := \mathsf{R}_C\mathsf{E}h_0[0]\mathsf{E}h_0[1]$ if $\mathrm{tp}(C) \in \{\top, \bigwedge\}$,
let $h[0] := \mathsf{R}_{\neg C}\mathsf{E}h_0[1]\mathsf{E}h_0[0]$ if $\mathrm{tp}(C) \notin \{\top, \bigwedge\}$.

Case 2. Otherwise, let $\mathrm{tp}(h) := \mathrm{tp}(h_0)$, and $h[i] := \mathsf{E}h_0[i]$.

It has been shown in [AB09] that the notation system for cut-elimination on $\mathcal{H}$ is a notation system in the sense of Definition 4.9.

4.5 Size Bounds of Notations for Cut-Elimination

Notation systems for propositional formulas and proofs will, as we will see later, be feasible in situations related to definable search problems of Bounded Arithmetic. We will now analyse the feasibility of notations for cut-reduction on propositional proofs, by studying the size of notations for cut-reduction. We will just state the necessary definitions and results, more details including full proofs can be found in [AB09].

Definition 4.13. $\mathcal{H}$ is called *bounded* if $|h[i]| \le |h|$ for all $h \in \mathcal{H}$, $i < |\mathrm{tp}(h)|$.

Definition 4.14. We define a "size function" $\vartheta\colon \mathbb{N} \to \mathbb{N}$ by induction on the inductive definition of $\mathcal{CH}$ as follows.

- For $h \in \mathcal{H}$ we set $\vartheta(h) = |h|$.
- $\vartheta(\mathsf{I}^k_C h) = \vartheta(h) + 1$
- $\vartheta(\mathsf{R}_C h_0 h_1) = \max\{|h_0|+1+\vartheta(h_1)\ ,\ \vartheta(h_0)+1\}$
- $\vartheta(\mathsf{E}h) = o(h)(\vartheta(h) + 2)$

Proposition 4.15. *If $\mathcal{H}$ is bounded then for every $h \in \mathcal{CH}$ we have $|h| \le \vartheta(h)$.*

Theorem 4.16. *If $\mathcal{H}$ is bounded, $h \in \mathcal{CH}$ and $i < |\mathrm{tp}(h)|$, then $\vartheta(h) \ge \vartheta(h[i])$.*

Definition 4.14, Proposition 4.15 and Theorem 4.16 together show that cut-reduction can behave feasibly on proof notations. E.g., assume that we have a proof notation $h(a)$ depending on some parameter a — such a notation may originate from a first order proof of a universal statement $(\forall x)\varphi(x)$, where we inverted the outermost universal quantifier and substituted the constant $\underline{a}$ for the new free variable x, thus considering a proof of $\varphi(\underline{a})$ for $a \in \mathbb{N}$ — such that $o(h(a))$ and $|h(a)|$ are polynomial in $|a|$. Applying cut-reduction once to $h(a)$ gives a propositional proof in which all subproofs can be denoted by a notation of size polynomial in $|a|$: Consider a subproof h' of $\mathsf{E}h(a)$ which is given by the path $i_1, \dots, i_k$, i.e. $h' = \mathsf{E}h(a)[i_1]\cdots[i_k]$. By

Proposition 4.15, $|h'| \leq \vartheta(h')$, and by Theorem 4.16, $\vartheta(h') \leq \vartheta(\mathsf{E}h(a))$. By Definition 4.14, the latter can be computed to

$$\vartheta(\mathsf{E}h(a)) = o(h(a)) \cdot (\vartheta(h(a)){+}2) = o(h(a)) \cdot (|h(a)|{+}2)$$

which is polynomial in $|a|$.

In the next section we will define concrete notation systems for propositional formulas and proofs based on translating Bounded Arithmetic according to the Paris-Wilkie translation. Together with the results from this section they provide the concrete machinery for characterising definable search problems via proof notations.

5 Notations based on Bounded Arithmetic

We start by defining a notation system for propositional formulas obtained by translating the language of Bounded Arithmetic according to the Paris-Wilkie translation, as given in [AB09].

Let $\mathcal{F}_{\mathrm{BA}}$ be the set of closed formulas in Δ_0. We define the outermost connective function on $\mathcal{F}_{\mathrm{BA}}$ by

$$\mathrm{tp}(A) := \begin{cases} \top & A \text{ true literal} \\ \bot & A \text{ false literal} \\ \bigwedge & A \text{ is of the form } A_0 \ \wedge \ A_1 \text{ or } (\forall x)B \\ \bigvee & A \text{ is of the form } A_0 \ \vee \ A_1 \text{ or } (\exists x)B \ \ , \end{cases}$$

and the subformula function on $\mathcal{F}_{\mathrm{BA}} \times \mathbb{N}$ by

$$A[n] := \begin{cases} A & A \text{ literal} \\ A_{\min(n,1)} & A \text{ is of the form } A_0 \ \wedge \ A_1 \text{ or } A_0 \ \vee \ A_1 \\ B_x(\underline{n}) & A \text{ is of the form } (\forall x)B \text{ or } (\exists x)B \ \ . \end{cases}$$

To define a suitable rank function on $\mathcal{F}_{\mathrm{BA}}$, we first define an auxiliary rank function rk'. Let $\mathcal{C}$ be a subset of $\mathcal{F}_{\mathrm{BA}}$, and A in $\mathcal{F}_{\mathrm{BA}}$. We define $\mathcal{C}$-rk'(A) by induction on the complexity of A. If $A \in \mathcal{C} \cup \neg\mathcal{C}$, let $\mathcal{C}$-rk'$(A) := -1$. For $A \notin \mathcal{C} \cup \neg\mathcal{C}$, $\mathcal{C}$-rk'(A) is defined as follows:

- Let $\mathcal{C}$-rk'$(A) := 1 + \max\{\mathcal{C}\text{-rk'}(B), \mathcal{C}\text{-rk'}(C)\}$ in case $A = B \ \wedge \ C$ or $A = B \ \vee \ C$.
- If $A = (\forall x)B$ or $A = (\exists x)B$, let $\mathcal{C}$-rk'$(A) := 1 + \mathcal{C}$-rk'(B).

Using the auxiliary rank function rk', we define the *$\mathcal{C}$-rank of A*, denoted $\mathcal{C}$-rk(A), by $\mathcal{C}\text{-rk}(A) := \max\{0, \mathcal{C}\text{-rk'}(A)\}$. Observe that $\mathrm{s}\Sigma^{\mathrm{b}}_i$-rk$(A) \leq$ $\mathrm{s}\Sigma^{\mathrm{b}}_{i+1}$-rk$(A) + 1$. If $\mathcal{C}$ is the set of quantifier-free formulas, and $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_\infty$, then the rank of φ as defined in Section 2 is the same as $\mathcal{C}$-rk(φ), i.e. $\mathcal{C}$-rk(φ) computes the minimal k such that $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_k \cup \mathrm{s}\Pi^{\mathrm{b}}_k$.

The negation function for the notation system is the same as defined for $\mathcal{L}_{\mathrm{BA}}$. Intensional equality is defined in the following way: For t a closed term its numerical value $t^{\mathbb{N}} \in \mathbb{N}$ is defined in the obvious way. Let $\to^1_{\mathbb{N}}$ denote the rewriting relation on $\mathcal{L}_{\mathrm{BA}}$-terms and $\mathcal{L}_{\mathrm{BA}}$-formulas obtained from

$$\Big\{(t, \underline{t^{\mathbb{N}}})\colon t \text{ a closed term}\Big\} \enspace .$$

Let $\approx_{\mathbb{N}}$ denote the reflexive, symmetric and transitive closure of $\to^1_{\mathbb{N}}$. For example, $(\forall x)((\underline{3} + \underline{1}) \cdot x = \underline{1} + \underline{5}) \approx_{\mathbb{N}} (\forall x)(\underline{4} \cdot x = \underline{6})$.

Proposition 5.1. *The system* $\langle \mathcal{F}_{\mathrm{BA}}, \mathrm{tp}, \cdot[\cdot], \neg, \mathrm{rk}, \approx_{\mathbb{N}} \rangle$ *which we have just defined forms a notation system for formulas in the sense of Definition 4.7.*

Let ${\approx_{\mathbb{N}}}^k$ denote the restriction of $\approx_{\mathbb{N}}$ to expressions of depth $\leq k$. In a feasible Gödel numbering, like the one defined in [Bus86], the Gödel number for c_a has size proportional to $|a|$. Thus, for each k, the relation ${\approx_{\mathbb{N}}}^k$ is a polynomial time predicate. We will always assume that $\mathcal{F}_{\mathrm{BA}}$ implicitly contains such a constant k without explicitly mentioning it. All formulas and terms used in $\mathcal{F}_{\mathrm{BA}}$ are thus assumed to obey the abovementioned restriction on depth. We will come back to this restriction at relevant places. The next observation already makes use of this assumption.

Observation 5.2. *All relations and functions in* $\mathcal{F}_{\mathrm{BA}}$ *are polynomial time computable.*

Definition 5.3. Let BA^∞ denote the propositional proof system over $\mathcal{F}_{\mathrm{BA}}$ according to Definition 4.8.

Definition 5.4. The *finitary proof system* $\mathrm{BA}^\star$ is the proof system over $\langle \Delta_0, \approx_{\mathbb{N}}, \mathrm{rk} \rangle$ which is given by the following set of inference symbols.

(Ax_Δ) $\quad \dfrac{}{\Delta}$ $\quad$ if $\bigvee \Delta \in \overline{\mathrm{BASIC}}$

$(\bigwedge_{A_0 \wedge A_1})$ $\quad \dfrac{A_0 \qquad A_1}{A_0 \wedge A_1}$ $\qquad$ $(\bigvee^k_{A_0 \vee A_1})$ $\quad \dfrac{A_k}{A_0 \vee A_1}$

$(\bigwedge^y_{(\forall x)A})$ $\quad \dfrac{A_x(y)}{(\forall x)A}$ $\qquad$ $(\bigvee^t_{(\exists x)A})$ $\quad \dfrac{A_x(t)}{(\exists x)A}$

$(\mathrm{IND}^{y,t}_F)$ $\quad \dfrac{\neg F, F_y(y+1)}{\neg F_y(0), F_y(2^{|t|})}$ $\qquad$ $(\mathrm{IND}^{y,n,i}_F)$ $\quad \dfrac{\neg F, F_y(y+1)}{\neg F_y(\underline{n}), F_y(\underline{n + 2^i})}$

(Cut_C) $\quad \dfrac{C \qquad \neg C}{\emptyset}$ for $C \in \Delta_0$ with C atomic or $\mathrm{tp}(C) = \bigwedge$

where in case $(\bigvee^k_{A_0 \vee A_1})$ we have that $k \in \{0, 1\}$, and in case $(\mathrm{IND}^{y,n,i}_F)$ that $n, i \in \mathbb{N}$.

According to Definition 4.4, $\mathrm{BA}^\star$-quasi derivations h are equipped with functions $\Gamma(h)$ denoting the endsequent of h, $\mathrm{hgt}(h)$ denoting the height of h, and $\mathrm{sz}(h)$ denoting the size of h.

In the following we will not need the cut-rank function which comes with $\mathrm{BA}^\star$-quasi derivations, but we will need a more general cut-rank function gcrk, which will also bound the rank of induction formulas.

Definition 5.5. Let h be a $\mathrm{BA}^\star$-quasi derivation, $h = \mathcal{I}h_0 \cdots h_{n-1}$. We define

$$\mathcal{C}\text{-gcrk}(h) := \sup(\{\mathcal{C}\text{-grk}(\mathcal{I})\} \cup \{\mathcal{C}\text{-gcrk}(h_i) \colon i < n\})$$

where $\mathcal{C}\text{-grk}(\mathcal{I})$, the *generalised cut-rank of* $\mathcal{I}$, is $\mathcal{C}\text{-rk}(C) + 1$ if $\mathcal{I}$ is of the form Cut_C, $\mathrm{IND}_C^{y,t}$ or $\mathrm{IND}_C^{y,n,i}$ for $C \notin \mathcal{C}$, and 0 otherwise.

Observe that $\mathrm{s}\Sigma_i^\mathrm{b}\text{-gcrk}(h) \leq \mathrm{s}\Sigma_{i+1}^\mathrm{b}\text{-gcrk}(h)+1$, which immediately follows from $\mathrm{s}\Sigma_i^\mathrm{b}\text{-gcrk}(\mathcal{I}) \leq \mathrm{s}\Sigma_{i+1}^\mathrm{b}\text{-gcrk}(\mathcal{I}) + 1$.

Definition 5.6 (Inductive definition of $\vec{x} \colon h$ and $\mathrm{BA}^\star$-derivations)**.** For $\vec{x}$ a finite list of disjoint variables and $h = \mathcal{I}h_0 \cdots h_{n-1}$ a $\mathrm{BA}^\star$-quasi-derivation we inductively define the relation $\vec{x} \colon h$ that h *is a* $\mathrm{BA}^\star$*-derivation with free variables among* $\vec{x}$ as follows.

- If $\vec{x}, y \colon h_0$ and $\mathcal{I} \in \{\bigwedge_{(\forall x)A}^y, \mathrm{IND}_F^{y,t}, \mathrm{IND}_F^{y,n,i}\}$ for some A, F, t, n, i, and $\mathrm{FV}(t) \cup \mathrm{FV}(\Gamma(\mathcal{I}h_0)) \subset \{\vec{x}\}$ then $\vec{x} \colon \mathcal{I}h_0$.
- If $\vec{x} \colon h_0$ and $\mathrm{FV}((\exists x)A), \mathrm{FV}(t) \subseteq \{\vec{x}\}$ then $\vec{x} \colon \bigvee_{(\exists x)A}^t h_0$.
- If $\vec{x} \colon h_0$, $\vec{x} \colon h_1$ and $\mathrm{FV}(C) \subseteq \{\vec{x}\}$ then $\vec{x} \colon \mathrm{Cut}_C h_0 h_1$.
- If $\mathrm{FV}(\Delta) \subseteq \{\vec{x}\}$ then $\vec{x} \colon \mathrm{Ax}_\Delta$,
- If $\vec{x} \colon h_0$, $\vec{x} \colon h_1$ and $\mathcal{I} = \bigwedge_{A_0 \wedge A_1}$ with $\mathrm{FV}(A_0 \wedge A_1) \subset \{\vec{x}\}$ then $\vec{x} \colon \mathcal{I}h_0h_1$.
- If $\vec{x} \colon h_0$ and $\mathcal{I} = \bigvee_{A_0 \vee A_1}^k$ with $\mathrm{FV}(A_0 \vee A_1) \subset \{\vec{x}\}$ then $\vec{x} \colon \mathcal{I}h_0$.

We call a $\mathrm{BA}^\star$-derivation h *closed*, if $\emptyset \colon h$.

Definition 5.7. For h a $\mathrm{BA}^\star$-derivation, y a variable and t a closed term of Bounded Arithmetic we define the substitution $h(t/y)$ inductively by setting $(\mathcal{I}h_0 \cdots h_{n-1})(t/y)$ to be $\mathcal{I}(t/y)h_0(t/y) \cdots h_{n-1}(t/y)$ if $\mathcal{I}$ is not of the form $\bigwedge_{(\forall x)A}^y$, $\mathrm{IND}_F^{y,t}$, or $\mathrm{IND}_F^{y,n,i}$ with the same variable y, and $\mathcal{I}h_0 \cdots h_{n-1}$ otherwise.

Substitution for inference symbols is defined by setting

$$\begin{array}{lcllcl}
\mathrm{Ax}_\Delta(t/y) & = & \mathrm{Ax}_{\Delta(t/y)} & & & \\
\bigwedge_{A_0 \wedge A_1}(t/y) & = & \bigwedge_{(A_0 \wedge A_1)(t/y)} & \bigvee_{A_0 \wedge A_1}^k(t/y) & = & \bigvee_{(A_0 \wedge A_1)(t/y)}^k \\
\bigwedge_{(\forall x)A}^z(t/y) & = & \bigwedge_{((\forall x)A)(t/y)}^z & \bigvee_{(\exists x)A}^{t'}(t/y) & = & \bigvee_{((\exists x)A)(t/y)}^{t'(t/y)} \\
\mathrm{IND}_F^{z,t'}(t/y) & = & \mathrm{IND}_{F(t/y)}^{z,t'(t/y)} & \mathrm{IND}_F^{z,n,i}(t/y) & = & \mathrm{IND}_{F(t/y)}^{z,n,i}
\end{array}$$

The next Lemma shows the substitution property for BA*-derivations. The strange looking "$\subseteq$" instead of the expected equality comes from the fact that a substitution may make formulas equal which are not equal without the substitution.

Lemma 5.8. *Assume $\vec{x}\colon h$ and let y be a variable and t a closed term, then $\vec{x} \setminus \{y\}\colon h(t/y)$ and moreover $\Gamma(h(t/y)) \subseteq (\Gamma(h))(t/y)$.*

We will now define the ingredients for a notation system $\mathcal{H}_{\mathrm{BA}}$ for BA$^\infty$ according to Definition 4.9. The interpretation $[\![h]\!]$ for $h \in \mathcal{H}_{\mathrm{BA}}$ according to Definition 4.10 formalises a translation of closed BA*-derivations into BA$^\infty$, which is called an *embedding.*

Let $\mathcal{H}_{\mathrm{BA}}$ be the set of closed BA*-derivations. For each $h \in \mathcal{H}_{\mathrm{BA}}$ we define the denoted last inference $\mathrm{tp}(h)$ as follows: Let $h = \mathcal{I}h_0 \cdots h_{n-1}$,

$$\mathrm{tp}(h) := \begin{cases} \mathrm{Ax}_A & \text{if } \mathcal{I} = \mathrm{Ax}_\Delta, \text{ where } A \text{ is the} \\ & \qquad\quad \text{“least” true literal in } \Delta \\ \bigwedge_{A_0 \wedge A_1} & \text{if } \mathcal{I} = \bigwedge_{A_0 \wedge A_1} \\ \bigvee^k_{A_0 \vee A_1} & \text{if } \mathcal{I} = \bigvee^k_{A_0 \vee A_1} \\ \bigwedge_{(\forall x)A} & \text{if } \mathcal{I} = \bigwedge^y_{(\forall x)A} \\ \bigvee^{t^{\mathbb{N}}}_{(\exists x)A} & \text{if } \mathcal{I} = \bigvee^t_{(\exists x)A} \\ \mathrm{Rep} & \text{if } \mathcal{I} = \mathrm{IND}^{y,t}_F \\ \mathrm{Rep} & \text{if } \mathcal{I} = \mathrm{IND}^{y,n,0}_F \\ \mathrm{Cut}_{F_y(\underline{n+2^i})} & \text{if } \mathcal{I} = \mathrm{IND}^{y,n,i+1}_F \\ \mathrm{Cut}_C & \text{if } \mathcal{I} = \mathrm{Cut}_C \end{cases}$$

For each $h \in \mathcal{H}_{\mathrm{BA}}$ and $j \in \mathbb{N}$ we define the denoted subderivation $h[j]$ as follows: Let $h = \mathcal{I}h_0 \cdots h_{n-1}$. If $j \geq |\,\mathrm{tp}(h)|$ let $h[j] := \mathrm{Ax}_{0=0}$. Otherwise, assume $j < |\,\mathrm{tp}(h)|$ and define

$$h[j] := \begin{cases} h_{\min(j,1)} & \text{if } \mathcal{I} = \bigwedge_{A_0 \wedge A_1} \\ h_0 & \text{if } \mathcal{I} = \bigvee^k_{A_0 \vee A_1} \\ h_0(\underline{j}/y) & \text{if } \mathcal{I} = \bigwedge^y_{(\forall x)A} \\ h_0 & \text{if } \mathcal{I} = \bigvee^t_{(\exists x)A} \\ \mathrm{IND}^{y,0,|t|^{\mathbb{N}}}_F h_0 & \text{if } \mathcal{I} = \mathrm{IND}^{y,t}_F \\ h_0(\underline{n}/y) & \text{if } \mathcal{I} = \mathrm{IND}^{y,n,0}_F \\ \mathrm{IND}^{y,n,i}_F h_0 & \text{if } \mathcal{I} = \mathrm{IND}^{y,n,i+1}_F \text{ and } j = 0 \\ \mathrm{IND}^{y,n+2^i,i}_F h_0 & \text{if } \mathcal{I} = \mathrm{IND}^{y,n,i+1}_F \text{ and } j = 1 \\ h_j & \text{if } \mathcal{I} = \mathrm{Cut}_C \end{cases}$$

The denoted end-sequent function on $\mathcal{H}_{\mathrm{BA}}$ is given by Γ. The size function $|\cdot|$ on $\mathcal{H}_{\mathrm{BA}}$ is given by $|h| := \mathrm{sz}(h)$. We define the denoted cut-rank function for $h \in \mathcal{H}_{\mathrm{BA}}$ to be $\mathcal{C}\text{-}\mathrm{crk}(h) := \mathcal{C}\text{-}\mathrm{gcrk}(h)$. We observe that $\mathcal{C}\text{-crk}(h[\iota]) \leq \mathcal{C}\text{-crk}(h)$ for $\iota < |\operatorname{tp}(h)|$, and that $\mathcal{C}\text{-rk}(C) < \mathcal{C}\text{-crk}(h)$ if $\operatorname{tp}(h) = \mathrm{Cut}_C$ and $C \notin \mathcal{C}$.

To define the denoted height function we need some analysis yielding an upper bound to the log of the lengths of inductions which may occur during the embedding (we take the log as this bounds the height of the derivation tree which embeds an application of induction). Let us first assume m is such an upper bound, and let us define the denoted height $\mathrm{o}_m(h)$ of h relative to m: For a $\mathrm{BA}^\star$-derivation $h = \mathcal{I}h_0 \cdots h_{n-1}$ we define

$$\mathrm{o}_m(h) := \begin{cases} \mathrm{o}_m(h_0) + i + 1 & \text{if } \mathcal{I} = \mathrm{IND}_F^{y,n,i} \\ \mathrm{o}_m(h_0) + m + 1 & \text{if } \mathcal{I} = \mathrm{IND}_F^{y,t} \\ 1 + \sup_{i<n} \mathrm{o}_m(h_i) & \text{otherwise} \end{cases}$$

Observe that $\mathrm{o}_m(h) > 0$ (in particular, $\mathrm{o}(\mathrm{Ax}_\Delta) = 1$).

To fill the gap of providing a suitable upper bound function of $\mathrm{BA}^\star$-derivations we first need to fix monotone bounding terms for any term in $\mathcal{L}_{\mathrm{BA}}$.

Bounding Terms for Language and Proofs

For a term t we define a term $\mathrm{bd}(t)$ which represents a monotone function with the following property: If $\mathrm{FV}(t) = \{\vec{x}\}$ then

$$(\forall \vec{n}) \qquad t_{\vec{x}}(\underline{\vec{n}})^{\mathbb{N}} \quad \leq \quad \mathrm{bd}(t)_{\vec{x}}(\underline{\vec{n}})^{\mathbb{N}}$$

The precise definition of $\mathrm{bd}(t)$ is not essential here, we can for example use the meta-function σ from [Bus86, p.77], or the explicit definition given in [AB09].

For $h \in \mathcal{H}_{\mathrm{BA}}$, the bounding term $\mathrm{bd}(h)$ is intended to bound any variable which occurs during the embedding of h. Then, the term $|\mathrm{bd}(h)|$ will bound the length of any induction which occurs during the embedding of h. This situation is related to the notion *proofs restricted by parameter variables* as defined in [Bus86, Section 4.5], where proofs are transformed in such a way that bounds to inductions and quantification only depend on the parameter variables of the proof — then the above mentioned bounding term $\mathrm{bd}(h)$ can simply be obtained by collecting all such bounds and taking their maximum. Let $h = \mathcal{I}h_0 \cdots h_{n-1}$ be in $\mathcal{H}_{\mathrm{BA}}$. Let $\max(n_1, \ldots, n_k)$ denote the maximal value amongst $\{n_1, \ldots, n_k\}$, where we set $\max() = 0$. We define

$$\mathrm{bd}(h) := \begin{cases} \max(\mathrm{bd}(h_0(\underline{\mathrm{bd}(t)}/y)), \mathrm{bd}(t)) & \text{if } \mathcal{I} = \bigwedge^y_{(\forall x \leq t)A} \\ \max(\mathrm{bd}(h_0), \mathrm{bd}(t)) & \text{if } \mathcal{I} = \bigvee^t_{(\exists x)A} \\ \max(\mathrm{bd}(h_0(\underline{2^{|\mathrm{bd}(t)|}}/y)), 2^{|\mathrm{bd}(t)|}) & \text{if } \mathcal{I} = \mathrm{IND}_F^{y,t} \\ \max(\mathrm{bd}(h_0(\underline{n + 2^i}/y)), n + 2^i) & \text{if } \mathcal{I} = \mathrm{IND}_F^{y,n,i} \\ \max(\mathrm{bd}(h_0), \ldots, \mathrm{bd}(h_{n-1})) & \text{otherwise.} \end{cases}$$

Now we define for $h \in \mathcal{H}_{\mathrm{BA}}$ the denoted height function $\mathrm{o}(h)$ as $\mathrm{o}_{|\mathrm{bd}(h)|}(h)$.

Theorem 5.9. *The just defined system* $\langle \mathcal{H}_{\mathrm{BA}}, \mathrm{tp}, \cdot[\cdot], \Gamma, \mathrm{crk}, \mathrm{o}(\cdot), |\cdot| \rangle$ *forms a notation system for* BA^∞ *in the sense of Definition 4.9. Furthermore,* $\mathcal{H}_{\mathrm{BA}}$ *is bounded in the sense of Definition 4.13.*

A proof of this Theorem can be found in [AB09]. The fact that $\mathcal{H}_{\mathrm{BA}}$ is bounded is easily observed by inspection.

Observation 5.10. *We assume that we have fixed a* $k \in \mathbb{N}$ *bounding depths of formulas and terms as explained in the remark on page 20, and some feasible Gödel numbering like the one in [Bus86]. Then, the following relations and functions are polynomial time computable (when interpreted as relations and functions on the corresponding Gödel numbers of syntactical objects): the finitary proof system* $\mathrm{BA}^\star$*, the set of* $\mathrm{BA}^\star$*-quasi derivations and the functions* $h \mapsto \Gamma(h)$*,* $h \mapsto \mathrm{hgt}(h)$*, and* $h \mapsto \mathrm{sz}(h)$ *denoting the endsequent, the height and the size for a* $\mathrm{BA}^\star$*-quasi derivation* h*; the bounding term* $t \mapsto \mathrm{bd}(t)$ *for terms* t *occurring in* $\mathcal{F}_{\mathrm{BA}}$ *and the relations* $\mathrm{bd}(h) \leq m$ *on* $\mathcal{H}_{\mathrm{BA}} \times \mathbb{N}$*; the set* $\mathcal{H}_{\mathrm{BA}}$ *and the functions* $h \mapsto \mathrm{tp}(h)$*,* $h, i \mapsto h[i]$*,* $h \mapsto \Gamma(h)$*,* $m, h \mapsto \mathrm{o}_m(h)$ *and* $h \mapsto |h|$*.*

We now provide a connection between $\mathrm{BA}^\star/\mathcal{H}_{\mathrm{BA}}$ and the theories of Bounded Arithmetic as defined in Section 2. This step also includes some proof normalisation which is similar to known ones in the literature, for example free cut-elimination in [Bus86] or partial cut-elimination in [Bec03].

Theorem 5.11 (Partial Cut-elimination)**.** *Assume* $\mathrm{T}^j_2 \vdash \varphi$ *with* $\varphi \in \Delta_0$ *and* $\mathrm{FV}(\varphi) \subseteq \{x\}$*. Then, there is some* $\mathrm{BA}^\star$*-derivation* h *such that* $\mathrm{FV}(h) \subseteq \{x\}$*,* $\Gamma(h) = \{\varphi\}$*,* $\mathrm{s}\Sigma^{\mathrm{b}}_j\text{-gcrk}(h) = 0$ *and* $\mathrm{o}(h(\underline{a}/x)) = |a|^{O(1)}$*.*

A proof of the last theorem can be found in [AB09].

5.1 Complexity Notions for $\mathrm{BA}^\star$

In order to describe local search problems based on proof notations we need some notions describing key complexity properties of $\mathrm{BA}^\star$ proof notations. Again, we will just state the necessary definitions and results, more details including full proofs can be found in [AB09].

Definition 5.12. We extend the definition of bounding terms $\mathrm{bd}(h)$ from $\mathcal{H}_{\mathrm{BA}}$ to $\mathcal{CH}_{\mathrm{BA}}$ by induction on $h \in \mathcal{CH}_{\mathrm{BA}}$ in the following way:

- If $h \in \mathcal{H}_{\mathrm{BA}}$ then the definition of $\mathrm{bd}(h)$ is inherited from the definition of $\mathrm{bd}(h)$ on $\mathcal{H}_{\mathrm{BA}}$.
- $\mathrm{bd}(\mathsf{I}^k_C h_0) := \mathrm{bd}(h_0)$.
- $\mathrm{bd}(\mathsf{R}_C h_0 h_1) := \max\{\mathrm{bd}(h_0), \mathrm{bd}(h_1)\}$.
- $\mathrm{bd}(\mathsf{E} h_0) := \mathrm{bd}(h_0)$.

Lemma 5.13. *Let $h \in \mathcal{CH}_{\mathrm{BA}}$.*

1. $\mathrm{bd}(h[j]) \leq \mathrm{bd}(h)$ *for all j.*

2. *If* $\mathrm{tp}(h) = \bigvee_C^k$ *then $k \leq \mathrm{bd}(h)$.*

Definition 5.14. For h a $\mathrm{BA}^\star$-derivation or $h \in \mathcal{CH}_{\mathrm{BA}}$, we define *the set of decorations of h,* $\mathrm{deco}(h)$, by induction on h. $\mathrm{deco}(h)$ will be a finite set of $\mathcal{L}_{\mathrm{BA}}$-terms and formulas in Δ_0. Let $h = \mathcal{I}h_0 \cdots h_{n-1}$, where $\mathcal{I}$ ranges over $\mathrm{BA}^\star \cup \{\mathsf{I}_C^k, \mathsf{R}_C, \mathsf{E}\}$. We define

$$\mathrm{deco}(h) := \mathrm{deco}(\mathcal{I}) \cup \bigcup_{i<n} \mathrm{deco}(h_i)$$

where

$$\begin{aligned}
\mathrm{deco}(\mathcal{I}) &:= \Delta(\mathcal{I}) \text{ for } \mathcal{I} = \mathrm{Ax}_\Delta, \textstyle\bigwedge_{A_0 \wedge A_1}, \bigvee^k_{A_0 \vee A_1} \\
\mathrm{deco}(\textstyle\bigwedge^y_{(\forall x)A}) &:= \{(\forall x)A, y\} \\
\mathrm{deco}(\textstyle\bigvee^t_{(\exists x)A}) &:= \{(\exists x)A, t\} \\
\mathrm{deco}(\mathrm{IND}_F^{y,t}) &:= \{F, \neg F_y(0), F_y(2^{|t|}), y, t\} \\
\mathrm{deco}(\mathrm{IND}_F^{y,n,i}) &:= \{F, \neg F_y(\underline{n}), F_y(\underline{n + 2^i}), y, c_n\} \\
\mathrm{deco}(\mathrm{Cut}_C) &:= \{C\} \\
\mathrm{deco}(\mathsf{I}_C^k) &:= \{C, C[k], c_k\} \\
\mathrm{deco}(\mathsf{R}_C) &:= \{C\} \\
\mathrm{deco}(\mathsf{E}) &:= \emptyset \ .
\end{aligned}$$

Observation 5.15. *We have $\Gamma(h) \subseteq \mathrm{deco}(h)$.*

Definition 5.16. Let Φ be a set of $\mathcal{L}_{\mathrm{BA}}$-terms and formulas in Δ_0, and let $K \in \mathbb{N}$ be a size parameter. With Φ_K we denote the set obtained by enlarging Φ by the set $\{c_i \colon 0 \leq i \leq K\}$ and the set of formulas and terms which result from formulas and terms in Φ by substituting constants from $\{c_i \colon 0 \leq i \leq K\}$ for some (possibly none, possibly all) of the free variables.

Lemma 5.17. *Let Φ be a set of $\mathcal{L}_{\mathrm{BA}}$-terms and formulas in Δ_0, such that $\Phi \cap \Delta_0$ is closed under negation and taking subformulas. Let $j, K \in \mathbb{N}$ and y be a variable.*

1. *If $j \leq K$ and $C \in \Phi \cap \Delta_0$, then $C[j] \in \Phi_K$.*

2. *If $h \in \mathrm{BA}^\star$ with* $\mathrm{deco}(h) \subseteq \Phi$, *and $j \leq K$, then* $\mathrm{deco}(h(\underline{j}/y)) \subseteq \Phi_K$.

3. $\Delta(\mathrm{tp}(h)) \subseteq \mathrm{deco}(h)_{\mathrm{bd}(h)}$ *with the subscript understood in the sense of Definition 5.16.*

4. If $h \in \mathcal{CH}_{\mathrm{BA}}$ *with* $\mathrm{deco}(h) \subseteq \Phi$ *and* $j \leq K$*, then* $\mathrm{deco}(h[j]) \subseteq \Phi_{\max\{K,\mathrm{bd}(h)\}}$*.*

Lemma 5.18. *For* $h \in \mathcal{CH}_{\mathrm{BA}}$ *we have that the cardinality of* $\Gamma(h)$ *is bounded above by* $2 \cdot \mathrm{sz}(h)$*.*

6 Searching for Truth

As explained in the introduction, the definition of search problems based on proof notations has to deal with properties whose computational complexity is too complicated to decide them directly. Therefore, instead of deciding them, we will replace them by some canonical search problem which determines their truth. This section will provide the definition and basic properties for such canonical search problems. In the next subsection we will present some general notation for tuples and sequences which will also be useful in later sections when we discuss the Skolemisation of prenex formulas that arise from search problems. The subsequent subsection then introduces canonical search problems for properties in $\mathrm{s}\Pi^{\mathrm{b}}_k$.

6.1 Notations for Tuples and Sequences

In order to have succinct notations for prenex formulas and for our discussion of Skolemisation, we introduce formal tuples, and in particular tuples of variables and quantifiers, and tuple quantification for tuples of variables. These tuples are formed and used on the meta level, they are not available in $\mathcal{L}_{\mathrm{BA}}$.

At the end of the section we will also introduce sequence coding which will be available within $\mathcal{L}_{\mathrm{BA}}$. Sequences will be used to define various functions and relations related to search problems.

Definition 6.1 (General Tuples)**.** A *tuple of length k* is an expression of the form $[t_1, \dots, t_k]$ with t_i some formal expression. We will use the letter $\mathfrak{t}$ as a meta-variable for general tuples. We will use subscripts of the form $\mathfrak{t}_i$ only to denote the i-th element t_i of $\mathfrak{t}$. Let $[t_1, \dots, t_k]\lceil_\ell$ denote $[t_1, \dots, t_{\min(k,\ell)}]$.

Definition 6.2 (Tuples of Variables)**.** A *tuple of variables of length k* is an expression of the form $[z_1, \dots, z_k]$ with z_i being a formal variable in $\mathcal{L}_{\mathrm{BA}}$. We will use the letter $\mathfrak{z}$ (possibly with superscripts) as a meta-variable for tuples of variables. $\mathfrak{z}_i$ and $\mathfrak{z}\lceil_\ell$ are defined as for general tuples.

Definition 6.3 (Tuples of Quantifiers)**.** A *tuple of quantifiers of length k* is an expression of the form $[Q_1, \dots, Q_k]$ with $Q_i \in \{\exists, \forall\}$. We will use the letter $\mathfrak{Q}$ (possibly with super-scripts) as a meta-variable for tuples of quantifiers.

Let $\mathfrak{Q} = [Q_1, \dots, Q_k]$ be a tuple of quantifiers of length k. The expression $\neg\mathfrak{Q}$ denotes the tuple $[\neg Q_1, \dots, \neg Q_k]$ where $\neg\forall$ denotes $\exists$, and $\neg\exists$ denotes

$\forall$. The expression $\forall^k$ denotes the tuple $[\forall, \ldots, \forall]$ of length k. The expression $\forall\exists^k$ denotes the tuple $[\forall, \exists, \forall, \exists, \ldots]$ of length k. The expression $\exists\forall^k$ denotes the tuple $\neg\forall\exists^k$.

Definition 6.4 (Tuple Quantification)**.** Let $\mathfrak{Q} = [Q_1, \ldots, Q_k]$ be a tuple of quantifiers of length k, and $\mathfrak{z} = [z_1, \ldots, z_k]$ a tuple of variables of length k. The expression $(\mathfrak{Q}\mathfrak{z})\beta$ denotes the formula

$$(Q_1 z_1)(Q_2 z_2) \cdots (Q_k z_k)\beta \ .$$

We now fix a coding of sequences of numbers of fixed length. As the length of sequences will always be fixed on the meta-level, we can choose a sequence coding based on a feasible pairing function. In principle we could define a concrete pairing function which does not use the #-function, but the mere existence will suffice for our investigations. This definition of sequence coding may however play a role in investigations of fragments of bounded arithmetic which do not include the #-function, but we do not pursue these here.

Let us remind that a feasible pairing function $a, b \mapsto \mathrm{pair}(a, b)$ with projection functions $c \mapsto (c)_1$ and $c \mapsto (c)_2$ are fixed in $\mathcal{L}_{\mathrm{BA}}$ which satisfy $(\mathrm{pair}(a, b))_1 = a$ and $(\mathrm{pair}(a, b))_2 = b$ and some natural bounding conditions like $(c)_i \leq c$ and $a, b \leq t \ \rightarrow \ \mathrm{pair}(a, b) \leq B(t)$ for some $\mathcal{L}_{\mathrm{BA}}$-term B.

Definition 6.5 (Sequence Coding)**.** We use pairing to define sequences of fixed length by letting $\langle\,\rangle = 0$, and $\langle a_1, \ldots, a_{k+1}\rangle = \mathrm{pair}(a_1, \langle a_2, \ldots, a_{k+1}\rangle)$ with corresponding projections p_i. The projection function p_i picks out the i-th element of a sequence; that is, $\mathrm{p}_i(\langle a_1, \ldots, a_k\rangle) = a_i$.

We use $\mathfrak{s}$ (possibly with superscripts) as meta-variables to denote sequences. For sequences denoted by $\mathfrak{s}$, we often write $\mathfrak{s}_i$ to denote the i-th element, $\mathrm{p}_i(\mathfrak{s})$, of $\mathfrak{s}$. We also use well-known list notation for sequences. The empty sequence of length 0 is denoted by $\langle\,\rangle$. If $\mathfrak{s}$ is a sequence of length l, then $\langle a \,|\, \mathfrak{s}\rangle$ denotes the sequence of length $l+1$ given by $\langle a \,|\, \mathfrak{s}\rangle = \mathrm{pair}(a, \mathfrak{s})$. We also use expressions of the form $\langle a, b, c \,|\, \mathfrak{s}\rangle \ = \ \langle a \,|\, \langle b \,|\, \langle c \,|\, \mathfrak{s}\rangle\rangle\rangle$, and $\langle a, b, c\rangle = \langle a, b, c \,|\, \langle\,\rangle\rangle$, etc.

We also define the application of the projection function p_i to formal tuples $\mathfrak{t} = [t_1, \ldots, t_k]$ to denote the application of p_i to each of the elements of $\mathfrak{t}$, that is, $\mathrm{p}_i(\mathfrak{t}) = [\mathrm{p}_i(t_1), \ldots, \mathrm{p}_i(t_k)]$.

6.2 Canonical Search Problems for Properties in $\mathrm{s}\Pi^{\mathrm{b}}_k$

In this subsection we define a canonical search problem for each formula in $\mathrm{s}\Sigma^{\mathrm{b}}_\infty$. The canonical search problem will be used to determine the truth of the formula. To define the search space for a formula φ, we need an upper bound to all values which may occur as quantified values in the evaluation of φ. The next definition provides the necessary requirements which we will need for such upper bounds.

Definition 6.6 (Strict Upper Bounds)**.** Let φ be of the form $(\mathfrak{Q}\mathfrak{z})\beta$ for some quantifier-free β, $\mathfrak{Q} = [Q_1, \ldots, Q_k]$ and $\mathfrak{z} = [z_1, \ldots, z_k]$. An $\mathcal{L}_{\mathrm{BA}}$-term D is called a *strict upper bound (s.u.b.) for* φ if its free variables are amongst those of φ, and if it satisfies the following properties: Let $\mathfrak{Q}^i := [Q_{i+1}, \ldots, Q_k]$ and $\mathfrak{z}^i := [z_{i+1}, \ldots, z_k]$. For all $1 \le i \le k$ with $Q_i = \forall$,

$$\mathrm{S}^1_2 \vdash (\forall z_1) \cdots (\forall z_{i-1}) \Big((\forall z_i < D)(\mathfrak{Q}^i \mathfrak{z}^i)\beta \;\rightarrow\; (\forall z_i)(\mathfrak{Q}^i \mathfrak{z}^i)\beta \Big) \ ,$$

and for all i with $Q_i = \exists$,

$$\mathrm{S}^1_2 \vdash (\forall z_1) \cdots (\forall z_{i-1}) \Big((\exists z_i)(\mathfrak{Q}^i \mathfrak{z}^i)\beta \;\rightarrow\; (\exists z_i < D)(\mathfrak{Q}^i \mathfrak{z}^i)\beta \Big) \ .$$

Definition 6.7. For $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_{\infty}$ we can define *the canonical s.u.b. D_φ for φ* inductively as follows:

- If φ is quantifier free, then let $D_\varphi := 0$.
- If φ is of the form $(\forall x \le t)\psi$ or $(\exists x \le t)\psi$, then let D_φ be the term $\max\{\mathrm{bd}(t) + 1, D_\psi(x/\,\mathrm{bd}(t))\}$.

We observe that D_φ represents a monotone function in its variables. Thus, D_φ is a s.u.b. in the sense of Definition 6.6, which can be shown immediately by induction on the complexity of φ.

Notation 6.8. Let 0^k denote the sequence of length k consisting only of zeros.

Let φ be a formula in $\mathrm{s}\Sigma^{\mathrm{b}}_{\infty}$ and $\vec{a}$ a list of variables such that $\mathrm{FV}(\varphi) \subseteq \{\vec{a}\}$. Let $D = D(\vec{a})$ be a s.u.b. for φ. We define the *canonical search problem* S^D_φ for φ whose aim is to determine the truth value for φ. S^D_φ is defined similar to a Π^{b}_k-PLS problem with Π^{b}_ℓ-goal from Definition 3.2, but instead of a goal set, S^D_φ has an *answer set* A^D_φ of low computational complexity which determines the truth of φ: For a solution $\mathfrak{s}$ to the search problem, φ is true iff $\mathfrak{s} \in A_\varphi$. The answer set will later be used to define the neighbourhood function for Π^{b}_k-PLS problems, which have to be of low complexity. The idea to determine the truth of φ of, say, the form $(\exists x < D)\psi(x)$ is to successively "search" for the truth of $\psi(0)$, $\psi(1)$,..., $\psi(D{-}1)$. If any of these intermediate searches are successful, the overall search will be successful and will yield a value d (usually the first such) for which $\psi(d)$ produces success; otherwise the overall search will yield a value D indicating that none of the intermediate searches were successful.

We start by defining the configuration space and cost function which only depend on rank of formulas and not on their actual form.

Definition 6.9 (Configuration Space)**.** Let $k \ge 0$ and $D \ge 1$. The *configuration space* $C^{k,D}$ is the set of all sequences of length k of elements $\le D$, i.e. $\{\langle u_1, \ldots, u_k\rangle : u_1, \ldots, u_k \leq D\}$. The *cost function* c^D can be defined on all sequences as

$$c^D(\langle u_k, \ldots, u_1\rangle) := \sum_{i=1}^{k}(D \dot{-} u_i)(D+1)^{(i-1)}$$

It has the properties that $0 \leq c^D(\mathfrak{s}) < (D+1)^k$ for all $\mathfrak{s} \in C^{k,D}$, and that $c^D(\mathfrak{s}_1) > c^D(\mathfrak{s}_2)$ if $\mathfrak{s}_1$ is smaller than $\mathfrak{s}_2$ w.r.t. the lexicographical order on tuples on $C^{k,D}$.

Definition 6.10. The *canonical search problem S^D_φ of* φ, given by the system $(C^D_\varphi, F^D_\varphi, A^D_\varphi, N^D_\varphi, c^D_\varphi)$, consists of a *configuration space* C^D_φ, a *set of feasible solutions* F^D_φ which is a subset of the configuration space, an *answer set* A^D_φ which is a subset of the configuration space, a *neighbourhood function* N^D_φ which maps configurations to configurations, and a *cost function* c^D_φ defined for configurations. The goal of the search problem is to find some $\mathfrak{s} \in F^D_\varphi$ with $N^D_\varphi(\mathfrak{s}) = \mathfrak{s}$.

The defined sets and functions all implicitly depend on the parameters $\vec{a}$ of φ. We will usually not mention D as it is understood from the context.

The configuration space C^D_φ is $C^{\mathrm{rk}(\varphi),D}$ from the previous definition, and the cost function c^D_φ is the cost function c^D from the previous definition with domain restricted to C^D_φ.

The set of feasible solutions F_φ, the neighbourhood function N_φ and the answer set A_φ also implicitly include parameter variables $\vec{a}$. They are defined by induction on the complexity of φ.

If φ is in $\mathrm{s}\Sigma^{\mathrm{b}}_0 \cup \mathrm{s}\Pi^{\mathrm{b}}_0$ we define

$$\begin{aligned} F_\varphi &:= \{\langle\,\rangle\} \\ N_\varphi(\langle\,\rangle) &:= \langle\,\rangle \\ \langle\,\rangle \in A_\varphi &:\Leftrightarrow \varphi \end{aligned}$$

Let φ be in $\mathrm{s}\Sigma^{\mathrm{b}}_{k+1} \setminus \mathrm{s}\Pi^{\mathrm{b}}_{k+1}$ of the form $(\exists x)\psi$. ψ has (potentially) one free variable in addition to φ which is x. Thus, when defining F, N and A in the following, their first argument will denote the value for this additional parameter. We will make this dependency explicit by writing ψx in the index of F, N, A, resp. We define

$$F_\varphi := \{\langle d \,|\, \mathfrak{s}\rangle \in C_\varphi \colon \mathfrak{s} \in F_{\psi x}(d) \ \wedge\ (\forall x < d)\neg\psi(x)\}$$

$$N_\varphi(\langle d \,|\, \mathfrak{s}\rangle) := \begin{cases} \langle d \,|\, N_{\psi x}(d, \mathfrak{s})\rangle & \text{if } d < D \ \wedge\ N_{\psi x}(d,\mathfrak{s}) \neq \mathfrak{s} \\ \langle d \,|\, \mathfrak{s}\rangle & \text{if } d < D \ \wedge\ N_{\psi x}(d,\mathfrak{s}) = \mathfrak{s} \in A_{\psi x}(d) \\ \left\langle d+1 \,|\, 0^k\right\rangle & \text{if } d < D \ \wedge\ N_{\psi x}(d,\mathfrak{s}) = \mathfrak{s} \notin A_{\psi x}(d) \\ \langle d \,|\, \mathfrak{s}\rangle & \text{if } d = D \end{cases}$$

$$\langle d \,|\, \mathfrak{s}\rangle \in A_\varphi \Leftrightarrow d < D$$

For $\varphi \in \mathrm{s}\Pi^{\mathrm{b}}_{k+1} \setminus \mathrm{s}\Sigma^{\mathrm{b}}_{k+1}$ we define

$$\begin{aligned} F_\varphi &:= F_{\neg\varphi} \\ N_\varphi(\mathfrak{s}) &:= N_{\neg\varphi}(\mathfrak{s}) \\ A_\varphi &:= C_\varphi \setminus A_{\neg\varphi} \end{aligned}$$

The latter choices imply for φ of the form $(\forall x)\psi$ that

$$\begin{aligned} F_\varphi &:= \{\langle d \,|\, \mathfrak{s}\rangle \in C_\varphi \colon \mathfrak{s} \in F_{\psi x}(d) \ \wedge\ (\forall x < d)\psi(x)\} \\ N_\varphi(\langle d \,|\, \mathfrak{s}\rangle) &:= \begin{cases} \langle d \,|\, N_{\psi x}(d, \mathfrak{s})\rangle & \text{if } d < D \ \wedge\ N_{\psi x}(d, \mathfrak{s}) \neq \mathfrak{s} \\ \langle d \,|\, \mathfrak{s}\rangle & \text{if } d < D \ \wedge\ N_{\psi x}(d, \mathfrak{s}) = \mathfrak{s} \notin A_{\psi x}(d) \\ \left\langle d+1 \,|\, 0^k \right\rangle & \text{if } d < D \ \wedge\ N_{\psi x}(d, \mathfrak{s}) = \mathfrak{s} \in A_{\psi x}(d) \\ \langle d \,|\, \mathfrak{s}\rangle & \text{if } d = D \end{cases} \\ \langle d \,|\, \mathfrak{s}\rangle \in A_\varphi &\Leftrightarrow d = D \qquad \text{assuming } \mathfrak{s} \in C_\psi \end{aligned}$$

Definition 6.11. Let $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_\infty$, and let $S^D_\varphi = (C_\varphi, F_\varphi, A_\varphi, N_\varphi, c_\varphi)$ be the canonical search problem for φ. Let k be the rank of φ. We extend the definition of F_φ, A_φ and N_φ to sequences of length $\ell > k$ in the obvious way:

$$\begin{aligned} \langle u_1, \ldots, u_\ell\rangle \in F_\varphi \quad &:\Longleftrightarrow \quad \langle u_1, \ldots, u_k\rangle \in F_\varphi \\ \langle u_1, \ldots, u_\ell\rangle \in A_\varphi \quad &:\Longleftrightarrow \quad \langle u_1, \ldots, u_k\rangle \in A_\varphi \end{aligned}$$

and if $N_\varphi(\langle u_1, \ldots, u_k\rangle) = \langle v_1, \ldots, v_k\rangle$ then

$$N_\varphi(\langle u_1, \ldots, u_\ell\rangle) \quad := \quad \langle v_1, \ldots, v_k, u_{k+1}, \ldots, u_\ell\rangle \ .$$

To explain the previous two definitions let us calculate F_φ for φ of rank $k > 0$: For $k = 1$ and $\varphi \equiv (\exists x)\beta(x)$ we have $\langle u \,|\, \mathfrak{s}\rangle \in F_\varphi \equiv (\forall x{<}u)\neg\beta(x)$. If $k = 2$ and $\varphi \equiv (\exists x)(\forall y)\beta(x, y)$ then $\langle u, v \,|\, \mathfrak{s}\rangle \in F_\varphi$ has the form

$$(\forall x{<}u)(\exists y)\neg\beta(x, y) \ \wedge\ (\forall y{<}v)\beta(u, y) \ .$$

If $k = 3$ and $\varphi \equiv (\exists x)(\forall y)(\exists z)\beta(x, y, z)$ we have that $\langle u, v, w \,|\, \mathfrak{s}\rangle \in F_\varphi$ is of the form

$$(\forall x{<}u)(\exists y)(\forall z)\neg\beta(x, y, z) \ \wedge\ (\forall y{<}v)(\exists z)\beta(u, y, z) \ \wedge\ (\forall z{<}w)\neg\beta(u, v, z) \ .$$

For the general case assume $\varphi \equiv (\exists x)(\forall y)\psi(x, y)$. Then $\langle u, v \,|\, \mathfrak{s}\rangle \in F_\varphi$ has the form

$$(\forall x{<}u)(\exists y)\neg\psi(x, y) \ \wedge\ (\forall y{<}v)\psi(u, y) \ \wedge\ \mathfrak{s} \in F_{\psi xy}(u, v)$$

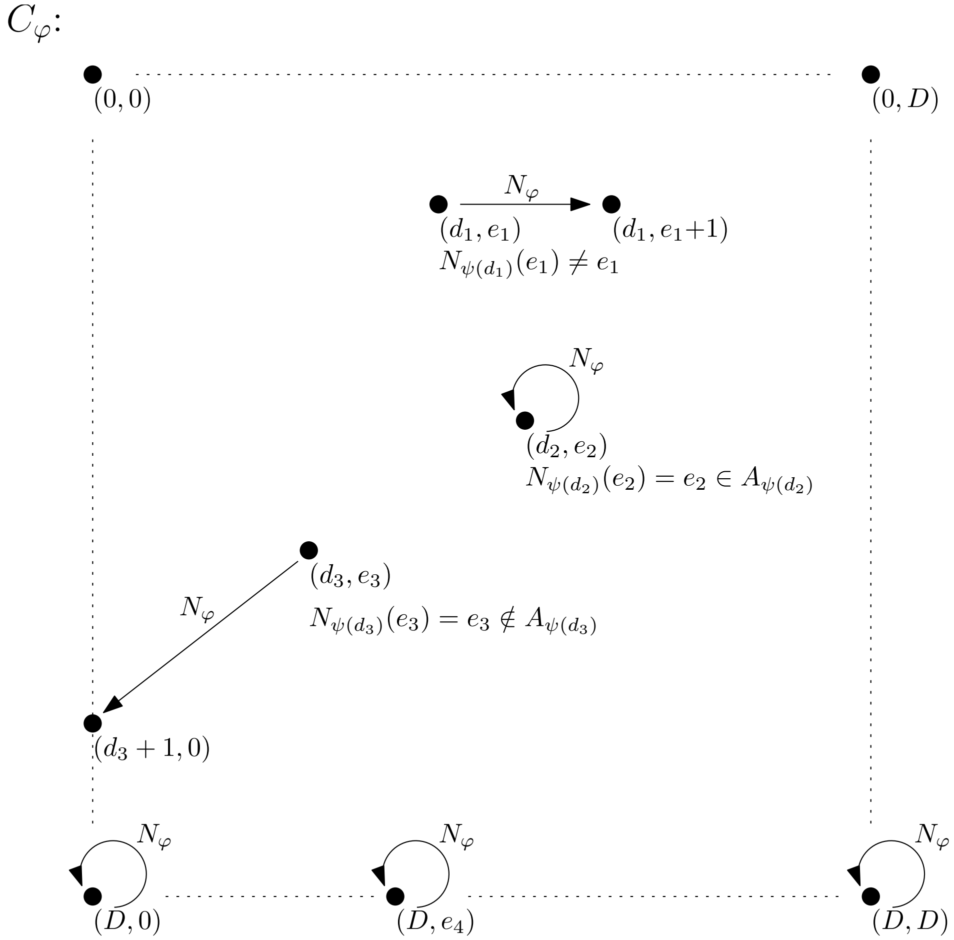

Figure 1: The canonical search problem $S_\varphi = (C_\varphi, F_\varphi, A_\varphi, N_\varphi, c_\varphi)$ for φ in $\mathrm{s}\Sigma^{\mathrm{b}}_2 \setminus \mathrm{s}\Pi^{\mathrm{b}}_2$ of the form $(\exists x)\psi(x)$, and D a strict upper bound for φ. The configuration space C_φ is a grid consisting of all points $\langle d,e\rangle$ with $0 \leq d \leq D$ and $0 \leq e \leq D$. N_φ is defined for all points on the grid. Its behaviour at $\langle d,e\rangle$ depends on the behaviour of the canonical search problem for $S_{\psi x}(d) = S_{\psi(d)}$, in particular on $N_{\psi x}(d,e) = N_{\psi(d)}(e)$ and $A_{\psi x}(d) = A_{\psi(d)}$.

Observation 6.12. *Let $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_{\infty}$, and let k be the rank of φ according to Definition 2.6. Let $S_\varphi = (C_\varphi, F_\varphi, A_\varphi, N_\varphi, c_\varphi)$ be the canonical search problem for φ. Then, $C_\varphi, A_\varphi, N_\varphi$ and c_φ are polynomial time computable, and F_φ is in the level Π^{p}_k of the polynomial time hierarchy. More precisely, we observe that $\mathfrak{s} \in C_\varphi(a)$, $\mathfrak{s} \in A_\varphi(a)$ and $N_\varphi(a, \mathfrak{s}) = \mathfrak{s}'$ can be defined by $\mathrm{s}\Sigma^{\mathrm{b}}_0$-formulas, $c_\varphi(a, \mathfrak{s})$ can be defined by $\mathcal{L}_{\mathrm{BA}}$-terms, and $\mathfrak{s} \in F_\varphi(a)$ is equivalent to a $\mathrm{s}\Pi^{\mathrm{b}}_k$-formula in $\overline{\mathrm{BASIC}}$.*

Proposition 6.13. *Let $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_{\infty} \setminus \mathrm{s}\Sigma^{\mathrm{b}}_1 \cup \mathrm{s}\Pi^{\mathrm{b}}_1$, D an s.u.b. for φ, and let $S^D_\varphi = (C^D_\varphi, F^D_\varphi, A^D_\varphi, N^D_\varphi, c^D_\varphi)$ be the canonical search problem for φ. The following is provable in $\overline{\mathrm{BASIC}}$. Assume $N^D_\varphi(\mathfrak{s}) = \mathfrak{s}$, then either $\mathfrak{s}_1 = D$, or $\mathfrak{s}_1 < D$ and $\mathfrak{s}_2 = D$.*

Proof. It is enough to consider φ of the form $(\exists x)(\forall y)\psi(x, y)$, as $N^D_{\neg\varphi}(\mathfrak{s}) = N^D_\varphi(\mathfrak{s})$. Let $\mathfrak{s} = \langle d, e \,|\, \mathfrak{s}' \rangle$ and assume $N^D_\varphi(\mathfrak{s}) = \mathfrak{s}$ and $d \neq D$, then we have to show $d < D$ and $e = D$. The definition of N^D_φ implies $d < D$ and $\langle e \,|\, \mathfrak{s}' \rangle \in A^D_{(\forall y)\psi(x,y)}(d)$. By definition of $A^D_{(\forall y)\psi(d,y)}$ the latter shows $e = D$. □

Corollary 6.14. *Let $S^D_\varphi = (C^D_\varphi, F^D_\varphi, A^D_\varphi, N^D_\varphi, c^D_\varphi)$ be the canonical search problem for a formula $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_{\infty}$, and D an s.u.b. for φ. Then, the following are provable in $\overline{\mathrm{BASIC}}$:*

1. *If $\mathrm{rk}(\varphi) \geq 2$, $N_\varphi(\mathfrak{s}) = \mathfrak{s}$, and either $\mathrm{tp}(\varphi) = \bigvee$ and $\mathfrak{s} \in A_\varphi$, or $\mathrm{tp}(\varphi) = \bigwedge$ and $\mathfrak{s} \notin A_\varphi$, then $\mathfrak{s}_2 = D$.*
2. *If $\mathrm{rk}(\varphi) \geq 1$, $N_\varphi(\mathfrak{s}) = \mathfrak{s}$, and either $\mathrm{tp}(\varphi) = \bigvee$ and $\mathfrak{s} \notin A_\varphi$, or $\mathrm{tp}(\varphi) = \bigwedge$ and $\mathfrak{s} \in A_\varphi$, then $\mathfrak{s}_1 = D$.*

Proof. For both 1. and 2., it is enough to consider the case $\mathrm{tp}(\varphi) = \bigvee$ as the "either. . . or" cases are equivalent due to the definition of A_φ. For 1. we observe that the definition of $\mathfrak{s} \in A_\varphi$ implies $\mathfrak{s}_1 < D$. Thus, $\mathfrak{s}_2 = D$ by the previous Proposition. In case 2. the definition of $\mathfrak{s} \notin A_\varphi$ implies $\mathfrak{s}_1 \not< D$, hence $\mathfrak{s}_1 = D$. □

The next proposition validates that canonical search problems correctly determine truth.

Proposition 6.15. *Let $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_{\infty}$, and let $S_\varphi = (C_\varphi, F_\varphi, A_\varphi, N_\varphi, c_\varphi)$ be the canonical search problem for φ. The following is provable in S^1_2:*

$$N_\varphi(\mathfrak{s}) = \mathfrak{s} \wedge \mathfrak{s} \in F_\varphi \quad \Rightarrow \quad (\varphi \quad \Leftrightarrow \quad \mathfrak{s} \in A_\varphi)$$

Proof. The proof is by induction on the rank of φ. It is enough to consider φ of the form $(\exists x)\psi(x)$, because the assertion is trivial for φ of rank 0, and for φ of the form $(\forall x)\psi(x)$ we can use $N_\varphi = N_{\neg\varphi}$, $F_\varphi = F_{\neg\varphi}$, and $A_\varphi = C_\varphi \setminus A_{\neg\varphi}$.

We argue in S^1_2. Let $\mathfrak{s} = \langle d \,|\, \mathfrak{s}' \rangle$ and assume $N_\varphi(\mathfrak{s}) = \mathfrak{s} \in F_\varphi$. Assume first $d < D$, hence $\mathfrak{s} \in A_\varphi$. We will show $\psi(d)$, which implies φ. By definition of N_φ we have $N_{\psi x}(d, \mathfrak{s}') = \mathfrak{s}'$ and $\mathfrak{s}' \in A_{\psi x}(d)$. The definition of F_φ shows $\mathfrak{s}' \in F_{\psi x}(d)$. If $\mathrm{rk}(\varphi) = 1$ we have $\mathfrak{s}' = \langle\,\rangle$. Thus, $\mathfrak{s}' \in A_{\psi x}(d)$ implies $\langle\,\rangle \in A_{\psi(d)}$, hence $\psi(d)$. For $\mathrm{rk}(\varphi) > 1$ we obtain by induction hypothesis $\psi(d)$ iff $\mathfrak{s}'_1 = D$. As $\mathfrak{s}_1 = d < D$, Proposition 6.13 shows $\mathfrak{s}'_1 = \mathfrak{s}_2 = D$. Hence $\psi(d)$.

Now assume $d = D$, hence $\mathfrak{s} \notin A_\varphi$. We have $(\forall x < D)\neg\psi(x)$ by definition of F_φ. As D is s.u.b. for φ, the latter shows $(\forall x)\neg\psi(x)$ (this is the only place where we need S^1_2). Hence $\neg\varphi$. □

The final proposition states that canonical search problems have the properties of search problems.

Proposition 6.16. *Let $S_\varphi = (C_\varphi, F_\varphi, A_\varphi, N_\varphi, c_\varphi)$ be the canonical search problem for a formula $\varphi \in \mathrm{s}\Sigma^{\mathrm{b}}_\infty$ of rank k. The following can be proven in S^1_2.*

1. *$0^k \in F_\varphi$.*

2. *If $\mathfrak{s} \in F_\varphi$, then $N_\varphi(\mathfrak{s}) \in F_\varphi$*

3. *If $N_\varphi(\mathfrak{s}) = \mathfrak{s}'$ and $\mathfrak{s} \neq \mathfrak{s}'$, then $c_\varphi(\mathfrak{s}') < c_\varphi(\mathfrak{s})$.*

Proof. The first and third assertion follow immediately from the definitions, and can be proven already in $\overline{\mathrm{BASIC}}$. The proof of the second assertion is by induction on the rank of φ. The non-trivial cases are that φ is of the form $(\exists x)\psi(x)$, and that $\mathfrak{s} = \langle d \,|\, \mathfrak{s}' \rangle$ and $N_\varphi(\mathfrak{s}) \neq \mathfrak{s}$. If $N_\varphi(\mathfrak{s}) = \langle d \,|\, N_{\psi x}(d, \mathfrak{s}') \rangle$ the assertion follows immediately from induction hypothesis. In case $N_\varphi(\mathfrak{s}) = \big\langle d+1 \,|\, 0^k \big\rangle$ the assertion follows using Proposition 6.15 to ensure $(\forall x{<}d{+}1)\psi(x)$. □

7 Search problems defined by proof notations

We are now ready to put things together: We first define a general local search problem based on proof notations which will be used in Subsection 7.2 to provide the characterisation of $\Sigma^{\mathrm{b}}_{\ell+1}$-definable search problems in T^{k+1}_2 in terms of Π^{b}_k-PLS problems with Σ^{b}_ℓ-goals.

7.1 Parameterised Local Search Problems based on Proof Notations

Let us start by describing the idea for computing witnesses using proof trees. Assume we have a T^{k+1}_2-proof of a formula $(\exists y)\varphi(y)$ in $\Sigma^{\mathrm{b}}_{\ell+1}$ and we want to compute an n such that $\varphi(n)$ is true — in case we are interested in definable search problems, such a situation is obtained from a proof of $(\forall x)(\exists y)\varphi(x, y)$

by inverting the universal quantifier to some $a \in \mathbb{N}$. Assume further, we have applied some proof theoretical transformations to obtain a BA^∞ derivation d_0 of $(\exists y)\varphi(y)$ with $\mathrm{s}\Sigma^{\mathrm{b}}_0$-$\mathrm{crk}(d_0) \leq k$. Then we can define a path through d_0, represented by sub-derivations $d_1, d_2, d_3 \ldots$, such that

- $d_{j+1} = d_j(\iota)$ for some $\iota \in |\operatorname{last}(d_j)|$
- $\Gamma(d_j) = (\exists y)\varphi(y), \Gamma_j$ where all formulae $A \in \Gamma_j$ are false and in $\mathrm{s}\Sigma^{\mathrm{b}}_k \cup \mathrm{s}\Pi^{\mathrm{b}}_k$.

Such a path must be finite as $\operatorname{hgt}(d_j)$ is strictly decreasing. Say it ends with some d_ℓ. In this situation we must have that $\operatorname{last}(d_\ell) = \bigvee^k_{(\exists y)\varphi(y)}$ and that $\varphi(k)$ is true. Hence we found our witness.

The path which we have just described can be viewed as the canonical path through a related local search problem. Before explaining this, let us fix the notion of a local search problem.

Definition 7.1. *An instance of a local search problem* consists of a set F of possible solutions, a goal set G which is a subset of F, an initial value $d \in F$, a cost function $c\colon F \to \mathbb{N}$, and a neighbourhood function $N\colon F \to F$ which satisfy that $c(N(d)) < c(d)$ if $N(d) \neq d$, and that $d \in G$ iff $d \in F$ and $N(d) = d$. A solution to a local search problem, called a *local optimum*, is any $d \in G$.

Observe that the ingredients of a local search problem guarantee the existence of a local optimum, by starting with the initial value and iterating the neighbourhood function (this defines the *canonical path through the search problem.*)

Now we define a local search problem whose canonical path is the one described above. The set F of possible solutions is defined as the set of all BA^∞-derivations d which have the properties that $\mathrm{s}\Sigma^{\mathrm{b}}_0$-$\mathrm{crk}(d_0) \leq k$, and that all formulae $A \in \Gamma(d) \setminus \{(\exists y)\varphi(y)\}$ are false and in $\mathrm{s}\Sigma^{\mathrm{b}}_k \cup \mathrm{s}\Pi^{\mathrm{b}}_k$. The cost of a possible solution $d \in F$ is given by the height $\operatorname{hgt}(d)$ of the proof tree d. We have already fixed some initial value $d_0 \in F$. The neighbourhood function $N\colon \mathrm{BA}^\infty \to \mathrm{BA}^\infty$ is defined by case distinction on the shape of $\operatorname{last}(d)$ for $d \in F$:

- $\operatorname{last}(d) = \mathrm{Ax}_A$ cannot occur as all atomic formulae in $\Gamma(d)$ are false by definition of F.
- $\operatorname{last}(d) = \bigwedge_{A_0 \,\wedge\, A_1}$, then $A_0 \;\wedge\; A_1$ must be false, hence some of A_0, A_1 must be false. Let $N(d) := d(0)$ if A_0 is false, and $d(1)$ otherwise.
- $\operatorname{last}(d) = \bigvee^k_{A_0 \,\vee\, A_1}$, then $A_0 \;\vee\; A_1$ must be false, hence both A_0, A_1 must be false. Let $N(d) := d(0)$.
- $\operatorname{last}(d) = \bigwedge_{(\forall x)A(x)}$. As $(\forall x)A(x)$ is false there is some i such that $A(i)$ is false. Let $N(d) := d(i)$.

- $\mathrm{last}(d) = \bigvee^{k}_{(\exists x)A(x)}$. If $(\exists x)A(x)$ is different from $(\exists y)\varphi(y)$ then $(\exists x)A(x)$ must be false; let $N(d) := d(0)$. Otherwise, if $\varphi(k)$ is false let $N(d) = d(0)$, and if it is true let $N(d) = d$. Observe that in the very last case we found our witness.

- $\mathrm{last}(d) = \mathrm{Cut}_C$. If C is false let $N(d) := d(0)$, otherwise let $N(d) := d(1)$.

Obviously, this defines a local search problem according to Definition 7.1. As remarked above, a local optimal solution to the search problem allows us to determine a witness.

The previous description covers the main idea for defining search problem via proof notations. It is not exactly the version we are looking for, as we want to have neighbourhood functions which are polynomial time computable, but the one that we describe above has to decide $\mathrm{s}\Sigma^{\mathrm{b}}_{k-1}$-formulas (in case of a cut) and maintain in some way the promise that the endsequent of elements in F consists of false formulas besides $(\exists y)\varphi(y)$. The adjustment we have to make is to incorporate the canonical search problems for deciding formulas from the previous section, instead of deciding them. We also have to store promised witnesses for false $\mathrm{s}\Pi^{\mathrm{b}}_{k}$ formulas in the endsequent of derivations, in order to obtain the optimal complexity for the set of feasible solutions, which is $\mathrm{s}\Pi^{\mathrm{b}}_{k}$. We do this by extending the set of possible solutions in the forthcoming Definition 7.3 to triples of the form $\langle d, f, \mathfrak{s}\rangle$, where d denotes a BA^{∞}-derivations as above, f stores witnesses of $\forall$ quantifiers, and $\mathfrak{s}$ is a position in a potential canonical search problems for deciding some formula related to the last inference of d.

In the next definition we fix some canonical choice function for the outermost quantifier of a sharply bounded formula. This is followed by the formal definition of parameterised local search problems, given as the adjustment of the local search problem described above.

Definition 7.2. Let ϵ denote the following choice function: For $\psi \in \mathrm{s}\Pi^{\mathrm{b}}_{0}$, let $\epsilon(\psi) = j$ for the smallest j such that $\psi[j]$ is false, and let $\epsilon(\psi) = 0$ if such a j cannot be found (including that $\psi \notin \mathrm{s}\Pi^{\mathrm{b}}_{0}$ and $\psi[j]$ is not defined etc).

Definition 7.3. We define a local search problem L which is parameterised by

- *complexity levels* ℓ, k with $0 \leq \ell \leq k$, denoting the formula classes $\mathrm{s}\Sigma^{\mathrm{b}}_{\ell}$ and $\mathrm{s}\Sigma^{\mathrm{b}}_{k}$,

- a $\mathrm{BA}^{\star}$-derivation $\bar{h}$ which is used to define an *initial value function* $h_{\bullet}\colon \mathbb{N} \to \mathcal{CH}_{\mathrm{BA}}$, mapping $a \mapsto h_a := \mathsf{E}\bar{h}(\underline{a}/x)$,

- a formula $(\exists y)\varphi(x, y) \in \mathrm{s}\Sigma^{\mathrm{b}}_{\ell+1}$,

such that S^1_2 proves, for $a \in \mathbb{N}$,

- $\Gamma(h_a) \subseteq \{(\exists y)\varphi(\underline{a}, y)\}$,
- $\mathrm{s}\Sigma^{\mathrm{b}}_0\text{-crk}(h_a) \leq k$,
- $\mathrm{o}(h_a) = 2^{|a|^{O(1)}}$,
- $\vartheta(h_a) = |a|^{O(1)}$.

We denote such a parametrisation by $L = \langle \ell, k, \bar{h}, (\exists y)\varphi(x, y)\rangle$.

An instance of L is given by $a \in \mathbb{N}$ which defines the following functions and relations of a local search problem:

- Let Φ be $\mathrm{deco}(\bar{h})$ together with the closure of $\mathrm{deco}(\bar{h}) \cap \Delta_0$ under negation and taking subformulas.
- $D_a := \mathrm{bd}(h_a) + 1$ defines a strict upper bound for all formulas in $\Phi_{\max(a,\mathrm{bd}(h_a))}$ in the sense of Definition 6.6.
- The (finite) set of *potential configurations* $\tilde{C}(a)$ consists of those pairs (h, f) of $h \in \mathcal{CH}_{\mathrm{BA}}$ and $f \colon A \to \{0, \ldots, D_a - 1\}$ for some finite subset A of $\mathcal{F}_{\mathrm{BA}}$, which satisfy:
  1. $\Gamma(h) \setminus \{(\exists y)\varphi(\underline{a}, y)\} \subset \mathrm{s}\Sigma^{\mathrm{b}}_k \cup \mathrm{s}\Pi^{\mathrm{b}}_k$,
  2. $\mathrm{dom}\, f$ consists of all $\psi \in \Gamma(h)$ with $\mathrm{tp}(\psi) = \bigwedge$ and $\psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0$,
  3. $\mathrm{s}\Sigma^{\mathrm{b}}_0\text{-crk}(h) \leq k$,
  4. $\mathrm{o}(h) \leq \mathrm{o}(h_a)$,
  5. $\mathrm{bd}(h) \leq \mathrm{bd}(h_a)$,
  6. $\vartheta(h) \leq \vartheta(h_a)$,
  7. $\mathrm{deco}(h) \subseteq \Phi_{\max(a,\mathrm{bd}(h_a))}$.
- The set of configurations is given by

$$C(a) \quad := \quad \{d \colon d < D_a\} \ \cup \ \left\{\langle h, f, \mathfrak{s}\rangle : (h, f) \in \tilde{C}(a) \text{ and } \mathfrak{s} \in C^{k,D_a}\right\} \ .$$

- The *initial value function* is given by $i(a) := \left\langle h_a, \emptyset, 0^k\right\rangle$.
- The *cost function* is defined as

$$c(a, \langle h, f, \mathfrak{s}\rangle) := \mathrm{o}(h) \cdot (D_a + 1)^k + c(\mathfrak{s})$$

  and

$$c(a, d) := 0$$

  for $d < D_a$.

- The *neighbourhood function* is defined by case distinction as follows: for $d < D_a$ let $N(a,d) := d$; for $\mathrm{tp}(h) = \mathrm{Ax}_\psi$ let $N(a, \langle h, f, \mathfrak{s}\rangle) := \langle h, f, \mathfrak{s}\rangle$; for $\mathrm{tp}(h) = \mathrm{Rep}$ let $N(a, \langle h, f, \mathfrak{s}\rangle) := \left\langle h[0], f^r, 0^k \right\rangle$, where f^r denotes the restriction of f to $\Gamma(h[0])$ — similar in future cases; for $\mathrm{tp}(h) = \bigwedge_\psi$ let

$$N(a, \langle h, f, \mathfrak{s}\rangle) := \begin{cases} \left\langle h[f(\psi)], f^r, 0^k \right\rangle & \text{if } \psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0, \\ \left\langle h[\epsilon(\psi)], f^r, 0^k \right\rangle & \text{if } \psi \in \mathrm{s}\Pi^{\mathrm{b}}_0 \ , \end{cases}$$

for $\mathrm{tp}(h) = \bigvee^i_\psi$ let $N(a, \langle h, f, \mathfrak{s}\rangle)$ be defined as

$$\begin{cases} \left\langle h[0], f^r, 0^k \right\rangle & \text{if } \psi \in \mathrm{s}\Sigma^{\mathrm{b}}_0, \\ \left\langle h, f, N_{\psi[i]}(\mathfrak{s}) \right\rangle & \text{if } \psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_0,\ N_{\psi[i]}(\mathfrak{s}) \neq \mathfrak{s}, \\ \left\langle h[0], f', 0^k \right\rangle & \text{if } \psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_0,\ N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s},\ \mathfrak{s} \notin A_{\psi[i]} \\ & \quad \text{and } f' = (f \cup \{\psi[i] \mapsto \mathfrak{s}_1\})^r \text{ if } \psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_1 \\ & \quad\ \ \text{or } f' = f^r \text{ if } \psi \in \mathrm{s}\Sigma^{\mathrm{b}}_1, \\ \langle h, f, \mathfrak{s}\rangle & \text{if } \psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_0,\ \psi \neq (\exists y)\varphi(\underline{a}, y), \\ & \quad N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s},\ \mathfrak{s} \in A_{\psi[i]}, \\ i & \text{if } \psi = (\exists y)\varphi(\underline{a}, y),\ N_{\varphi(\underline{a},\underline{i})}(\mathfrak{s}) = \mathfrak{s},\ \mathfrak{s} \in A_{\varphi(\underline{a},\underline{i})} \ , \end{cases}$$

for $\mathrm{tp}(h) = \mathrm{Cut}_\psi$ let $N(a, \langle h, f, \mathfrak{s}\rangle)$ be defined as

$$\begin{cases} \langle h, f, N_\psi(\mathfrak{s})\rangle & \text{if } N_\psi(\mathfrak{s}) \neq \mathfrak{s}, \\ \left\langle h[1], f^r, 0^k \right\rangle & \text{if } N_\psi(\mathfrak{s}) = \mathfrak{s},\ \mathfrak{s} \in A_\psi, \\ \left\langle h[0], f', 0^k \right\rangle & \text{if } N_\psi(\mathfrak{s}) = \mathfrak{s},\ \mathfrak{s} \notin A_\psi \\ & \quad \text{and } f' = (f \cup \{\psi \mapsto \mathfrak{s}_1\})^r \text{ if } \psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0 \\ & \quad\ \ \text{or } f' = f^r \text{ if } \psi \in \mathrm{s}\Pi^{\mathrm{b}}_0 \ . \end{cases}$$

- The set of *feasible solutions* $F(a)$ is given by those $\langle h, f, \mathfrak{s}\rangle$ which satisfy

  - $\langle h, f, \mathfrak{s}\rangle \in C(a)$ and $\mathrm{tp}(h) \neq \mathrm{Ax}_\psi$;
  - for all $\psi \in \Pi := \mathrm{dom}(f)$ we have that $\psi[f(\psi)]$ is false;
  - for $\psi \in \Sigma := \Gamma(h) \setminus (\{(\exists y)\varphi(\underline{a}, y)\} \cup \Pi)$ we have that ψ is false;
  - $\mathrm{tp}(h) = \mathrm{Cut}_\psi$ implies $\mathfrak{s} \in F_\psi$;
  - $\mathrm{tp}(h) = \bigvee^i_\psi$ implies $\mathfrak{s} \in F_{\psi[i]}$;

  together with those $d < D_a$ such that $\varphi(a,d)$ holds.

- The *goal set* $G(a) := \{d < D_a \colon \varphi(a,d)\} \subset F(a)$.

We will now argue that the relations and functions defined above define a Π^{b}_{k}-PLS problem with Π^{b}_{ℓ}-goal according to Definition 3.2. One of the main considerations for this is to see that the computational complexity of the involved relations and functions fall into the right classes, in particular, that the set of configurations and the neighbourhood function are polynomial time computable. This is not difficult to see once we understood how notations for derivations are coded: any $h \in \mathcal{CH}_{\mathrm{BA}}$ is a term of inference symbols, and each inference symbol is given by its decoration consisting of formulas and terms and numbers — the formulas and terms have to come from Φ, and the numbers are bounded by $\max(a, \mathrm{bd}(h_a))$. Thus, a natural feasible Gödel numbering of such terms, as defined in [Bus86], will give us a suitable set of codes on which all necessary functions are easy to compute, as they all are either performing syntactic checks according to inference symbols and their decoration, or evaluating (in the case of feasible solutions) formulas in Φ (which is a *finite* set) under a numerical substitution.

Proposition 7.4. *The local search problem L from Definition 7.3, parameterised by $\langle \Phi, \ell, k, h, (\exists y)\varphi(x,y)\rangle$, provides a Π^{b}_{k}-PLS problem with Π^{b}_{ℓ}-goal according to Definition 3.2.*

Proof. As shown in [AB09] the functions $a \mapsto i(a) = h_a$, $a \mapsto \mathrm{bd}(h_a)$, $a \mapsto \mathrm{o}(h_a)$, $a \mapsto \vartheta(h_a)$, and $a \mapsto \mathrm{deco}(h_a)$ are polynomial time computable. Furthermore, the relations $\mathcal{CH}_{\mathrm{BA}}$, $\mathrm{s}\Sigma^{\mathrm{b}}_{0}$-$\mathrm{crk}(h) \leq k$, $\mathrm{bd}(h) \leq m$ and $\mathrm{deco}(h) \subseteq \Phi_m$ are polynomial time computable, and once $\mathrm{bd}(h) \leq m$ is established we also can compute $\mathrm{o}(h) \leq m'$ and then $\mathrm{o}(h)$ in polynomial time. Hence $c \in \mathrm{FP}$. Also, the functions $\mathrm{tp}(h)$ and $h[i]$ are polynomial time computable on $\mathcal{CH}_{\mathrm{BA}}$. Using Observation 6.12, this shows that N is polynomial time computable, because the case distinction which defines N depends only on essentially finitely many N_ψ: Each such ψ is obtained from a formula in Φ (which is a finite set) by substituting constants for free variables.

To check that $F \in \Pi^{\mathrm{b}}_{k}$ we look at the critical cases — here we use, similar to the case above, that the definition of F depends essentially only on finitely many N_ψ. "$d \in F(a)$", for $d < D_a$, is a Π^{b}_{l}-property. The definition of "$(h, f, \mathfrak{s}) \in F(a)$" has three critical entries: Observe that $\Sigma \cup \Pi \subseteq \Gamma(h) \subseteq \mathrm{deco}(h) \subseteq \Phi_{\mathrm{bd}(h_a)}$, hence for $\psi \in \Pi$ the condition "$\psi[f(\psi)]$ is false" is a Π^{b}_{k-1}-property, and for $\psi \in \Sigma$ the condition "ψ is false" is a Π^{b}_{k}-property; the condition "$\mathfrak{s} \in F_\psi$" for ψ of rank $\leq k$ is Π^{b}_{k} according to Observation 6.12.

That "$s \in G(a)$" is in Π^{b}_{ℓ} is obvious by definition.

So it remains to show that the properties (3.1)-(3.5) of Definition 3.2 do hold. For (3.1), $(\forall x, s)(s \in F(x) \rightarrow |s| \leq d(|x|))$, we observe that if $(h, f) \in \tilde{C}(a)$, then h is a term built up from inference symbols, the length of the term, i.e. the number of inference symbols, is $\vartheta(h) \leq \vartheta(h_a) = |a|^{O(1)}$, and each occurring inference symbol is decorated with expressions from $\mathrm{deco}(h) \subseteq \Phi_{\max(a,\mathrm{bd}(h_a))}$ and $|\,\mathrm{bd}(h_a)| = |a|^{O(1)}$. Thus, the polynomial bound d can be found assuming a feasible Gödel numbering as in [Bus86]. Property (3.2), $(\forall x)(i(x) \in F(x))$, is obvious. The last one, (3.5),

$$(\forall x, s)(s \in G(x) \ \leftrightarrow \ (N(x,s) = s \ \wedge \ s \in F(x)))$$

also follows from the definition. For this, observe that for "$\leftarrow$" the premise of the implication $N(x,s) = s \ \wedge \ s \in F(x)$ implies that s cannot be of the form $\langle h, f, \mathfrak{s}\rangle$: Assume it is, then either $\mathrm{tp}(h) = \mathrm{Ax}_\psi$ which would imply $\psi \in \Gamma(h)$ and ψ true, or $\mathrm{tp}(h) = \bigvee^i_\psi$, $\psi \neq (\exists y)\varphi(\underline{a}, y)$, $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \in A_{\psi[i]}$, and $s \in F(x)$ implies $\mathfrak{s} \in F_{\psi[i]}$, thus Proposition 6.15 shows $\psi[i]$, hence ψ, is true; both times we get a contradiction to the fact implied by $s \in F(a)$ that all formulas in $\Gamma(h) \setminus \{(\exists y)\varphi(\underline{a}, y)\}$ are false.

Property (3.3)

$$(\forall x, s)(s \in F(x) \ \rightarrow \ N(x,s) \in F(x))$$

follows by case distinction according to the definition $N(x,s)$, using the corresponding properties for canonical search problems as shown in Proposition 6.16. For example, consider the case that $s = \langle h, f, \mathfrak{s}\rangle \in F(x)$ with $\mathrm{tp}(h) = \bigwedge_\psi$ and $\psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0$. Then $N(a,s) = \left\langle h[f(\psi)], f^r, 0^k \right\rangle$ and we have to show that $(h[f(\psi)], f^r) \in \tilde{C}(a)$. Let $j = f(\psi)$, then $h[j] \vdash_{\approx} \Gamma(h), \psi[j]$ thus obviously $\Gamma(h[j]) \subset \mathrm{s}\Sigma^{\mathrm{b}}_k \cup \mathrm{s}\Pi^{\mathrm{b}}_k$. As $\mathrm{tp}(\psi) = \bigwedge$ and $\psi \in \mathrm{s}\Sigma^{\mathrm{b}}_\infty$, it follows that $\mathrm{tp}(\psi[j]) \neq \bigwedge$, thus $\mathrm{dom}\, f^r$ satisfies the property under 2. We compute $\mathrm{s}\Sigma^{\mathrm{b}}_0\text{-}\mathrm{crk}(h[j]) \leq \mathrm{s}\Sigma^{\mathrm{b}}_0\text{-}\mathrm{crk}(h) \leq k$, $\mathrm{o}(h[j]) < \mathrm{o}(h) \leq \mathrm{o}(h_a)$, $\mathrm{bd}(h[j]) \leq \mathrm{bd}(h) \leq \mathrm{bd}(h_a)$ by Lemma 5.13, 1., $\vartheta(h[j]) \leq \vartheta(h) \leq \vartheta(h_a)$ by Theorem 4.16, and that $\mathrm{deco}(h) \subseteq \Phi_{\max(a, \mathrm{bd}(h_a))}$, $j = f(\psi) \leq \mathrm{bd}(h_a)$ and $\mathrm{bd}(h) \leq \mathrm{bd}(h_a)$ imply $\mathrm{deco}(h[j]) \subseteq (\Phi_{\max(a,\mathrm{bd}(h_a))})_{\max(\mathrm{bd}(h_a), \mathrm{bd}(h))} = \Phi_{\max(a,\mathrm{bd}(h_a))}$ by Lemma 5.17, 4.

Other interesting cases occur when $s = \langle h, f, \mathfrak{s}\rangle \in F(x)$ with $\mathrm{tp}(h) = \bigvee^i_\psi$, $\psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_0$ and $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$. If $\mathfrak{s} \notin A_{\psi[i]}$ and $\psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_1$, then $N(a,s) = \left\langle h[0], f', 0^k \right\rangle$ and $f' = (f \cup \{\psi[i] \mapsto \mathfrak{s}_1\})^r$. The condition $\langle h[0], f'\rangle \in \tilde{C}(a)$ can be shown as before. If $\psi[i] \in \mathrm{dom}(f')$ we also have to show that $\psi[i][\mathfrak{s}_1]$ is false. $\mathfrak{s}$ can be written as $\langle d \,|\, \mathfrak{s}'\rangle$ because $\mathrm{rk}(\psi) \geq 2$. As $s \in F(x)$ we have $\mathfrak{s} \in F_{\psi[i]}$ by definition of $F(x)$, which implies $\mathfrak{s}' \in F_{\psi[i][d]}$ by definition of $F_{\psi[i]}$. By assumptions we also have $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \notin A_{\psi[i]}$. As $\mathrm{tp}(\psi[i]) = \bigwedge$, $\mathfrak{s} \notin A_{\psi[i]}$ shows $d < D_a$, hence both $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \notin A_{\psi[i]}$ together with the definition of $N_{\psi[i]}$ show $N_{\psi[i][d]}(\mathfrak{s}') = \mathfrak{s}'$ and $\mathfrak{s}' \notin A_{\psi[i][d]}$. Now we can conclude using Proposition 6.15 that $\psi[i][d]$ is false.

If $\mathfrak{s} \in A_{\psi[i]}$ and $\psi \neq (\exists y)\varphi(\underline{a}, y)$, then $N(x,s) = s$ and there is nothing to show.

Finally, if $\mathfrak{s} \in A_{\psi[i]}$ and $\psi = (\exists y)\varphi(\underline{a}, y)$, then $N(x,s) = i$ and we have to show that $i < D_a$ and that $\varphi(\underline{a}, \underline{i})$ is true. Lemma 5.13, 2., shows that $i < \mathrm{bd}(h)$, thus $i < \mathrm{bd}(h_a) \leq D_a$. Again, $s \in F(x)$ implies $\mathfrak{s} \in F_{\psi[i]}$. Thus the assumptions $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \in A_{\psi[i]}$ together with Proposition 6.15 show that $\psi[i]$ is true, that is $\varphi(\underline{a}, \underline{i})$ is true.

Finally, Property (3.4)

$$(\forall x, s)(N(x,s) = s \ \vee \ c(x, N(x,s)) < c(x,s))$$

also follows immediately from the definitions. Because, for $s = (h, f, \mathfrak{s})$ with $N(x,s) = (h', f', \mathfrak{s}') \neq s$, either $h' = h[j]$ for some j, and then $\mathrm{o}(h') < \mathrm{o}(h)$, or $h' = h$ and $\mathfrak{s}' = N_\psi(\mathfrak{s}) \neq \mathfrak{s}$ and then $c(\mathfrak{s}') < c(\mathfrak{s})$ using Proposition 6.16. □

7.2 $\Sigma^{\mathrm{b}}_{\ell+1}$-definable search problems in T^{k+1}_2 for $\ell \leq k$

Let $0 \leq \ell \leq k$ and assume that $\mathrm{T}^{k+1}_2 \vdash (\forall x)(\exists y)\varphi(x,y)$ with $(\exists y)\varphi(x,y) \in \mathrm{s}\Sigma^{\mathrm{b}}_{\ell+1}$, $\varphi \in \mathrm{s}\Pi^{\mathrm{b}}_{\ell}$. Inverting the $(\forall x)$ quantifier we also obtain $\mathrm{T}^{k+1}_2 \vdash (\exists y)\varphi(x,y)$. By partial cut-elimination, Theorem 5.11, we obtain some $\mathrm{BA}^\star$-derivation h such that $\mathrm{FV}(h) \subseteq \{x\}$, $\Gamma(h) = \{(\exists y)\varphi(x,y)\}$, $\mathrm{s}\Sigma^{\mathrm{b}}_{k+1}$-gcrk$(h) = 0$, and $\mathrm{o}(h(\underline{a}/x)) = |a|^{O(1)}$.

Let Φ be deco(h) together with the closure of deco$(h) \cap \Delta_0$ under negation and taking subformulas. Then $L = \langle \Phi, \ell, k, h, (\exists y)\varphi(x,y)\rangle$ defines a local search problem according to Definition 7.3, because the following are provable in S^1_2:

- $\Gamma(h_a) = \Gamma(\mathsf{E}h(\underline{a}/x)) = \Gamma(h(\underline{a}/x)) \subseteq \Gamma(h)(\underline{a}/x) = \{(\exists y)\varphi(\underline{a},y)\}$, where we used Lemma 5.8 for "$\subseteq$";
- $$\begin{aligned} \mathrm{s}\Sigma^{\mathrm{b}}_0\text{-crk}(h_a) &= \mathrm{s}\Sigma^{\mathrm{b}}_0\text{-crk}(\mathsf{E}h(\underline{a}/x)) = \mathrm{s}\Sigma^{\mathrm{b}}_0\text{-crk}(h(\underline{a}/x)) \dot{-} 1 \\ &= \mathrm{s}\Sigma^{\mathrm{b}}_0\text{-gcrk}(h(\underline{a}/x)) \dot{-} 1 = \mathrm{s}\Sigma^{\mathrm{b}}_0\text{-gcrk}(h) \dot{-} 1 \\ &\leq (\mathrm{s}\Sigma^{\mathrm{b}}_{k+1}\text{-gcrk}(h) + k + 1) \dot{-} 1 = k \ , \end{aligned}$$

  using the properties mentioned directly after Definition 5.5 for "$\leq$";
- $\mathrm{o}(h_a) = \mathrm{o}(\mathsf{E}h(\underline{a}/x)) = 2^{\mathrm{o}(h(\underline{a}/x))} - 1 = 2^{|a|^{O(1)}}$;
- $$\begin{aligned} \vartheta(h_a) &= \vartheta(\mathsf{E}h(\underline{a}/x)) = \mathrm{o}(h(\underline{a}/x)) \cdot (\vartheta(h(\underline{a}/x)) + 2) \\ &= |a|^{O(1)} \cdot (|h(\underline{a}/x)| + 2) = |a|^{O(1)} \cdot (|h| + 2) = |a|^{O(1)} \ ; \end{aligned}$$
- deco$(h_a) = $ deco$(\mathsf{E}h(\underline{a}/x)) = $ deco$(h(\underline{a}/x)) \subseteq \Phi_a$, where we have used Lemma 5.17, 2. for the last inclusion.

By Proposition 7.4, this defines a search problem in Π^{b}_k-PLS with Π^{b}_ℓ-goal. Thus we have proven Theorem 3.5, that the $\Sigma^{\mathrm{b}}_{\ell+1}$-definable total search problems in T^{k+1}_2 can be characterised by Π^{b}_k-PLS problems with Π^{b}_ℓ-goals. Together with Theorem 3.4 we obtain a full characterisation of the $\Sigma^{\mathrm{b}}_{\ell+1}$-definable total search problems in T^{k+1}_2:

Corollary 7.5. *Let $0 \leq \ell \leq k$. The $\Sigma^{\mathrm{b}}_{\ell+1}$-definable total search problems in T^{k+1}_2 are exactly characterised by Π^{b}_k-PLS problems with Π^{b}_ℓ-goals.*

8 Skolemising Search for Truth

In the remaining sections we will strengthen our results by showing that the properties (3.1)–(3.5) of the Π^{b}_k-PLS problems extracted from T^{k+1}_2-proofs according to Theorem 3.5 can be written in a prenex form which can be skolemised by simple polynomial time functions, provably in S^1_2.

Notation 8.1. We use α, β,... to range over formulas in Σ^{b}_0.

Definition 8.2 (Prenex forms)**.** ψ is called *a prenex form of* φ iff ψ has the shape $(\mathfrak{Q}\mathfrak{z})\beta$ for some $\beta \in \Sigma^{\mathrm{b}}_0$, such that $\overline{\mathrm{BASIC}} \vdash \varphi \leftrightarrow \psi$.

Definition 8.3 (Simple Skolemisation)**.** Let $(\mathfrak{Q}\mathfrak{z})\beta(x, \mathfrak{z})$ with $\beta \in \Sigma^{\mathrm{b}}_0$ be a prenex form for $\varphi(x)$, where $\mathfrak{z} = [z_1, \ldots, z_k]$ and $\mathfrak{Q} = [Q_1, \ldots, Q_k]$. Let f be some function symbol. We say that

$$(\forall x)(\varphi(x) \rightarrow \varphi(f(x)))$$

admits simple Skolem functions iff there are polynomial time computable functions $f_1, \ldots, f_k$ such that

$$(\forall x)(\forall^k \mathfrak{z})(\beta(x, t_1, \ldots, t_k) \rightarrow \beta(f(x), t'_1, \ldots, t'_k))$$

is provable in S^1_2, where

$$t_i := \begin{cases} z_i & \text{if } Q_i = \exists \\ f_i(x, z_1, \ldots, z_i) & \text{otherwise} \end{cases}$$

$$t'_i := \begin{cases} f_i(x, z_1, \ldots, z_i) & \text{if } Q_i = \exists \\ z_i & \text{otherwise} \end{cases}$$

The main result of this section will be to fix a suitable prenex form for $\mathfrak{s} \in F_\varphi$ in such a way that the *canonical* prenex form of

$$(\forall \mathfrak{s})(\mathfrak{s} \in F_\varphi \rightarrow N_\varphi(\mathfrak{s}) \in F_\varphi) \tag{8.1}$$

admits simple Skolem functions — we explain later what we mean by a canonical prenex form. In the next subsection we fix a suitable prenex form for $\mathfrak{s} \in F_\varphi$; that it enjoys the above mentioned property will be shown later in Theorem 8.5.

8.1 A suitable prenex form for $\mathfrak{s} \in F_\varphi$

Formulas have many prenex forms. We will now pick a suitable one for the formula $\mathfrak{s} \in F_\varphi$. Remember that we defined the application of the projection function p_i to formal tuples $\mathfrak{t} = [t_1, \ldots, t_k]$ as $\mathrm{p}_i(\mathfrak{t}) = [\mathrm{p}_i(t_1), \ldots, \mathrm{p}_i(t_k)]$.

Theorem 8.4. *Let φ be a strict formula of rank k, and D a s.u.b. for φ. Then there is a* $\mathrm{s}\Sigma_0^{\mathrm{b}}$*-formula γ_φ such that the following are provable in* $\overline{\text{BASIC}}$*:*

1. $\mathfrak{s} \in F_\varphi \quad \Leftrightarrow \quad (\forall\!\exists^k \mathfrak{z})\gamma_\varphi(\mathfrak{s}, \mathfrak{z})$.
2. $(\forall \mathfrak{s})(\forall^k \mathfrak{z}^1)(\forall^k \mathfrak{z}^2)\Big(\bigwedge_{1\le i,j\le k} \mathrm{p}_j(\mathfrak{z}_i^1) = \mathrm{p}_j(\mathfrak{z}_i^2) \ \wedge\ \gamma_\varphi(\mathfrak{s}, \mathfrak{z}^1) \ \to\ \gamma_\varphi(\mathfrak{s}, \mathfrak{z}^2)\Big)$.
3. $(\forall^k \mathfrak{z})\gamma_\varphi(0^k, \mathfrak{z})$.
4. *If $k \ge 1$ and $\varphi \equiv (\exists\!\forall^k \mathfrak{z})\beta(\mathfrak{z})$, then*
$$\gamma_\varphi(\mathfrak{s}, \mathfrak{z}) \ \to\ (\mathrm{p}_k(\mathfrak{z}_1) < \mathfrak{s}_1 \ \to\ \neg\beta(\mathrm{p}_k(\mathfrak{z})))$$
Here, $\mathrm{p}_k(\mathfrak{z})$ *denotes* $[\mathrm{p}_k(\mathfrak{z}_1), \ldots, \mathrm{p}_k(\mathfrak{z}_k)]$.
5. *If $k \ge 2$ and $\varphi \equiv (\exists\!\forall^k \mathfrak{z})\beta(\mathfrak{z})$, then*
$$\gamma_\varphi(\mathfrak{s}, \mathfrak{z}) \ \to\ (\mathrm{p}_{k-1}(\mathfrak{z}_1) < \mathfrak{s}_2 \ \to\ \beta(\mathfrak{s}_1, \mathrm{p}_{k-1}(\mathfrak{z}\lceil_{k-1})))$$
Observe that $\mathrm{p}_{k-1}(\mathfrak{z}\lceil_{k-1})$ *denotes* $[\mathrm{p}_{k-1}(\mathfrak{z}_1), \ldots, \mathrm{p}_{k-1}(\mathfrak{z}_{k-1})]$.

Proof. The definition and proof are by induction on k. If $k = 0$ let γ_φ be the formula $0 = 0$. All properties are obviously satisfied.

For $k > 0$ and $\varphi \equiv (\forall x)\beta(x)$ we define $\gamma_\varphi(\mathfrak{s}, \mathfrak{z})$ to be the same as $\gamma_{\neg\varphi}(\mathfrak{s}, \mathfrak{z})$.

For $k = 1$ and $\varphi \equiv (\exists x)\beta(x)$ we have $\langle u\rangle \in F_\varphi \equiv (\forall x{<}u)\neg\beta(x)$. Let $\gamma_\varphi(\langle u\rangle, x)$ be the formula

$$(\mathrm{p}_1(x){<}u \ \to\ \neg\beta(\mathrm{p}_1(x)))$$

Again it is easy to see that all properties are satisfied.

Although the general inductive case is for $k \ge 2$ already, we write out the cases for $k = 2$ and $k = 3$ explicitly, to make the definition of γ_φ more clear. The mentioning of "$\wedge\ 0 = 0$" in the following case is to suit the general inductive case. Let $k = 2$ and $\varphi \equiv (\exists x)(\forall y)\beta(x, y)$. Then $\langle u, v\rangle \in F_\varphi$ has the form

$$(\forall x{<}u)(\exists y)\neg\beta(x, y) \ \wedge\ (\forall y{<}v)\beta(u, y) \ .$$

Let $\gamma_\varphi(\langle u, v\rangle, x, y)$ be the formula

$$\begin{aligned} &(\mathrm{p}_2(x){<}u \ \to\ \neg\beta(\mathrm{p}_2(x), \mathrm{p}_2(y))) \\ \wedge\ &(\mathrm{p}_1(x){<}v \ \to\ \beta(u, \mathrm{p}_1(x))) \\ \wedge\ &0 = 0 \ . \end{aligned}$$

If $k = 3$ and $\varphi \equiv (\exists x)(\forall y)(\exists z)\beta(x, y, z)$ we have that $\langle u, v, w\rangle \in F_\varphi$ is of the form

$$(\forall x{<}u)(\exists y)(\forall z)\neg\beta(x, y, z) \ \wedge\ (\forall y{<}v)(\exists z)\beta(u, y, z) \ \wedge\ (\forall z{<}w)\neg\beta(u, v, z) \ .$$

Let $\gamma_\varphi(\langle u, v, w\rangle, x, y, z)$ be the formula

$$\begin{aligned} & (\mathrm{p}_3(x) < u \;\rightarrow\; \neg\beta(\mathrm{p}_3(x), \mathrm{p}_3(y), \mathrm{p}_3(z))) \\ \wedge\; & (\mathrm{p}_2(x) < v \;\rightarrow\; \beta(u, \mathrm{p}_2(x), \mathrm{p}_2(y))) \\ \wedge\; & (\mathrm{p}_1(z) < w \;\rightarrow\; \neg\beta(u, v, \mathrm{p}_1(z)))\ . \end{aligned}$$

For all cases considered so far it is easy to verify that the assertions 1.–6. are satisfied. We have explicitly written out case $k = 3$ to stress the dependency of quantifiers: It will be crucial for our later developments that the 3rd conjunct uses "z" and not "x" as a naive inductive continuation might suggest.

For the general inductive case we assume $\varphi \equiv (\exists x)(\forall y)\psi(x, y)$, $\psi \equiv (\exists\forall^k \mathfrak{z})\beta(x, y, \mathfrak{z})$ and $\mathrm{rk}(\psi) = k \geq 0$. Then $\langle u, v \,|\, \mathfrak{s}\rangle \in F_\varphi$ has the form

$$\begin{aligned} & (\forall x < u)(\exists y)\neg\psi(x, y) \;\wedge\; (\forall y < v)\psi(u, y) \;\wedge\; \mathfrak{s} \in F_{\psi xy}(u, v) \\ \Leftrightarrow\quad & \qquad (\forall x)(\exists y)(\forall\exists^k \mathfrak{z})(x < u \;\rightarrow\; \neg\beta(x, y, \mathfrak{z})) \\ & \quad \wedge\;\; (\forall y)(\exists\forall^k \mathfrak{z})(y < v \;\rightarrow\; \beta(u, y, \mathfrak{z})) \\ & \quad \wedge\;\; ((\forall\exists^k \mathfrak{z})\gamma_{\psi xy}(u, v, \mathfrak{s}, \mathfrak{z}) \\ \Leftrightarrow\quad & (\forall x)(\exists y)(\forall\exists^k \mathfrak{z})\gamma_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle, x, y, \mathfrak{z}) \end{aligned}$$

where we define $\gamma_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle, x, y, \mathfrak{z})$ to be the formula

$$\begin{aligned} & (\mathrm{p}_{k+2}(x) < u \;\rightarrow\; \neg\beta(\mathrm{p}_{k+2}(x), \mathrm{p}_{k+2}(y), \mathrm{p}_{k+2}(\mathfrak{z}))) \\ \wedge\; & (\mathrm{p}_{k+1}(x) < v \;\rightarrow\; \beta(u, \mathrm{p}_{k+1}(x), \mathrm{p}_{k+1}(y), \mathrm{p}_{k+1}(\mathfrak{z}\lceil_{k-1}))) \\ \wedge\; & \gamma_{\psi xy}(u, v, \mathfrak{s}, \mathfrak{z})\ . \end{aligned}$$

This choice of γ_φ obviously satisfies all assertions. □

8.2 A simple Skolemisation for $(\forall\mathfrak{s})(\mathfrak{s} \in F_\varphi \;\rightarrow\; N_\varphi(\mathfrak{s}) \in F_\varphi)$

Now that we have fixed prenex forms for $\mathfrak{s} \in F_\varphi$, we choose a suitable prenex form of $(\forall\mathfrak{s})(\mathfrak{s} \in F_\varphi \;\rightarrow\; N_\varphi(\mathfrak{s}) \in F_\varphi)$ in a canonical way:

$$\begin{aligned} & (\forall\mathfrak{s})(\mathfrak{s} \in F_\varphi \;\rightarrow\; N_\varphi(\mathfrak{s}) \in F_\varphi) \\ \Leftrightarrow\quad & (\forall\mathfrak{s})\Big((\forall\exists^k \mathfrak{z})\gamma_\varphi(\mathfrak{s}, \mathfrak{z}) \;\rightarrow\; (\forall\exists^k \bar{\mathfrak{z}})\gamma_\varphi(N_\varphi(\mathfrak{s}), \bar{\mathfrak{z}})\Big) \\ \Leftrightarrow\quad & (\forall\mathfrak{s})(\forall\bar{\mathfrak{z}}_1)(\exists\mathfrak{z}_1)(\forall\mathfrak{z}_2)(\exists\bar{\mathfrak{z}}_2)(\forall\bar{\mathfrak{z}}_3)(\exists\mathfrak{z}_3)\cdots\Big(\gamma_\varphi(\mathfrak{s}, \mathfrak{z}) \;\rightarrow\; \gamma_\varphi(N_\varphi(\mathfrak{s}), \bar{\mathfrak{z}})\Big) \end{aligned}$$

The latter is the prenex form which we fix.

Theorem 8.5. *Let φ be a strict formula of rank k, and D a s.u.b for φ. The prenex form which we fixed for $(\forall\mathfrak{s})(\mathfrak{s} \in F_\varphi \;\rightarrow\; N_\varphi(\mathfrak{s}) \in F_\varphi)$ admits simple Skolem functions.*

Proof. We have to show that there are polynomial time computable functions

$$f_1(\mathfrak{s}, z_1),\ \ f_2(\mathfrak{s}, z_1, z_2),\ \ f_3(\mathfrak{s}, z_1, z_2, z_3),\ \ \dots$$

such that

$$\begin{aligned}
&(\forall \mathfrak{s}, z_1, z_2, z_3, \dots\,) \\
&\quad\Big(\gamma_\varphi(\mathfrak{s}, f_1(\mathfrak{s}, z_1), z_2, f_3(\mathfrak{s}, z_1, z_2, z_3), z_4, \dots\,) \\
&\qquad\quad \to\ \gamma_\varphi(N_\varphi(\mathfrak{s}), z_1, f_2(\mathfrak{s}, z_1, z_2), z_3, f_4(\dots, z_4), \dots\,)\Big)\ .
\end{aligned} \tag{8.2}$$

In the following we suppress the argument $\mathfrak{s}$ from the Skolem functions. The Skolem functions may also depend on further parameters of φ which we also do not mention. We say that *the i-th slice of $f_1(z_1)$ ($f_2(z_1, z_2)$, $f_3(z_1, z_2, z_3)$, $\dots$ respectively) is chosen canonically* if $\mathrm{p}_i(f_1(z_1)) = \mathrm{p}_i(z_1)$ ($\mathrm{p}_i(f_2(z_1, z_2)) = \mathrm{p}_i(z_2)$, $\mathrm{p}_i(f_3(z_1, z_2, z_3)) = \mathrm{p}_i(z_3)$, $\dots$ respectively.) Choosing the i-th slice of $f_1, f_2, f_3, \dots$ canonically implies that

$$\begin{aligned}
&\mathrm{p}_i([f_1(z_1), z_2, f_3(z_1, z_2, z_3), z_4, \dots]) \\
&\qquad\qquad = \mathrm{p}_i([z_1, z_2, z_3, z_4, \dots]) \\
&\qquad\qquad = \mathrm{p}_i([z_1, f_2(z_1, z_2), z_3, f_4(z_1, z_2, z_3, z_4), \dots])
\end{aligned}$$

We now define the Skolem functions and prove (8.2) by induction on k.

If $k = 0$ there is nothing to show. If $k = 1$ and $\varphi \equiv (\exists x)\beta(x)$ we choose the first slice of f_1 canonically. Then (8.2) is equivalent to

$$\begin{aligned}
&(\forall u, x)(\gamma_\varphi(\langle u\rangle\,, f_1(x))\ \to\ \gamma_\varphi(N_\varphi(\langle u\rangle), x)) \\
\Leftrightarrow\quad &(\forall u, \bar{u}, x)\Big(N_\varphi(\langle u\rangle) = \langle \bar{u}\rangle\ \wedge\ (\mathrm{p}_1(x) < u\ \to\ \neg\beta(\mathrm{p}_1(x))) \\
&\qquad\qquad \to\ (\mathrm{p}_1(x) < \bar{u}\ \to\ \neg\beta(\mathrm{p}_1(x)))\Big)
\end{aligned}$$

The non-trivial case is when $N_\varphi(\langle u\rangle) = \langle \bar{u}\rangle$, $\bar{u} = u{+}1$ and $\mathrm{p}_1(x) = u$. By definition of N_φ this implies $\neg\beta(u)$, hence (8.2) follows.

For the inductive case we consider $\varphi \equiv (\exists x)(\forall y)\psi(x, y)$ with $\psi(x, y) \equiv (\exists\forall^k \mathfrak{z})\beta(x, y, \mathfrak{z})$ and $k \geq 0$. Then (8.2) is equivalent to

$$\begin{aligned}
&(\forall u, v, \bar{u}, \bar{v}, \mathfrak{s}, \bar{\mathfrak{s}}, z_1, z_2, \dots\,) \\
&\Big(N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) = \langle \bar{u}, \bar{v} \,|\, \bar{\mathfrak{s}}\rangle \\
&\qquad \wedge\ \ (\mathrm{p}_{k+2}(f_1(z_1)){<}u \\
&\qquad\qquad\quad \to\ \ \neg\beta(\mathrm{p}_{k+2}([f_1(z_1), z_2, f_3(z_1, z_2, z_3), z_4, \dots]))) \\
&\qquad \wedge\ \ (\mathrm{p}_{k+1}(f_1(z_1)){<}v\ \to\ \ \beta(u, \mathrm{p}_{k+1}([f_1(z_1), z_2, f_3(\dots\,), \dots]))) \\
&\qquad \wedge\ \ \gamma_{\psi xy}(u, v, \mathfrak{s}, f_3(z_1, z_2, z_3), z_4, \dots\,) \\
&\ \ \to\ (\mathrm{p}_{k+2}(z_1){<}\bar{u}\ \to\ \neg\beta(\mathrm{p}_{k+2}([z_1, f_2(z_1, z_2), z_3, f_4(\dots\,), \dots]))) \\
&\qquad \wedge\ \ (\mathrm{p}_{k+1}(z_1){<}\bar{v}\ \to\ \beta(\bar{u}, \mathrm{p}_{k+1}([z_1, f_2(z_1, z_2), z_3, \dots]))) \\
&\qquad \wedge\ \ \gamma_{\psi xy}(\bar{u}, \bar{v}, \bar{\mathfrak{s}}, z_3, f_4(z_1, z_2, z_3, z_4), \dots\,)\Big)
\end{aligned} \tag{8.3}$$

Let $u, v, \bar{u}, \bar{v}, \mathfrak{s}, \bar{\mathfrak{s}}, z_1, z_2, z_3, \dots$ be given with $N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) = \langle \bar{u}, \bar{v} \,|\, \bar{\mathfrak{s}}\rangle$. The possible cases for N_φ are that $N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) = \langle u, v \,|\, \mathfrak{s}\rangle$ which is trivial, or that $N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) \neq \langle u, v \,|\, \mathfrak{s}\rangle$, in which case we distinguish the following three sub-cases according to the definition of N_φ:

1. $N_{\psi xy}(u, v, \mathfrak{s}) = \mathfrak{s}' \neq \mathfrak{s}$, thus
$$N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) = \left\langle u, v \,|\, \mathfrak{s}' \right\rangle \ .$$
2. $N_{\psi xy}(u, v, \mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \in A_{\psi xy}(u, v)$, thus
$$N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) = \left\langle u, v+1 \,|\, 0^k \right\rangle \ .$$
3. $N_{\psi xy}(u, v, \mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \notin A_{\psi xy}(u, v)$, thus
$$N_\varphi(\langle u, v \,|\, \mathfrak{s}\rangle) = \left\langle u+1, 0 \,|\, 0^k \right\rangle \ .$$

As $N_{\psi xy}$ and $A_{\psi xy}$ are polynomial time computable, and $u, v, \bar{u}, \bar{v}, \mathfrak{s}, \bar{\mathfrak{s}}$ are parameters to all Skolem functions, we can define the Skolem functions by case distinction according to the above three cases.

Case 1. We have $\bar{u} = u$, $\bar{v} = v$, $\bar{\mathfrak{s}} = \mathfrak{s}'$. By induction hypothesis there are $f_3, f_4, \dots$ such that

$$\begin{aligned} &\gamma_{\psi xy}(u, v, \mathfrak{s}, f_3(z_1, z_2, z_3), z_4, \dots) \\ &\quad \to \ \gamma_{\psi xy}(u, v, \mathfrak{s}', z_3, f_4(z_1, z_2, z_3, z_4), \dots) \end{aligned}$$

where the functions do not yet depend on z_1, z_2. By Definition 8.4, 2. this still holds if we modify slice $k+1$ and $k+2$ of $f_3, f_4, \dots$. We choose slices $k+1$ and $k+2$ of $f_1, f_2, f_3, f_4, \dots$ canonically. Then (8.3) turns into

$$\begin{aligned} &(\mathrm{p}_{k+2}(z_1) {<} u \ \to\ \neg\beta(\mathrm{p}_{k+2}([z_1, z_2, z_3, \dots]))) \\ &\quad\wedge\ \ (\mathrm{p}_{k+1}(z_1) {<} v \ \to\ \beta(u, \mathrm{p}_{k+1}([z_1, z_2, z_3, \dots]))) \\ &\quad\wedge\ \ \gamma_{\psi xy}(u, v, \mathfrak{s}, f_3(z_1, z_2, z_3), z_4, \dots) \\ \to\ &(\mathrm{p}_{k+2}(z_1) {<} u \ \to\ \neg\beta(\mathrm{p}_{k+2}([z_1, z_2, z_3, \dots]))) \\ &\quad\wedge\ \ (\mathrm{p}_{k+1}(z_1) {<} v \ \to\ \beta(u, \mathrm{p}_{k+1}([z_1, z_2, z_3, \dots]))) \\ &\quad\wedge\ \ \gamma_{\psi xy}(u, v, \mathfrak{s}', z_3, f_4(z_1, z_2, z_3, z_4), \dots) \end{aligned}$$

which is obviously satisfied using the induction hypothesis.

Case 2. We have $\bar{u} = u$, $\bar{v} = v+1$, and $\bar{\mathfrak{s}} = 0^k$. Observe that $\gamma_{\psi xy}(u, v{+}1, 0^k, \dots)$ is always true by Theorem 8.4, 3. We choose slice $k{+}2$ of the Skolem functions canonically. Thus, (8.3) follows from

$$\begin{aligned} &(\mathrm{p}_{k+1}(f_1(z_1)) < v \ \to\ \ \beta(u, \mathrm{p}_{k+1}([f_1(z_1), z_2, f_3(\dots), \dots]))) \\ &\quad\wedge\ \ \gamma_{\psi xy}(u, v, \mathfrak{s}, f_3(z_1, z_2, z_3), z_4, \dots) \\ \to\ &(\mathrm{p}_{k+1}(z_1) < v+1 \ \to\ \beta(u, \mathrm{p}_{k+1}([z_1, f_2(z_1, z_2), z_3, \dots]))) \end{aligned} \tag{8.4}$$

If $\mathrm{p}_{k+1}(z_1) \neq v$ choose all slices of Skolem functions canonically, then (8.4) is obviously satisfied.

Now assume $\mathrm{p}_{k+1}(z_1) = v$. If $k = 0$ we choose all slices of Skolem functions canonically. Then (8.4) is equivalent to $\beta(u,v)$ which is satisfied, because we have by construction of N_φ that $\mathfrak{s} \in A_{\beta(x,y)xy}(u,v)$, which implies that $\beta(u,v)$ is true.

If $k \geq 1$, we choose Skolem functions in the following way:

$$\begin{array}{rlr}
 & \mathrm{p}_{k+1}(f_2(z_1,z_2)) = \mathfrak{s}_1 & \\
\mathrm{p}_{k-1}(f_3(z_1,z_2,z_3)) = \mathrm{p}_{k+1}(z_3) & \mathrm{p}_{k+1}(f_4(\dots,z_4)) = \mathrm{p}_{k-1}(z_4) & \\
\mathrm{p}_{k-1}(f_5(\dots,z_5)) = \mathrm{p}_{k+1}(z_5) & \mathrm{p}_{k+1}(f_6(\dots,z_6)) = \mathrm{p}_{k-1}(z_6) & \dots
\end{array}$$

and all other slices canonically. Assuming the antecedent of (8.4) we have to show $\beta(u,v,\mathfrak{s}_1,\mathrm{p}_{k+1}(z_3),\mathrm{p}_{k-1}(z_4),\mathrm{p}_{k+1}(z_5),\dots)$.

If $k = 1$, the definition of N_φ shows $\mathfrak{s} \in A_{(\exists z)\beta(x,y,z)}(u,v)$, which by construction implies that $\beta(u,v,\mathfrak{s}_1)$ is true.

In case $k \geq 2$ we obtain from Theorem 8.4, 5 that

$$\gamma_{\psi xy}(u,v,\mathfrak{s},\mathfrak{t}) \ \to\ (\mathrm{p}_{k-1}(\mathfrak{t}_1) < \mathfrak{s}_2 \ \to\ \beta(u,v,\mathfrak{s}_1,\mathrm{p}_{k-1}(\mathfrak{t}\lceil_{k-1})))$$

for $\mathfrak{t} = [f_3(z_1,z_2,z_3), z_4, f_5(\dots),\dots]$. Together with the antecedent of (8.4) this implies

$$\mathrm{p}_{k-1}(f_3(z_1,z_2,z_3)) < \mathfrak{s}_2 \ \to\ \beta(u,v,\mathfrak{s}_1,\mathrm{p}_{k-1}([f_3(z_1,z_2,z_3),z_4,\dots])) \ .$$

By our choice of Skolem functions the latter simplifies to

$$\mathrm{p}_{k+1}(z_3) < \mathfrak{s}_2 \ \to\ \beta(u,v,\mathfrak{s}_1,\mathrm{p}_{k+1}(z_3),\mathrm{p}_{k-1}(z_4),\mathrm{p}_{k+1}(z_5),\dots) \ .$$

As $\mathfrak{s} \in A_{\psi xy}(u,v)$ and $\mathrm{tp}(\psi) = \bigvee$ we have $\mathfrak{s}_2 = D$ by Corollary 6.14, thus $\beta(u,v,\mathfrak{s}_1,\mathrm{p}_{k+1}(z_3),\mathrm{p}_{k-1}(z_4),\mathrm{p}_{k+1}(z_5),\dots)$ is satisfied.

Case 3. We have $\bar{u} = u+1$, $\bar{v} = 0$ and $\bar{\mathfrak{s}} = 0^k$. Observe that the formula $\gamma_{\psi xy}(u+1,0,0^k,\dots)$ is always true by Theorem 8.4, 3. Thus, (8.3) follows from

$$\begin{array}{l}
\quad(\mathrm{p}_{k+2}(f_1(z_1)) < u \ \to\ \neg\beta(\mathrm{p}_{k+2}([f_1(z_1),z_2,f_3(\dots,z_3),\dots]))) \\
\ \wedge\ \gamma_{\psi xy}(u,v,\mathfrak{s},f_3(z_1,z_2,z_3),z_4,\dots) \\
\to\ (\mathrm{p}_{k+2}(z_1) < u+1 \ \to\ \neg\beta(\mathrm{p}_{k+2}([z_1,f_2(z_1,z_2),z_3,\dots])))
\end{array} \tag{8.5}$$

If $\mathrm{p}_{k+2}(z_1) \neq u$ choose all slices of Skolem functions canonically, then (8.5) is obviously satisfied.

Now assume $\mathrm{p}_{k+2}(z_1) = u$. We choose Skolem functions in the following way:

$$\begin{array}{rlr}
 & \mathrm{p}_{k+2}(f_2(z_1,z_2)) = v & \\
\mathrm{p}_{k}(f_3(z_1,z_2,z_3)) = \mathrm{p}_{k+2}(z_3) & \mathrm{p}_{k+2}(f_4(\dots,z_4)) = \mathrm{p}_{k}(z_4) & \\
\mathrm{p}_{k}(f_5(\dots,z_5)) = \mathrm{p}_{k+2}(z_5) & \mathrm{p}_{k+2}(f_6(\dots,z_6)) = \mathrm{p}_{k}(z_6) & \dots
\end{array}$$

and all other slices canonically. Assuming the antecedent of (8.5) we thus have to show $\neg\beta(u, v, \mathrm{p}_{k+2}(z_3), \mathrm{p}_k(z_4), \mathrm{p}_{k+2}(z_5), \dots)$.

If $k = 0$, the definition of N_φ shows $\mathfrak{s} \notin A_{\beta(x,y)}(u, v)$ which by construction implies that $\neg\beta(u, v)$ is true.

In case $k \geq 1$ we obtain from Theorem 8.4, 4 that

$$\gamma_{\psi xy}(u, v, \mathfrak{s}, \mathfrak{t}) \;\rightarrow\; (\mathrm{p}_k(\mathfrak{t}_1) < \mathfrak{s}_1 \;\rightarrow\; \neg\beta(u, v, \mathrm{p}_k(\mathfrak{t})))$$

for $\mathfrak{t} = [f_3(z_1, z_2, z_3), z_4, f_5(\dots), \dots]$. Together with the antecedent of (8.5) this implies

$$\mathrm{p}_k(f_3(z_1, z_2, z_3)) < \mathfrak{s}_1 \;\rightarrow\; \neg\beta(u, v, \mathrm{p}_k([f_3(z_1, z_2, z_3), z_4, \dots])) \ .$$

By our choice of Skolem functions the latter simplifies to

$$\mathrm{p}_{k+2}(z_3) < \mathfrak{s}_1 \;\rightarrow\; \neg\beta(u, v, \mathrm{p}_{k+2}(z_3), \mathrm{p}_k(z_4), \mathrm{p}_{k+2}(z_5), \dots) \ .$$

As $\mathfrak{s} \notin A_{\psi xy}(u, v)$ and $\mathrm{tp}(\psi) = \bigvee$ we have $\mathfrak{s}_1 = D$ by Corollary 6.14, thus the latter implies $\neg\beta(u, v, \mathrm{p}_{k+2}(z_3), \mathrm{p}_k(z_4), \mathrm{p}_{k+2}(z_5), \dots)$. □

Definition 8.6. Let φ be a strict formula of rank k, and D a s.u.b. for φ. We extend γ_φ from Definition 8.4 to sequences of length $\ell > k$ in the obvious way:

$$\gamma_\varphi(\langle u_1, \dots, u_\ell \rangle, \mathfrak{z}) \quad :\Longleftrightarrow \quad \gamma_\varphi(\langle u_1, \dots, u_k \rangle, \mathfrak{z}) \ .$$

9 Skolemising Π^{b}_k-PLS Conditions

We have seen in Proposition 7.4 that the local search problem L parameterised by $\langle \Phi, \ell, k, h, (\exists y)\varphi(x, y) \rangle$ defines a Π^{b}_k-PLS problem with Π^{b}_ℓ-goal. In this section, we are going to show that the Π^{b}_k-PLS conditions (3.1)-(3.5) for L can be skolemised by simple polynomial time Skolem functions. For the rest of this section, we assume the parametrisation for L is fixed.

Definition 9.1. For each strict formula we fix a notation of its syntactic form. Let $k = \mathrm{rk}(\psi)$ and choose $\beta_\psi(z_1, \dots, z_k) \in \mathrm{s}\Sigma^{\mathrm{b}}_0 \cup \mathrm{s}\Pi^{\mathrm{b}}_0$ such that the following holds: If $\mathrm{tp}(\psi) = \bigvee$ then $\psi \equiv (\exists\forall^k \mathfrak{z})\beta_\psi(\mathfrak{z})$; if $\mathrm{tp}(\psi) = \bigwedge$ then $\psi \equiv (\forall\exists^k \mathfrak{z})\beta_\psi(\mathfrak{z})$. Further parameters to ψ may be denoted as convenient.

We are now going to fix a suitable prenex form of $s \in F(a)$, which will then be used to show that the Π^{b}_k-PLS conditions (3.1)-(3.5) admit simple Skolem functions.

First, let us bring the formula $s \in F(a)$ into a more readable form: $s \in F(a)$ is equivalent to

$$\begin{aligned}
&\Big[s < D_a \ \wedge\ \varphi(a,s)\Big] \\
&\vee\ \Big[\ s \geq D_a \ \wedge\ s = \langle h, f, \mathfrak{s}\rangle \ \wedge\ s \in C(a) \ \wedge\ \mathrm{tp}(h) \neq \mathrm{Ax}_\psi \\
&\quad \wedge\ (\forall\sigma)\Big(\ \ \big(\sigma = \langle 1,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_1(s,\psi,\nu) \ \to\ \neg\psi[f(\psi)]\ \big) \\
&\qquad\qquad \wedge\ \big(\sigma = \langle 2,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_2(s,\psi,\nu) \ \to\ \quad \neg\psi \quad\ \big) \\
&\qquad\qquad \wedge\ \big(\sigma = \langle 3,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_3(s,\psi,\nu) \ \to\ \ \mathfrak{s} \in F_\psi \ \ \big)\Big)\ \Big]
\end{aligned}$$

using the following abbreviations:

- $\mathit{Cond}_1(\langle h, f, \mathfrak{s}\rangle, \psi, \nu)$ expresses
$$\nu = \mathrm{rk}(\psi) \ \wedge\ \psi \in \mathrm{dom}(f)$$
- $\mathit{Cond}_2(\langle h, f, \mathfrak{s}\rangle, \psi, \nu)$ expresses
$$\nu = \mathrm{rk}(\psi) \ \wedge\ \psi \in \Gamma(h) \setminus \big(\mathrm{dom}(f) \cup \{(\exists y)\varphi(\underline{a}, y)\}\big)$$
- $\mathit{Cond}_3(\langle h, f, \mathfrak{s}\rangle, \psi, \nu)$ expresses
$$\nu = \mathrm{rk}(\psi) \ \wedge\ \Big(\mathrm{tp}(h) = \mathrm{Cut}_\psi \ \vee\ \big(\mathrm{tp}(h) = \textstyle\bigvee_\chi^i \ \wedge\ \psi = \chi[i]\big)\Big)$$

To increase readability, we have used additional informal parameters as in "$s = \langle h, f, \mathfrak{s}\rangle$", which, when making everything formal, would have to be replaced by appropriate projections, e.g. "h" by "$\mathrm{p}_1(s)$" etc.

The occurrence of ν is currently superfluous but will play a role later. The conditions $s \in C(a)$ and Cond_1 to Cond_3 are obviously polynomial time computable and thus can be expressed by sharply bounded formulas. Thus, their exact shape is irrelevant for determining a suitable prenex form. The evaluation of formulas $\neg\psi[f(\psi)]$ and $\neg\psi$ can be expressed because each ψ has to be a numerical substitution of a formula from Φ which is a *finite* set.

We continue to determine a suitable prenex form of $s \in F(a)$. Using the suitable prenex form which we have fixed for $\mathfrak{s} \in F_\psi$ in Section 8, and the notation fixed in Definition 9.1, we transform $s \in F(a)$ equivalently into

$$\begin{aligned}
&\Big[s < D_a \ \wedge\ (\forall\exists^\ell \mathfrak{z})\beta_\varphi(a,s,\mathfrak{z})\Big] \\
&\vee\ \Big[s \geq D_a \ \wedge\ s = \langle h, f, \mathfrak{s}\rangle \ \wedge\ s \in C(a) \ \wedge\ \mathrm{tp}(h) \neq \mathrm{Ax}_\psi \ \wedge\ (\forall\sigma)\Big(\\
&\qquad\quad \big(\sigma = \langle 1,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_1(s,\psi,\nu) \ \to\ \ \neg\big((\forall\exists^\nu \mathfrak{z})\beta_\psi(\mathfrak{z})[f(\psi)]\big)\ \ \big) \\
&\qquad \wedge\ \big(\sigma = \langle 2,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_2(s,\psi,\nu) \ \to\ \qquad \neg(\exists\forall^\nu \mathfrak{z})\beta_\psi(\mathfrak{z}) \qquad \big) \\
&\qquad \wedge\ \big(\sigma = \langle 3,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_3(s,\psi,\nu) \ \to\ (\forall\exists^\nu \mathfrak{z})\gamma_\psi(\mathfrak{s},\mathfrak{z})\big) \qquad \Big)\ \Big]\ .
\end{aligned}$$

This is equivalent to

$$(\forall\sigma)(\forall\!\!\!\exists^k\mathfrak{z})\Psi(a,s,\sigma,\mathfrak{z}) \tag{9.1}$$

for $\Psi(a,s,\sigma,\mathfrak{z})$ expressing

$$\begin{array}{l}
\Big[s < D_a \ \wedge\ \beta_\varphi(a,s,\mathrm{p}_\ell(\mathfrak{z}\lceil_\ell))\Big] \\
\quad \vee\ \Big[s \geq D_a \ \wedge\ s = \langle h,f,\mathfrak{s}\rangle \ \wedge\ s \in C(a) \ \wedge\ \mathrm{tp}(h) \neq \mathrm{Ax}_\psi \\
\qquad \wedge\ \big(\sigma = \langle 1,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_1(s,\psi,\nu) \ \rightarrow\ \neg\beta_\psi(f(\psi),\mathrm{p}_{\nu-1}(\mathfrak{z}\lceil_{\nu-1}))\big) \\
\qquad \wedge\ \big(\sigma = \langle 2,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_2(s,\psi,\nu) \ \rightarrow\ \qquad \neg\beta_\psi(\mathrm{p}_\nu(\mathfrak{z}\lceil_\nu)) \qquad \big) \\
\qquad \wedge\ \big(\sigma = \langle 3,\psi,\nu\rangle \ \wedge\ \mathit{Cond}_3(s,\psi,\nu) \ \rightarrow\ \quad \gamma_\psi(\mathfrak{s},\mathfrak{z}\lceil_\nu)\big) \qquad \Big]\ .
\end{array}$$

All these equivalences are provable in $\overline{\mathrm{BASIC}}$. The prenex form (9.1) is the one we fix for $s \in F(a)$.

We have implicitly used several independent quantifiers, i.e. we are reading $\mathfrak{z}$ as $[z_1,\ldots,z_k]$ where each variable z_i consists of k "slices" $\mathrm{p}_1(z_i)$, $\ldots$, $\mathrm{p}_k(z_i)$. Slice i is used for formulas of rank i. As D_a is an s.u.b. for all formulas we have to consider, we may assume w.l.o.g. that the slices in each $\mathfrak{z}_i$ are strictly bounded by D_a, and that quantification and Skolem functions also respect this. We could enforce this by adding further conditions to Ψ, but we refrain from doing so as it only makes the exposition less clear.

Based on the above prenex form of $s \in F(a)$, we now consider the Π^{b}_k-PLS conditions (3.1)-(3.5) for the fixed parameterised local search problem L, and we show that they have prenex forms which admit simple Skolem functions, provable in $\overline{\mathrm{BASIC}}$. We start with the simplest case first.

9.1 Π^{b}_k-PLS condition (3.4)

Condition (3.4) of a Π^{b}_k-PLS problem in general has the form

$$(\forall a,s)(N(a,s) \neq s \ \rightarrow\ c(a,N(a,s)) < c(a,s))\ .$$

As N and c are polynomial time functions, this condition is equivalent to a $\mathrm{s}\Pi^{\mathrm{b}}_1$-formula, so there is nothing to show.

9.2 Π^{b}_k-PLS condition (3.2)

This condition has the form

$$(\forall a)(i(a) \in F(a))$$

which, as we just showed, is equivalent to

$$(\forall a,\sigma)(\forall\!\!\!\exists^k\mathfrak{z})\Psi(a,i(a),\sigma,\mathfrak{z})$$

The latter obviously follows from the following stronger form:

$$(\forall a,\sigma)(\forall^k\mathfrak{z})\Psi(a,i(a),\sigma,\mathfrak{z}) \tag{9.2}$$

Theorem 9.2. (9.2) *is provable in* $\overline{\mathrm{BASIC}}$.

Proof. We argue in $\overline{\mathrm{BASIC}}$. Let $a, \sigma, \mathfrak{z}$ be given, and assume $\sigma = \langle j, \psi, \nu \rangle$. By definition, $i(a) = \left\langle h_a, \emptyset, 0^k \right\rangle$. The definition of L shows that $\left\langle h_a, \emptyset, 0^k \right\rangle \in C(a)$ and that $\mathrm{tp}(h_a) \neq \mathrm{Ax}_\psi$. We observe that $Cond_1(s, \psi, \nu)$ and $Cond_2(s, \psi, \nu)$ are false as $\Gamma(h_a) \subseteq \{(\exists y)\varphi(\underline{a}, y)\}$. For $j = 3$ we observe that $\mathfrak{s} = 0^k$ and $\gamma_\psi(0^k, \mathfrak{z}\lceil_{\mathrm{rk}(\psi)})$ is true by Theorem 8.4, 3 and Definition 8.6. Hence $\Psi(a, \left\langle h_a, \emptyset, 0^k \right\rangle, \sigma, \mathfrak{z})$ is true. □

9.3 Π^{b}_k-PLS condition (3.1)

This condition has the form

$$(\forall a, s)(s \in F(a) \ \rightarrow\ |s| \leq d(|a|))$$

which can be transformed equivalently over $\overline{\mathrm{BASIC}}$ in the following way:

$$\begin{aligned}
&(\forall a, s)(s \in F(a) \ \rightarrow\ |s| \leq d(|a|))\\
&\quad \Leftrightarrow \quad (\forall a, s)\big[(\forall \sigma)(\forall\!\exists^k \mathfrak{z})\Psi(a, s, \sigma, \mathfrak{z}) \ \rightarrow\ |s| \leq d(|a|)\big]\\
&\quad \Leftrightarrow \quad (\forall a, s)(\exists \sigma)(\exists\!\forall^k \mathfrak{z})\big[\Psi(a, s, \sigma, \mathfrak{z}) \ \rightarrow\ |s| \leq d(|a|)\big]
\end{aligned}$$

The latter obviously follows from the following stronger form:

$$(\forall a, s, \sigma)(\forall^k \mathfrak{z})\big[\Psi(a, s, \sigma, \mathfrak{z}) \ \rightarrow\ |s| \leq d(|a|)\big] \tag{9.3}$$

Theorem 9.3. (9.3) *is provable in* $\overline{\mathrm{BASIC}}$.

Proof. We argue in $\overline{\mathrm{BASIC}}$. Let $a, s, \sigma, \mathfrak{z}$ be given with $\Psi(a, s, \sigma, \mathfrak{z})$. If $s < D_a$ then obviously $|s| \leq d(|a|)$ by definition of d. Otherwise, $s \geq D_a$, and we obtain $s \in C(a)$ by definition of Ψ. Again we obtain $|s| \leq d(|a|)$ by construction of d as indicated in the proof of Proposition 7.4. □

9.4 Π^{b}_k-PLS condition (3.3)

This condition has the form

$$(\forall a, s)(s \in F(a) \ \rightarrow\ N(a, s) \in F(a)) \ .$$

Using the prenex form fixed in (9.1), this formula can be transformed equivalently over $\overline{\mathrm{BASIC}}$ in the following way:

$$\begin{aligned}
&(\forall a, s)(s \in F(a) \ \rightarrow\ N(a, s) \in F(a))\\
&\quad \Leftrightarrow \quad (\forall a, s)\big[(\forall \sigma)(\forall\!\exists^k \mathfrak{z})\Psi(a, s, \sigma, \mathfrak{z}) \ \rightarrow\ (\forall \bar{\sigma})(\forall\!\exists^k \bar{\mathfrak{z}})\Psi(a, N(a, s), \bar{\sigma}, \bar{\mathfrak{z}})\big]\\
&\quad \Leftrightarrow \quad (\forall a, s, \bar{\sigma}, \bar{z}_1)(\exists \sigma, z_1)(\forall z_2)(\exists \bar{z}_2)(\forall \bar{z}_3)(\exists z_3)(\forall z_4)\cdots\\
&\qquad\qquad \big[\Psi(a, s, \sigma, z_1, z_2, \dots) \ \rightarrow\ \Psi(a, N(a, s), \bar{\sigma}, \bar{z}_1, \bar{z}_2, \dots)\big]
\end{aligned} \tag{9.4}$$

Formula (9.4) is the prenex form which we fix for Condition (3.3).

Theorem 9.4. *The prenex formula* (9.4) *admits simple Skolem functions.*

Proof. We have to show that there are polynomial time functions

$$h_\sigma(a,s,\sigma,z_1),\ h_1(a,s,\sigma,z_1),\ h_2(a,s,\sigma,z_1,z_2),\ h_3(a,s,\sigma,z_1,z_2,z_3),\ \dots$$

such that S^1_2 proves

$$\begin{aligned}&(\forall a,s,\,\sigma,z_1,z_2,z_3,z_4,\dots)\\ &\qquad\big[\Psi(a,s,h_\sigma(a,s,\sigma,z_1),h_1(a,s,\sigma,z_1),z_2,h_3(\dots,z_3),z_4,\dots)\\ &\qquad\ \to\ \Psi(a,N(a,s),\sigma,z_1,h_2(\dots,z_2),z_3,h_4(\dots,z_4),\dots)\big]\end{aligned} \tag{9.5}$$

In the following we suppress the arguments a,s from the Skolem functions. We say that $h_\sigma(\sigma,z_1)$ (resp., $h_1(\sigma,z_1)$, $h_2(\sigma,z_1,z_2)$, $\dots$) is chosen *canonically* if $h_\sigma(\sigma,z_1)=\sigma$ (resp., $h_1(\sigma,z_1)=z_1$, $h_2(\sigma,z_1,z_2)=z_2$, $\dots$.)

Let $a,s,\sigma,z_1,z_2,z_3,\dots$ be given. We consider cases according to the definition of $N(a,s)$.

Let us start with some simple cases. Let $s=\big\langle h,f,0^k\big\rangle$, $\psi\notin\mathrm{s}\Pi^{\mathrm{b}}_0$ and $N(a,s)=\big\langle h[f(\psi)],f^r,0^k\big\rangle$ with $\mathrm{tp}(h)=\bigwedge_\psi$ and $0<\nu:=\mathrm{rk}(\psi)\le k$. If $\sigma\neq\langle 2,\psi[f(\psi)],\nu{-}1\rangle$ or $\mathit{Cond}_2(N(a,s),\psi[f(\psi)],\nu{-}1)$ is false, then choosing Skolem functions canonically obviously satisfies (9.5). So assume $\sigma=\langle 2,\psi[f(\psi)],\nu{-}1\rangle$ and $\mathit{Cond}_2(N(a,s),\psi[f(\psi)],\nu{-}1)$ is true. Choose $h_\sigma(\dots)=\langle 1,\psi,\nu\rangle$ and all other Skolem functions canonically. Then $\mathit{Cond}_1(s,\psi,\nu)$ is satisfied, and (9.5) is equivalent to

$$\neg\beta_\psi(f(\psi),\mathrm{p}_{\nu-1}([z_1,\dots,z_{\nu-1}]))\ \to\ \neg\beta_{\psi[f(\psi)]}(\mathrm{p}_{\nu-1}([z_1,\dots,z_{\nu-1}]))$$

which is obviously true.

Another simple case is if $s=\langle h,f,\mathfrak{s}\rangle$ and $N(a,s)=\langle h,f,N_\psi(\mathfrak{s})\rangle$ with $\mathrm{tp}(h)=\mathrm{Cut}_\psi$, $\nu:=\mathrm{rk}(\psi)$ and $N_\psi(\mathfrak{s})\neq\mathfrak{s}$. If $\sigma\neq\langle 3,\psi,\nu\rangle$ or $\mathit{Cond}_3(N(a,s),\psi,\nu)$ is false, then choosing Skolem functions canonically obviously satisfies (9.5). So assume $\sigma=\langle 3,\psi,\nu\rangle$ and $\mathit{Cond}_3(N(a,s),\psi,\nu)$ is true. Choose h_σ canonically. As $\mathit{Cond}_3(s,\psi,\nu)$ is obviously satisfied, (9.5) is equivalent to

$$\gamma_\psi(\mathfrak{s},h_1(\sigma,z_1),z_2,h_3(\dots),\dots)\ \to\ \gamma_\psi(N_\psi(\mathfrak{s}),z_1,h_2(\sigma,z_1,z_2),z_3,\dots)\ .$$

Choosing $h_1,h_2,\dots$ according to Theorem 8.5 will satisfy this implication.

We now list all non-trivial cases. In all other cases not mentioned here, choosing canonical Skolem functions immediately proves the assertion, as above. Let $s=\langle h,f,\mathfrak{s}\rangle$, then the following cases in the definition of $F(a,s)$ have to be considered:

1. $N(a,s)=\big\langle h[\epsilon(\psi)],f^r,0^k\big\rangle$ with $\mathrm{tp}(h)=\bigwedge_\psi$ and $\psi\in\mathrm{s}\Pi^{\mathrm{b}}_0$.

2. $N(a,s)=\big\langle h[0],f',0^k\big\rangle$ with $\mathrm{tp}(h)=\bigvee^i_\psi$, $\psi\notin\mathrm{s}\Sigma^{\mathrm{b}}_1$, $N_{\psi[i]}(\mathfrak{s})=\mathfrak{s}$, $\mathfrak{s}\notin A_{\psi[i]}$ and $f'=(f\cup\{\psi[i]\mapsto\mathfrak{s}_1\})^r$.

3. $N(a,s) = i$ with $\mathrm{tp}(h) = \bigvee^{i}_{(\exists y)\varphi(\underline{a},y)}$, $N_{\varphi(\underline{a},\underline{i})}(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \in A_{\varphi(\underline{a},\underline{i})}$.

4. $N(a,s) = \langle h[1], f^r, 0^k \rangle$ with $\mathrm{tp}(h) = \mathrm{Cut}_{\psi}$, $\psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0$, $N_{\psi}(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \in A_{\psi}$.

5. $N(a,s) = \langle h[0], f', 0^k \rangle$ with $\mathrm{tp}(h) = \mathrm{Cut}_{\psi}$, $\psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0$, $N_{\psi}(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \notin A_{\psi}$, and $f' = (f \cup \{\psi \mapsto \mathfrak{s}_1\})^r$.

We will now study these cases one by one, thereby considering only critical sub-cases; for all other sub-cases the canonical choices for Skolem functions will already satisfy (9.5).

Case 1. $N(a,s) = \langle h[\epsilon(\psi)], f^r, 0^k \rangle$ with $\mathrm{tp}(h) = \bigwedge_{\psi}$ and $\psi \in \mathrm{s}\Pi^{\mathrm{b}}_0$. If $\sigma = \langle 2, \psi[\epsilon(\psi)], 0 \rangle$ such that $\mathit{Cond}_2(N(a,s), \psi[\epsilon(\psi)], 0)$ is true, we choose $h_{\sigma}(\sigma, \dots) = \langle 2, \psi, 0 \rangle$ and all other Skolem functions canonically. Then (9.5) is equivalent to $\neg\beta_{\psi} \rightarrow \neg\beta_{\psi[\epsilon(\psi)]}$ which is satisfied by definition of $\epsilon(\psi)$, cf. Definition 7.2.

Case 2. $N(a,s) = \langle h[0], f', 0^k \rangle$ with $\mathrm{tp}(h) = \bigvee^{i}_{\psi}$, $\psi \notin \mathrm{s}\Sigma^{\mathrm{b}}_1$, $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \notin A_{\psi[i]}$ and $f' = f^r \cup \{\psi[i] \mapsto \mathfrak{s}_1\}$. In this case we have that ψ is of the form $(\exists\forall^{\nu}\mathfrak{z})\beta_{\psi}(\mathfrak{z})$ with $\nu \geq 2$. Assume $\sigma = \langle 1, \psi[i], \nu{-}1 \rangle$ and $\mathit{Cond}_1(N(a,s), \psi[i], \nu{-}1)$. Let $j := \mathfrak{s}_1$, then $f'(\psi[i]) = j$.

If $\nu = 2$ then $\mathfrak{s} \notin A_{\psi[i]}$ implies $\neg\psi[i][j]$, thus $\neg\beta_{\psi[i][j]}$. In this situation, the conclusion of (9.5) is of the form $\neg\beta_{\psi[i][j]}$ which is true. Hence, any choice of Skolem functions will satisfy (9.5).

Now assume $\nu > 2$. Choose $h_{\sigma}(\sigma, \dots) = \langle 3, \psi[i], \nu{-}1 \rangle$ and all other Skolem functions canonically. $\mathit{Cond}_3(s, \psi[i], \nu{-}1)$ is obviously satisfied, thus (9.5) is equivalent to

$$\gamma_{\psi[i]}(\mathfrak{s}, z_1, z_2, \dots) \rightarrow \neg\beta_{\psi[i][j]}(\mathfrak{t})$$

with $\mathfrak{t} = \mathrm{p}_{\nu-2}([z_1, z_2, z_3, \dots])$. Assume $\gamma_{\psi[i]}(\mathfrak{s}, z_1, z_2, \dots)$. Theorem 8.4, 5, shows, as $\mathrm{rk}(\psi[i]) = \nu{-}1$ and $\mathrm{tp}(\psi[i]) = \bigwedge$, that $\mathrm{p}_{\nu-2}(z_1) < \mathfrak{s}_2 \rightarrow \neg\beta_{\psi[i]}(\mathfrak{s}_1, \mathfrak{t})$. As $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \notin A_{\psi[i]}$ and $\mathrm{tp}(\psi[i]) = \bigwedge$, we have $\mathfrak{s}_2 = D_a$ by Corollary 6.14, 1. Hence the latter implies $\neg\beta_{\psi[i]}(\mathfrak{s}_1, \mathfrak{t})$ which is the same as $\neg\beta_{\psi[i][j]}(\mathfrak{t})$.

Case 3. $N(a,s) = i$ with $\mathrm{tp}(h) = \bigvee^{i}_{(\exists y)\varphi(\underline{a},y)}$, $N_{\varphi(\underline{a},\underline{i})}(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \in A_{\varphi(\underline{a},\underline{i})}$. We have that $\varphi(\underline{a}, \underline{i})$ is of the form $(\forall\exists^{\ell}\mathfrak{z})\beta_{\varphi(\underline{a},\underline{i})}(\mathfrak{z})$.

If $\ell = 0$ then $\mathfrak{s} \in A_{\varphi(\underline{a},\underline{i})}$ implies $\varphi(\underline{a}, \underline{i})$, which is the same as $\beta_{\varphi(\underline{a},\underline{i})}$. This implies the succedent of (9.5), which is of the form $\beta_{\varphi}(a, i)$.

If $\ell > 0$, choose $h_{\sigma}(\sigma, \dots) = \langle 3, \varphi(\underline{a}, \underline{i}), \ell \rangle$ and all other Skolem functions canonically. $\mathit{Cond}_3(s, \varphi(\underline{a}, \underline{i}), \ell)$ is obviously satisfied, thus (9.5) is equivalent to

$$\gamma_{\varphi(\underline{a},\underline{i})}(\mathfrak{s}, z_1, z_2, \dots) \rightarrow \beta_{\varphi(\underline{a},\underline{i})}(\mathfrak{t})$$

with $\mathfrak{t} = \mathrm{p}_\ell([z_1, z_2, z_3, \ldots])$. Assume $\gamma_{\varphi(\underline{a},\underline{i})}(\mathfrak{s}, z_1, z_2, \ldots)$. As $\mathrm{rk}(\varphi) = \ell$ and $\mathrm{tp}(\varphi) = \bigwedge$, Theorem 8.4, 4, shows $\mathrm{p}_\ell(z_1) < \mathfrak{s}_1 \rightarrow \beta_{\varphi(\underline{a},\underline{i})}(\mathfrak{t})$. As $N_{\varphi(\underline{a},\underline{i})}(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \in A_{\varphi(\underline{a},\underline{i})}$ and $\mathrm{tp}(\varphi(\underline{a}, \underline{i})) = \bigwedge$, we have $\mathfrak{s}_1 = D_a$ by Corollary 6.14, 2. Hence the latter implies $\beta_{\varphi(\underline{a},\underline{i})}(\mathfrak{t})$.

Case 4. $N(a, s) = \langle h[1], f^r, 0^k \rangle$ with $\mathrm{tp}(h) = \mathrm{Cut}_\psi$, $N_\psi(\mathfrak{s}) = \mathfrak{s}$ and $\mathfrak{s} \in A_\psi$. We have that $\psi \equiv (\forall\exists^\nu \mathfrak{z})\beta_\psi(\mathfrak{z})$ for $\nu = \mathrm{rk}(\psi)$. Assume $\sigma = \langle 2, \neg\psi, \nu \rangle$ and $\mathit{Cond}_2(N(a, s), \neg\psi, \nu)$ is true.

If $\nu = 0$ choose Skolem functions arbitrarily. Then, the conclusion of (9.5) is equivalent to β_ψ, which is satisfied because $\mathfrak{s} \in A_\psi$ already implies ψ which is the same as β_ψ.

Now assume $\nu > 0$, and choose $h_\sigma(\sigma, \ldots) = \langle 3, \psi, \nu \rangle$ and all other Skolem functions canonically. $\mathit{Cond}_3(s, \psi, \nu)$ is obviously satisfied. Then (9.5) is equivalent to

$$\gamma_\psi(\mathfrak{s}, z_1, z_2, \ldots) \rightarrow \beta_\psi(\mathfrak{t})$$

with $\mathfrak{t} = \mathrm{p}_\nu([z_1, z_2, z_3, \ldots])$. Assume $\gamma_\psi(\mathfrak{s}, z_1, z_2, \ldots)$. As $\mathrm{rk}(\psi) = \nu$ and $\mathrm{tp}(\psi) = \bigwedge$, Theorem 8.4, 4, shows $\mathrm{p}_\nu(z_1) < \mathfrak{s}_1 \rightarrow \beta_\psi(\mathfrak{t})$. By assumption $N_\psi(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \in A_\psi$ and $\mathrm{tp}(\psi) = \bigwedge$, so $\mathfrak{s}_1 = D_a$ by Corollary 6.14, 2. Hence $\beta_\psi(\mathfrak{t})$ follows.

Case 5. $N(a, s) = \langle h[0], f', 0^k \rangle$ with $\mathrm{tp}(h) = \mathrm{Cut}_\psi$, $\psi \notin \mathrm{s}\Pi^{\mathrm{b}}_0$, $N_\psi(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \notin A_\psi$, and $f' = (f \cup \{\psi \mapsto \mathfrak{s}_1\})^r$. We have that $\psi \equiv (\forall\exists^\nu \mathfrak{z})\beta_\psi(\mathfrak{z})$ for $\nu = \mathrm{rk}(\psi)$, and $\nu > 0$. Let $j := \mathfrak{s}_1$.

If $\nu = 1$, the assumption $\mathfrak{s} \notin A_\psi$ implies $\neg\psi[\mathfrak{s}_1]$ which is $\neg\beta_{\psi[j]}$. Now the critical case is $\sigma = \langle 1, \psi, 1 \rangle$, when the conclusion of (9.5) has the form $\neg\beta_{\psi[f(\psi)]}$ which is the same as $\neg\beta_{\psi[j]}$ and satisfied. Arbitrary choices for Skolem functions will satisfy (9.5).

Now assume $\nu > 1$. The critical case now is that $\sigma = \langle 1, \psi, \nu \rangle$ and that $\mathit{Cond}_1(N(a, s), \psi, \nu)$ is true, that is $\psi \in \mathrm{dom}(f')$, and $f'(\psi) = j$ by definition. Choose $h_\sigma(\sigma, \ldots) = \langle 3, \psi, \nu \rangle$ and all other Skolem functions canonically. $\mathit{Cond}_3(s, \psi, \nu)$ is obviously satisfied. Then (9.5) is equivalent to

$$\gamma_\psi(\mathfrak{s}, z_1, z_2, \ldots) \rightarrow \neg\beta_{\psi[j]}(\mathfrak{t})$$

with $\mathfrak{t} = \mathrm{p}_{\nu-1}([z_1, z_2, z_3, \ldots])$, as $j = f(\psi)$. Assume $\gamma_\psi(\mathfrak{s}, z_1, z_2, \ldots)$. As $\mathrm{tp}(\psi) = \bigwedge$ and $\mathrm{rk}(\psi) = \nu$, Theorem 8.4, 5, shows $\mathrm{p}_{\nu-1}(z_1) < \mathfrak{s}_2 \rightarrow \neg\beta_\psi(\mathfrak{s}_1, \mathfrak{t})$. As $N_\psi(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \notin A_\psi$ and $\mathrm{tp}(\psi) = \bigwedge$, we have $\mathfrak{s}_2 = D_a$ by Corollary 6.14, 1. Hence $\neg\beta_\psi(\mathfrak{s}_1, \mathfrak{t})$ follows, which is the same as $\neg\beta_{\psi[j]}(\mathfrak{t})$. □

9.5 Π^{b}_k-PLS condition (3.5)

Condition (3.5) can be divided into two parts which we consider independently:

$$(\forall a, s)(s \in G(a) \rightarrow (N(a, s) = s \wedge s \in F(a))) \tag{9.6}$$

and

$$(\forall a, s)((N(a,s) = s \ \wedge\ s \in F(a)) \ \rightarrow\ s \in G(a)) \tag{9.7}$$

The goal set $G(a)$ is given as the set of all $s < D_a$ with $\varphi(a,s)$. Using the prenex form fixed for φ according to Definition 9.1, and the prenex form fixed for $s \in F(a)$ in (9.1), formula (9.6) can be transformed equivalently as follows, provably in $\overline{\text{BASIC}}$:

$$\begin{aligned}
&(\forall a, s)\big(s \in G(a) \ \rightarrow\ (N(a,s) = s \ \wedge\ s \in F(a))\big) \\
&\quad\Leftrightarrow\quad (\forall a, s)\big(s < D_a \ \wedge\ (\forall\exists^{\ell}\mathfrak{z})\beta_{\varphi}(a, s, \mathrm{p}_{\ell}(\mathfrak{z})) \\
&\qquad\qquad\qquad \rightarrow\ N(a,s) = s \ \wedge\ (\forall\sigma)(\forall\exists^{k}\bar{\mathfrak{z}})\Psi(a, s, \sigma, \bar{\mathfrak{z}})\big) \\
&\quad\Leftrightarrow\quad (\forall a, s)(\forall\sigma)(\forall\bar{z}_1)(\exists z_1)(\forall z_2)(\exists\bar{z}_2)\cdots \\
&\qquad\qquad\qquad \big(s < D_a \ \wedge\ \beta_{\varphi}(a, s, \mathrm{p}_{\ell}([z_1, z_2, \ldots])) \\
&\qquad\qquad\qquad\qquad \rightarrow\ N(a,s) = s \ \wedge\ \Psi(a, s, \sigma, \bar{z}_1, \bar{z}_2, \ldots)\big) \ .
\end{aligned}$$

The latter assertion obviously follows from the following stronger one:

$$\begin{aligned}
&(\forall a, s, \sigma, z_1, z_2, z_3, \ldots)\big(s < D_a \ \wedge\ \beta_{\varphi}(a, s, \mathrm{p}_{\ell}([z_1, z_2, \ldots])) \\
&\qquad\qquad \rightarrow\ N(a,s) = s \ \wedge\ \Psi(a, s, \sigma, z_1, z_2, \ldots)\big) \ .
\end{aligned} \tag{9.8}$$

We show that (9.8) is provable in S^1_2.

Theorem 9.5. S^1_2 *proves* (9.8).

Proof. We argue in S^1_2. Let $a, s, \sigma, z_1, z_2, z_3, \ldots$ be given, and assume $s < D_a$ and $\beta_{\varphi}(a, s, \mathrm{p}_{\ell}([z_1, z_2, \ldots]))$. Hence, $N(a,s) = s$ by definition of N, and $\Psi(a, s, \sigma, z_1, z_2, \ldots)$ by definition of Ψ. □

We now turn to condition (9.7). Instead of working directly with this condition we split it into two according to whether $s < D_a$ or not, and simplify the resulting conditions according to their meaning.

$$(\forall a, s)((N(a,s) = s \ \wedge\ s < D_a \ \wedge\ s \in F(a)) \ \rightarrow\ s \in G(a)) \tag{9.9}$$

and

$$(\forall a, s)((N(a,s) = s \ \wedge\ s \geq D_a \ \rightarrow\ s \notin F(a))) \tag{9.10}$$

We observe that (9.9) and (9.10) together imply (9.7) in $\overline{\text{BASIC}}$.

We consider conditions (9.9) and (9.10) in turn. The former is straight forward to deal with. We transform (9.9) equivalently as follows, provable in $\overline{\mathrm{BASIC}}$:

$$\begin{aligned}
&(\forall a, s)\big((N(a,s) = s \ \wedge\ s < D_a \ \wedge\ s \in F(a)) \ \rightarrow\ s \in G(a)\big) \\
&\quad\Leftrightarrow\quad (\forall a, s)\big(N(a,s) = s \ \wedge\ s < D_a \ \wedge\ (\forall\sigma)(\forall\exists^k \mathfrak{z})\Psi(a, s, \sigma, \mathfrak{z}) \\
&\qquad\qquad \rightarrow\ (\forall\exists^\ell \bar{\mathfrak{z}})\beta_\varphi(a, s, \mathrm{p}_\ell(\bar{\mathfrak{z}}))\big) \\
&\quad\Leftrightarrow\quad (\forall a, s)(\forall \bar{z}_1)(\exists\sigma)(\exists z_1)\ (\forall z_2)(\exists \bar{z}_2)\ (\forall \bar{z}_3)(\exists z_3)\ (\forall z_4)(\exists \bar{z}_4)\ \dots \\
&\qquad\qquad\quad \big(N(a,s) = s \ \wedge\ s < D_a \ \wedge\ \Psi(a, s, \sigma, z_1, z_2, z_3, \dots) \\
&\qquad\qquad\qquad \rightarrow\ \beta_\varphi(a, s, \mathrm{p}_\ell([\bar{z}_1, \bar{z}_2, \bar{z}_3, \dots]))\big)\ .
\end{aligned}$$

The latter is the prenex form which we fix for (9.9). We now show that this prenex form admits simple Skolem functions.

Theorem 9.6. *The prenex form fixed for* (9.9) *admits simple Skolem functions.*

Proof. We have to show that there are polynomial time functions

$$h^\sigma(a, s, z_1),\ h_1(a, s, z_1),\ h_2(a, s, z_1, z_2),\ h_3(a, s, z_1, z_2, z_3),\ \dots$$

such that the following is provable in S^1_2:

$$\begin{aligned}
&(\forall a,\ s, z_1, z_2, z_3, z_4, \dots)\big(N(a,s) = s \ \wedge\ s < D_a \\
&\quad \wedge\ \Psi(a, s, h^\sigma(a, s, z_1), h_1(a, s, z_1), z_2, h_3(\dots, z_3), \dots) \\
&\quad \rightarrow\ \beta_\varphi(a, s, \mathrm{p}_\ell([z_1, h_2(a, s, z_1, z_2), z_3, h_4(\dots, z_4), \dots]))\big)\ .
\end{aligned} \tag{9.11}$$

We argue in S^1_2. Let $a, s, z_1, z_2, z_3, z_4, \dots$ be given with $N(a,s) = s$ and $s < D_a$. Choose $h^\sigma(\dots) = 0$, and all other Skolem functions canonically. Assume $\Psi(a, s, 0, z_1, z_2, z_3, z_4 \dots)$, then $\beta_\varphi(a, s, \mathrm{p}_\ell([z_1, z_2, z_3, z_4, \dots]))$ follows by definition of $\Psi(a, s, 0, 0, z_1, z_2, z_3, z_4 \dots)$ as $s < D_a$. □

We now turn to condition (9.10) to transform it into a suitable prenex form. This is not at all obvious because the canonical prenex form does not admit simple Skolem functions. The premise of the implication is of low complexity and can be ignored for the prenex form and later the Skolemisation. The only relevant part is the formula "$s {\notin} F(a)$". First, we double this part to the formula "$s {\notin} F(a) \vee s {\notin} F(a)$" to obtain two independent sets of quantifiers. This step is inessential and could have been incorporated already in the prenex form that we fixed for "$s {\notin} F(a)$". In the second step, we pull out quantifiers, but not in the canonical way (that is those of the same level at the same time, putting universal before existential ones.) Instead, we first pull out the first $(\exists, \forall)$ quantifier pair of the first "$s {\notin} F(a)$", followed by the first $(\exists, \forall)$ pair of the second "$s {\notin} F(a)$". Then comes the second $(\exists, \forall)$ pair of the first "$s {\notin} F(a)$", followed by the second $(\exists, \forall)$ pair of the second "$s {\notin} F(a)$", and so on. As "$s {\notin} F(a)$" is of rank k, we produce in this way a prenex formula of rank $2k$, where the canonical prenex form would be of rank k. Thus, we transform (9.10) equivalently as follows, provable in $\overline{\text{BASIC}}$, where the very last equivalence just renames variables:

$$\begin{aligned}
&(\forall a,s)\big((N(a,s)=s \ \wedge\ s\geq D_a \ \rightarrow\ s\notin F(a))\big)\\
&\quad\Leftrightarrow\quad (\forall a,s)\big((N(a,s)=s \ \wedge\ s\geq D_a \ \rightarrow\ s\notin F(a)\ \vee\ s\notin F(a))\big)\\
&\quad\Leftrightarrow\quad (\forall a,s)\big(N(a,s)=s \ \wedge\ s\geq D_a \ \rightarrow\ (\exists\sigma^1)(\exists\!\forall^k\mathfrak{z}^1)\neg\Psi(a,s,\sigma^1,\mathfrak{z}^1)\\
&\qquad\qquad\quad \vee\ (\exists\sigma^2)(\exists\!\forall^k\mathfrak{z}^2)\neg\Psi(a,s,\sigma^2,\mathfrak{z}^2)\big)\\
&\quad\Leftrightarrow\quad (\forall a,s)(\exists\sigma^1,\sigma^2)(\exists z^1_1)\\
&\qquad\quad (\forall z^1_2)(\exists z^2_1)\ (\forall z^2_2)(\exists z^1_3)\ (\forall z^1_4)(\exists z^2_3)\ \cdots\\
&\qquad\qquad \big(N(a,s)=s \ \wedge\ s\geq D_a \ \rightarrow\ \neg\Psi(a,s,\sigma^1,z^1_1,z^1_2,z^1_3,\dots)\\
&\qquad\qquad\quad \vee\ \neg\Psi(a,s,\sigma^2,z^2_1,z^2_2,z^2_3,\dots)\big)\\
&\quad\Leftrightarrow\quad (\forall a,s)(\exists\sigma^1,\sigma^2)(\exists z^1_1)\\
&\qquad\quad (\forall z^1_2)(\exists z^2_2)\ (\forall z^2_3)(\exists z^1_3)\ (\forall z^1_4)(\exists z^2_4)\ \cdots\\
&\qquad\qquad \big(N(a,s)=s \ \wedge\ s\geq D_a \ \rightarrow\ \neg\Psi(a,s,\sigma^1,z^1_1,z^1_2,z^1_3,\dots)\\
&\qquad\qquad\quad \vee\ \neg\Psi(a,s,\sigma^2,z^2_2,z^2_3,z^2_4,\dots)\big)\ .
\end{aligned}$$

The latter is the prenex form which we fix for (9.10). We now show that this prenex form admits simple Skolem functions.

Theorem 9.7. *The prenex form fixed for* (9.10) *admits simple Skolem functions.*

Proof. We have to show that there are polynomial time functions

$$\begin{aligned}
&h^{\sigma^1}(a,s),\ h^{\sigma^2}(a,s),\\
&h_1(a,s),\ h_2(a,s,z_2),\ h_3(a,s,z_2,z_3),\ h_4(a,s,z_2,z_3,z_4),\ \dots
\end{aligned}$$

such that the following is provable in S^1_2:

$$\begin{aligned}
&(\forall a,\,s,z_2,z_3,z_4,\dots)\big(N(a,s)=s \ \wedge\ s\geq D_a\\
&\qquad \rightarrow\ \neg\Psi(a,s,h^{\sigma^1}(a,s),h_1(a,s),z_2,h_3(a,s,z_2,z_3),\dots)\\
&\qquad\quad \vee\ \neg\Psi(a,s,h^{\sigma^2}(a,s),h_2(a,s,z_2),z_3,h_4(\dots,z_4),\dots)\big)\ .
\end{aligned} \tag{9.12}$$

We argue in S^1_2. Let $a,s,z_2,z_3,z_4,\dots$ be given with $N(a,s)=s$ and $s\geq D_a$. Then $N(a,s)=s$ implies by definition of N that $s=\langle h,f,\mathfrak{s}\rangle$, $\mathrm{tp}(h)=\bigvee^i_\psi$, $\nu:=\mathrm{rk}(\psi[i])>0$, $N_{\psi[i]}(\mathfrak{s})=\mathfrak{s}$, $\mathfrak{s}\in A_{\psi[i]}$ and $\psi\not\equiv(\exists y)\varphi(\underline{a},y)$. Choose $h^{\sigma^1}(a,s)=\langle 2,\psi,\nu{+}1\rangle$, $h^{\sigma^2}(a,s)=\langle 3,\psi[i],\nu\rangle$, $\mathrm{p}_{\nu+1}(h_1(a,s))=i$,

$$\mathrm{p}_\nu(h_j(\dots,z_j))=\mathrm{p}_{\nu+1}(z_j) \qquad\qquad \mathrm{p}_{\nu+1}(h_j(\dots,z_j))=\mathrm{p}_\nu(z_j)$$

for $j=2,\dots,k$, and all remaining slices canonically. Let

$$\mathfrak{t}:=[\mathrm{p}_{\nu+1}(z_2),\mathrm{p}_\nu(z_3),\mathrm{p}_{\nu+1}(z_4),\mathrm{p}_\nu(z_5),\dots]$$

then we have

$$\begin{aligned}
\mathrm{p}_{\nu+1}([h_1(a,s), z_2, h_3(a,s,z_2,z_3), \ldots]) &= [i, \mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3, \ldots] && (9.13)\\
\mathrm{p}_{\nu}([h_2(a,s,z_2), z_3, h_4(\ldots, z_4), \ldots]) &= [\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3, \ldots] && (9.14)
\end{aligned}$$

Now, (9.12) is equivalent to

$$\begin{aligned}
&\neg\Psi(a,\, s, \langle 2, \psi, \nu{+}1\rangle\,, h_1(a,s), z_2, h_3(a,s,z_2,z_3), \ldots\,)\\
&\qquad \vee\ \neg\Psi(a, s, \langle 3, \psi[i], \nu\rangle\,, h_2(a,s,z_2), z_3, h_4(\ldots, z_4), \ldots\,)\\
\Leftrightarrow\quad & \beta_\psi(\mathrm{p}_{\nu+1}([h_1(a,s), z_2, h_3(a,s,z_2,z_3), \ldots]))\\
&\qquad\quad \vee\ \neg\gamma_{\psi[i]}(\mathfrak{s}, h_2(a,s,z_2), z_3, h_4(\ldots, z_4), \ldots\,)\\
\Leftrightarrow\quad & \beta_\psi(i, \mathfrak{t}{\restriction}_\nu)\ \vee\ \neg\gamma_{\psi[i]}(\mathfrak{s}, h_2(a,s,z_2), z_3, h_4(\ldots, z_4), \ldots\,) && (9.15)
\end{aligned}$$

using (9.13) for the last equivalence. To show the last statement (9.15), assume $\gamma_{\psi[i]}(\mathfrak{s}, h_2(a,s,z_2), z_3, h_4(\ldots, z_4), \ldots\,)$. As $\mathrm{tp}(\psi[i]) = \bigwedge$ and $\mathrm{rk}(\psi[i]) = \nu$, Theorem 8.4, 4, shows

$$\mathrm{p}_\nu(h_2(\ldots, z_2)) < \mathfrak{s}_1 \ \rightarrow\ \beta_{\psi[i]}(\mathfrak{t}{\restriction}_\nu)$$

using (9.14). Now, $N_{\psi[i]}(\mathfrak{s}) = \mathfrak{s}$, $\mathfrak{s} \in A_{\psi[i]}$ and $\mathrm{tp}(\psi[i]) = \bigwedge$ show $\mathfrak{s}_1 = D_a$ by Corollary 6.14, 2. Hence, the latter implies $\beta_{\psi[i]}(\mathfrak{t}{\restriction}_\nu)$ which is the same as $\beta_\psi(i, \mathfrak{t}{\restriction}_\nu)$. □

The next Corollary summarises the results obtained in this section.

Corollary 9.8. *Let $0 \leq \ell \leq k$. The $\Sigma^{\mathrm{b}}_{\ell+1}$-definable total search problems in T^{k+1}_2 can be characterised by some Π^{b}_k-PLS problems with Π^{b}_ℓ-goals, such that conditions* (3.1)–(3.5) *have prenex forms (over $\overline{\mathrm{BASIC}}$) which admit simple Skolem functions.*

10 A Proposed Hard Principle for T^k_2

The separation problem of Bounded Arithmetic, i.e. the question whether the hierarchy of Bounded Arithmetic theories is strict or not, is one of the central problems in this area, due to the connections of Bounded Arithmetic theories to complexity classes. There are several ways to approach the separation question. One path which is followed in current research, is by studying relativised theories. Relativised Bounded Arithmetic theories can be obtained by adding one unspecified set variable α to the language of Bounded Arithmetic, which counts as a new atomic formula and is allowed in $\mathrm{s}\Sigma^{\mathrm{b}}_k(\alpha)$-formulas and in induction formulas. Relativised separations have been obtained between all relativised Bounded Arithmetic theories [KPT91, Bus95, Zam96, Jeř09], the goal in current research is to improve the separations, ultimately to find $\forall\Sigma^{\mathrm{b}}_1(\alpha)$ principles which separate the theories, or even $\forall\Pi^{\mathrm{b}}_1(\alpha)$ principles — $\forall\Pi^{\mathrm{b}}_1$ is the complexity of consistency statements.

In this section we will derive, for each k, a generic $\forall\Sigma^{\mathrm{b}}_1(\alpha)$ principle from the results of the previous sections, and show that it gives rise to a class of $\forall\Sigma^{\mathrm{b}}_1$ formulas which characterise the $\forall\Sigma^{\mathrm{b}}_1$ consequences of T^{k+1}_2. The generic form of the principle is therefore conjectured to separate $\mathrm{T}^{k+1}_2(\alpha)$ from $\mathrm{T}^{k}_2(\alpha)$. Such generic principles are well-known in the literature. We will briefly discuss later the relation of the principle which we will define here to the game principles defined in [ST07].

Fix $k \geq 0$. The Skolemisation of the Π^{b}_k-PLS conditions from the previous section forms the basis for the generic $\forall\mathrm{s}\Sigma^{\mathrm{b}}_1(\alpha)$-principle which we will denote by $\mathcal{P}_k$. We replace the polynomial time functions and predicates in the Skolemised versions of (3.1)-(3.5) from the previous section by new function and predicate symbols in the following way: Let N, c, i be new function symbols which will be used for the neighbourhood function, the cost function, and the initial value function respectively. Let G, F' be new relation symbols, where G is binary and is used for the goal set, and F' is $k{+}2$-ary and represents $\Psi(a, s, \sigma, z_1, z_2, \ldots, z_k)$ from the prenex form (9.1) fixed for $s \in F(a)$ in the previous section. Let b be a parameter, and let $a = \mathrm{p}_1(b)$, $a_1 = \mathrm{p}_1(\mathrm{p}_2(b))$ and $a_2 = \mathrm{p}_2(\mathrm{p}_2(b))$. We assume $D_a = a_1$, and that a_2 serves as a bound for all quantifiers. The Skolemised versions of (3.1)-(3.5) read as follows — strictly speaking, $(3.1)^{\mathrm{SK}}$ below is not the Skolemisation of (3.1), but a reformulation and adaptation to the current setting, as the original (3.1) is unsuitable. We take b as a parameter to these formulas, from which a, a_1 and a_2 can be computed.

$(3.1)^{\mathrm{SK}}$
$$i(a) < a_2 \ \wedge\ (\forall s < a_2)(N(a, s) < a_2)$$

$(3.2)^{\mathrm{SK}}$
$$(\forall \sigma, z_1, \ldots, z_k < a_2) F'(a, i(a), \sigma, z_1, \ldots, z_k)$$

$(3.3)^{\mathrm{SK}}$
$$\begin{aligned} &(\forall s, \sigma, z_1, \ldots, z_k < a_2)\\ &\quad (F'(a, s, h_\sigma(a, s, \sigma, z_1), h_1(a, s, \sigma, z_1), z_2, h_3(a, s, \sigma, z_1, z_2, z_3), \ldots)\\ &\quad\ \rightarrow\ F'(a, N(a, s), \sigma, z_1, h_2(a, s, \sigma, z_1, z_2), z_3, h_4(\ldots, z_4), \ldots)) \end{aligned}$$

$(3.4)^{\mathrm{SK}}$
$$(\forall s < a_2)(N(a, s) = s \ \vee\ c(a, N(a, s)) < c(a, s))$$

$(3.5\mathrm{a})^{\mathrm{SK}}$
$$\begin{aligned} &(\forall s, z_1, z_2, \ldots, z_k < a_2)(N(a, s) = s \ \wedge\ s < a_1\\ &\quad \wedge\ F'(a, s, 0, z_1, z_2, z_3, \ldots) \ \rightarrow\ G(a, s)) \end{aligned}$$

$(3.5\mathrm{b})^{\mathrm{SK}}$
$$\begin{aligned} &(\forall s, z_2, \ldots, z_k, z_{k+1} < a_2)(N(a, s) = s \ \wedge\ s \geq a_1\\ &\quad \rightarrow\ \neg F'(a, s, g_{\sigma,1}(a, s), g_1(a, s), z_2, g_3(a, s, z_2, z_3), \ldots)\\ &\qquad \vee\ \neg F'(a, s, g_{\sigma,2}(a, s), g_2(a, s, z_2), z_3, g_4(\ldots, z_4), \ldots)) \end{aligned}$$

where $h_\sigma, h_1, h_2, \ldots$ and $g_{\sigma,1}, g_{\sigma,2}, g_1, g_2, \ldots$ are further function symbols representing polynomial time Skolem functions. We have used only one direction of the equivalence in the Skolemisation of (3.5), as we only need this one to prove the principle $\mathcal{P}_k$. This direction comes in two parts, $(3.5\mathrm{a})^{\mathrm{SK}}$ and $(3.5\mathrm{b})^{\mathrm{SK}}$.

Let $\mathcal{X}$ be the list of new function and predicate symbols, that is

$$\mathcal{X} = G, F', N, c, i, h_\sigma, h_1, h_2, \ldots, g_{\sigma,1}, g_{\sigma,2}, g_1, g_2, \ldots$$

Observe that $(3.1)^{\mathrm{SK}}$-$(3.5\mathrm{b})^{\mathrm{SK}}$ are all $\mathrm{s}\Pi^{\mathrm{b}}_1(\mathcal{X})$-formulas. Then the principle $\mathcal{P}_k(\mathcal{X})$ is given by the $\forall\mathrm{s}\Sigma^{\mathrm{b}}_1(\mathcal{X})$-formula obtained from

$$(\forall b)(a_1 < a_2 \ \wedge\ (3.1)^{\mathrm{SK}} \ \wedge\ \cdots \ \wedge\ (3.5\mathrm{b})^{\mathrm{SK}} \ \rightarrow\ (\exists s < a) G(a, s)) \qquad (10.1)$$

by turning the independent bounded existential quantifiers into one using the pairing function and its bound $B(z)$. We observe that the shape of $\mathcal{P}_k$ depends on k.

Theorem 10.1. $\mathrm{T}^{k+1}_2(\mathcal{X}) \vdash \mathcal{P}_k(\mathcal{X})$

Proof. The proof is similar to that of Theorem 3.4. We argue in $\mathrm{T}^{k+1}_2(\mathcal{X})$. Let b be given, Let $a = \mathrm{p}_1(b)$, $a_1 = \mathrm{p}_1(\mathrm{p}_2(b))$ and $a_2 = \mathrm{p}_2(\mathrm{p}_2(b))$. Assume that $a_1 < a_2$, and that $(3.1)^{\mathrm{SK}}$-$(3.5\mathrm{b})^{\mathrm{SK}}$ are satisfied. Let $s \in F(b)$ denote the formula

$$s < a_2 \ \wedge\ (\forall \sigma{<}a_2)(\forall z_1{<}a_2)(\exists z_2{<}a_2) \cdots F'(a, s, \sigma, z_1, z_2, \ldots, z_k) \ .$$

Consider the set $X := \{c(a, s) \colon s < a_2 \ \wedge\ s \in F(b)\}$. This set can be described by some $\mathrm{s}\Sigma^{\mathrm{b}}_{k+1}(\mathcal{X})$-formula. By $(3.1)^{\mathrm{SK}}$ and $(3.2)^{\mathrm{SK}}$ we have $c(a, i(a)) \in X$. As $\mathrm{T}^{k+1}_2(\mathcal{X})$ proves minimisation for $\mathrm{s}\Sigma^{\mathrm{b}}_{k+1}(\mathcal{X})$-properties, we can find some $c \in X$ which is minimal in X. Choose $s < a_2$ and $s \in F(b)$ with $c = c(a, s)$.

As $(3.3)^{\mathrm{SK}}$ is derived from the Skolemisation of a prenex form for (3.3), we obtain $s \in F(b) \ \rightarrow\ N(a, s) \in F(b)$. Thus $N(a, s) \in F(b)$. Also $N(a, s) < a_2$ by $(3.1)^{\mathrm{SK}}$, hence $c(a, N(a, s)) \in X$. As c is minimal in X we obtain $c(a, s) = c \leq c(a, N(a, s))$. Hence with $(3.4)^{\mathrm{SK}}$

$$N(a, s) = s \ .$$

As $(3.5\mathrm{b})^{\mathrm{SK}}$ is derived from the Skolemisation of a prenex form for one part of (3.5), we obtain

$$N(a, s) = s \ \wedge\ s \geq a_1 \ \rightarrow\ s \notin F(b) \ .$$

As $N(a, s) = s$ and $s \in F(b)$ we thus have

$$s < a_1 \ .$$

Also, $(3.5\text{a})^{\mathrm{SK}}$ is derived from the Skolemisation of a prenex form for another part of (3.5). Here we obtain

$$N(a,s) = s \;\wedge\; s < a_1 \;\wedge\; s \in F(b) \;\rightarrow\; G(a,s) \;\;.$$

Hence we have $G(a,s)$. Altogether this shows $s < a_1 \;\wedge\; G(a,s)$. □

By choosing appropriate substitutions for the parameters, this generic formula can be used to define syntactic search problem classes which characterise the $\forall\Sigma_1^{\mathrm{b}}$-consequences of T_2^{k+1}: Let $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ be the set of all formulas obtained by replacing in $\mathcal{P}_k(\mathcal{X})$, the list of function and predicate symbols $\mathcal{X}$ by polynomial time computable functions and relations (i.e., their definitions in S_2^1.) Note that $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ is a Skolemized version of the principle $\mathrm{PiPLS}(k,0)$ defined in Section 3. The last theorem shows that each formula in $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ is provable in T_2^{k+1}. A converse is also true and can be shown using the results from Section 9. The next Corollary is a refinement of Corollary 3.6.

Corollary 10.2. *Over* S_2^1*, the theories* $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ *and* T_2^{k+1} *have the same* $\forall\Sigma_1^{\mathrm{b}}$*-consequences.*

Proof. We already argued for one inclusion. We still have to show that if T_2^{k+1} proves $(\forall x)\varphi(x)$ with $\varphi \in \Sigma_1^{\mathrm{b}}$, then this formula also follows from a formula in $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ over S_2^1.

By Theorem 3.5 and the strengthening in Section 9, we obtain a formalised Π_k^{p}-PLS problem with goal formula identical to φ, whose condition (3.1)–(3.5) have prenex forms which can be Skolemised as described in Section 9, and be proven in S_2^1. Let $\mathcal{X}$ be the list of polynomial time computable functions and predicates coming from this characterisation.

Let D_a be an s.u.b. for the search problem, and d the polynomial bound on the feasible solutions. W.l.o.g. we may assume that d also bounds all occurring σ, i.e., all triples $\langle i, \psi, \nu\rangle$ with $i \leq 3$, $\nu \leq k$, and ψ an instance of a formula in the set of decorations obtained from the original T_2^{k+1}-proof of $(\forall x)\varphi(x)$, by substituting free variables with constants for values $< D_a$. Let $E(a)$ be $2^{d(|a|)}$. Then let b be $\mathrm{pair}(a, \mathrm{pair}(a_1, a_2))$, for $a_1 = D_a$ and $a_2 = B(B(\ldots B(D_a + E(a))\ldots))$, k iterations of B (here, B is the term giving a bound on the size of pairs: $x, y < z \;\rightarrow\; \mathrm{pair}(x,y) < B(z)$.) We define

$$N'(a,s) = \begin{cases} N(a,s) & \text{if } s{<}E(a) \;\wedge\; N(a,s){<}E(a) \\ E(a) & \text{otherwise} \end{cases}$$

$$c'(a,s) = \begin{cases} c(a,s) + 2 & \text{if } s < E(a) \\ 1 & \text{if } s > E(a) \\ 0 & \text{if } s = E(a) \end{cases}$$

Let $\mathcal{X}'$ be $\mathcal{X}$ in which N, resp. c, has been replaced by N', resp. c'. Consider the formula $\mathcal{P}_k(\mathcal{X}')$ in $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ defined by $\mathcal{X}'$. Given an input a, we choose an instance b for $\mathcal{P}_k(\mathcal{X}')$ as described above. Then it is easy to show that the strengthenings of the formalised Π^{p}_k-PLS problem proved in Section 9 imply

$$a_1 < a_2 \ \wedge \ (3.1)^{\mathrm{SK}} \ \wedge \ \cdots \ \wedge \ (3.5\mathrm{b})^{\mathrm{SK}}$$

in S^1_2, from which we immediately obtain $\varphi(a)$ over S^1_2 assuming $\mathcal{P}_k(\mathcal{X}')$.

We briefly discuss some cases for the above: $(3.1)^{\mathrm{SK}}$ follows immediately from the definitions. $(3.2)^{\mathrm{SK}}$ follows immediately from the related case in Section 9. Same for $(3.4)^{\mathrm{SK}}$.

To show $(3.3)^{\mathrm{SK}}$ let $s, \sigma, z_1, \ldots, z_k < a_2$ such that

$$F'(a, s, h_\sigma(a, s, \sigma, z_1), h_1(\ldots), z_2, \ldots) \ .$$

Thus $\Psi(a, s, h_\sigma(a, s, \sigma, z_1), h_1(\ldots), z_2, \ldots)$ which implies by Theorem 9.4 $\Psi(a, N(a, s), \sigma, z_1, h_2(a, s, \sigma, z_1, z_2), z_3, h_4(\ldots, z_4), \ldots)$. Theorem 9.3 shows that $s, N(a, s) < E(a)$. Thus, $N'(a, s) = N(a, s)$ and we obtain $F'(a, N'(a, s), \sigma, z_1, h_2(\ldots), \ldots)$. The cases $(3.5\mathrm{a})^{\mathrm{SK}}$ and $(3.5\mathrm{b})^{\mathrm{SK}}$ are similar. □

We observe that similar generic principles can be defined for the $\forall\Sigma^{\mathrm{b}}_{\ell+1}$-consequences of T^{k+1}_2.

As the principle $\mathrm{PiPLS}^{\mathrm{SK}}(k)$ characterises all $\forall\Sigma^{\mathrm{b}}_1$ consequences of T^{k+1}_2, we conjecture that its generic version $\mathcal{P}_k(\mathcal{X})$ defined in (10.1) will separate $\mathrm{T}^k_2(\mathcal{X})$ from $\mathrm{T}^{k+1}_2(\mathcal{X})$.

Conjecture 10.3. $\mathrm{T}^k_2(\mathcal{X}) \nvdash \mathcal{P}_k$

By applying standard techniques using bit-graphs of functions and coding different relations into one, the principle $\mathcal{P}_k$ can be transformed into a principle which depends on only one relation variable α. The resulting principle is still a $\forall \mathrm{s}\Sigma^{\mathrm{b}}_1(\alpha)$ sentence conjectured to separate $\mathrm{T}^k_2(\alpha)$ from $\mathrm{T}^{k+1}_2(\alpha)$.

The formula $\mathcal{P}_k$ can also be transformed into a propositional principle conjectured to provide exponential separations between constant-depth propositional proof systems, by using well-known connections between Bounded Arithmetic and constant-depth propositional proof systems via the Paris-Wilkie translation. There are different ways to view the resulting propositional principle. One way is to read it as a polynomial size set of clauses, where each clause is a logarithmic size set of literals.

We do not go into more depth on these constructions, as they are discussed in detail in the related paper [BB08]. The interested reader is kindly referred to that exposition.

We finish this section by comparing our approach to the characterisation of the $\forall\Sigma^{\mathrm{b}}_{\ell+1}$-consequences of T^{k+1}_2 to the results in [ST07]. The game principles GI_k from [ST07] and the principle $\mathrm{PiPLS}^{\mathrm{SK}}(k+1)$ defined here both characterise the $\forall\Sigma^{\mathrm{b}}_1$ consequences of T^{k+2}_2 over S^1_2. From this we immediately obtain that they are reducible to each other under the canonical reduction of total Σ^{b}_1 search problems as discussed e.g. in [ST07]: Let $A = (\forall x)(\exists y)\varphi(x, y)$ and $B = (\forall u)(\exists v)\psi(u, v)$ be two total Σ^{b}_1 search problems, then we call A reducible to B, in symbols $A \leq B$, if there are two polynomial time computable functions f and g, such that for any x, if v is a solution to B on input $f(x)$, i.e. $\psi(f(x), v)$, then $g(x, v)$ is a solution to A on input x, i.e. $\varphi(x, g(x, v))$. The results of [ST07] show that for any formula A in $\mathrm{PiPLS}^{\mathrm{SK}}(k+1)$, there is an instance B in GI_k with $A \leq B$, provable in S^1_2. In the other direction, using the results obtained here, we obtain that for any B in GI_k, there is a formula A in $\mathrm{PiPLS}^{\mathrm{SK}}(k+1)$ with $B \leq A$, provable in S^1_2. An inspection of the proof of Corollary 10.2 shows that in the latter case the reducing functions are given by the identity for f and a projection to the last component of the second argument (which codes, using the pairing function, the values of several existential quantifiers into one) for g. It is also possible to give a simple direct reduction from the GI_k principle to an instance of $\mathcal{P}_{k+1}$ by a construction that directly matches the combinatorial structure of GI_k. It is not clear whether there is a similarly simple direct reduction from $\mathcal{P}_{k+1}$ to GI_k.

References

[AB09] Klaus Aehlig and Arnold Beckmann. On the computational complexity of cut-reduction, 2009. Accepted for publication, DOI 10.1016/j.apal.2009.06.004.

[BB08] Arnold Beckmann and Samuel R. Buss. Polynomial local search in the polynomial hierarchy and witnessing in fragments of bounded arithmetic. Technical Report CSR15-2008, Department of Computer Science, Swansea University, December 2008.

[Bec03] Arnold Beckmann. Dynamic ordinal analysis. *Arch. Math. Logic*, 42:303–334, 2003.

[BK94] Samuel R. Buss and Jan Krajíček. An application of Boolean complexity to separation problems in bounded arithmetic. *Proc. London Math. Soc. (3)*, 69(1):1–21, 1994.

[Buc91] Wilfried Buchholz. Notation systems for infinitary derivations. *Archive for Mathematical Logic*, 30:277–296, 1991.

[Buc97] Wilfried Buchholz. Explaining Gentzen's consistency proof within infinitary proof theory. In *Computational logic and proof theory*

(Vienna, 1997), volume 1289 of *Lecture Notes in Comput. Sci.*, pages 4–17. Springer, Berlin, 1997.

[Bus86] Samuel R. Buss. *Bounded arithmetic*, volume 3 of *Studies in Proof Theory. Lecture Notes.* Bibliopolis, Naples, 1986.

[Bus95] Samuel R. Buss. Relating the bounded arithmetic and the polynomial time hierarchies. *Annals of Pure and Applied Logic*, 75:67–77, 1995.

[Jeř09] Emil Jeřábek. Approximate counting by hashing in bounded arithmetic. *Journal of Symbolic Logic*, 74(3):829–860, 2009.

[KPT91] Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52:143–153, 1991.

[Kra93] Jan Krajíček. Fragments of bounded arithmetic and bounded query classes. *Trans. Amer. Math. Soc.*, 338(2):587–598, 1993.

[KST07] Jan Krajíček, Alan Skelley, and Neil Thapen. NP search problems in low fragments of bounded arithmetic. *J. Symbolic Logic*, 72(2):649–672, 2007.

[Min78] Grigori E. Mints. Finite investigations of transfinite derivations. *Journal of Soviet Mathematics*, 10:548–596, 1978. Translated from: Zap. Nauchn. Semin. LOMI 49 (1975). Cited after Grigori Mints. *Selected papers in Proof Theory.*Studies in Proof Theory. Bibliopolis, 1992.

[Pol99] Chris Pollett. Structure and definability in general bounded arithmetic theories. *Ann. Pure Appl. Logic*, 100(1-3):189–245, 1999.

[Pud06] Pavel Pudlák. Consistency and games—in search of new combinatorial principles. In *Logic Colloquium '03*, volume 24 of *Lect. Notes Log.*, pages 244–281. Assoc. Symbol. Logic, La Jolla, CA, 2006.

[Pud07] Pavel Pudlák. Fragments of bounded arithmetic and the lengths of proofs, 2007. Preprint.

[PW85] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. In A. Dold and B. Eckmann, editors, *Methods in Mathematical Logic (Proceedings Caracas 1983)*, number 1130 in Lecture Notes in Mathematics, pages 317–340. Springer, 1985.

[ST07] Alan Skelley and Neil Thapen. The provable total search problems of bounded arithmetic, 2007. Preprint.

[Tai68] William W. Tait. Normal derivability in classical logic. In J. Barwise, editor, *The Syntax and Semantics of Infinitatry Languages*, number 72 in Lecture Notes in Mathematics, pages 204–236. Springer, 1968.

[Zam96] Domenico Zambella. Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, 61:942–966, 1996.