A Sequent Calculus with Implicit Term Representation

Stefan Hetzl

A Sequent Calculus with Implicit Term Representation

Stefan Hetzl

Laboratoire Preuves, Programmes et Systèmes (PPS)
Université Paris Diderot
175 Rue du Chevaleret, 75013 Paris, France

Abstract. We investigate a modification of the sequent calculus which separates a first-order proof into its abstract deductive structure and a unifier which renders this structure a valid proof. We define a cut-elimination procedure for this calculus and show that it produces the same cut-free proofs as the standard calculus, but, due to the implicit representation of terms, it provides exponentially shorter normal forms. This modified calculus is applied as a tool for theoretical analyses of the standard calculus and as a mechanism for a more efficient implementation of cut-elimination.

1 Introduction

It is a fundamental observation, made independently by several researchers, that a formal proof can be subdivided into its abstract deductive structure, often called skeleton, and a way of instantiating it with formulas which renders it a valid proof. For proof-search, the separation of these two layers is a principle whose importance can hardly be overemphasised. It is already visible in the original resolution rule [24] but even more apparent in the extension [18] of resolution to type theory. It is central for matings [1] and has applications in logic programming where proof-search provides an operational semantics for Prolog-like languages [21]. From a proof-theoretic point of view, the relation between these two levels has been investigated in [22]. Such questions give rise naturally to unification problems [20, 10]: filling up a skeleton for a cut-free first-order proof can be done by solving a first-order unification problem, the case with cuts corresponds to second-order unification, which is undecidable [15].

In the present paper this separation is investigated *from the point of view of cut-elimination*. We introduce the calculus $\mathbf{LK^s}$, for first-order classical logic, which makes these two levels explicit: a proof contains formulas with free variables whose instantiation is specified independently. We define a cut-elimination procedure for $\mathbf{LK^s}$ and show that it has the same set of normal forms as the standard sequent calculus. We describe two applications of this calculus: on the one hand we obtain an exponential compression of the size of normal forms which makes $\mathbf{LK^s}$ a powerful mechanism for the implemention of $\mathbf{LK}$. On the other hand the implicit representation of terms is used to give a considerably

simplified proof of a characterisation of the form of witness terms obtainable by cut-elimination in terms of a regular tree grammar.

From an implementational perspective, we investigate the role of sharing in the context of first-order proofs from a novel point of view. Previous work on proof normalisation with sharing treated the level of the proof, respectively the term calculus associated to it via a Curry-Howard correspondence: for example the work on optimal reduction for the lambda calculus, see [2] for a survey, or deduction graphs [12, 13] which treat natural deduction directly. The present paper provides a complementary study of redundancy in the formulas of a proof, in particular the exponential compression described in Section 5 cannot be obtained by the above-mentioned sharing mechanisms.

2 The calculus $\mathbf{LK^s}$

In order to introduce the calculus $\mathbf{LK^s}$ we first need some preliminary notions and results about first-order substitutions. We assume two disjoint countably infinite sets of variables at our disposal: one for free variables and one for bound variables; the letters $\alpha, \beta, \gamma, \ldots$ will only be used for free variables, the letters $x, y, z, \ldots$ will be used for both free and bound variables, substitutions may contain free and bound variables. The variables in some expression e will be denoted by $\mathrm{V}(e)$. A substitution σ is a function mapping variables to terms s.t. its domain $\mathrm{dom}(\sigma) := \{x \mid x \neq x\sigma\}$ is finite. The variable-range is $\mathrm{vrge}(\sigma) := \mathrm{V}(\{x\sigma \mid x \in \mathrm{dom}(\sigma)\})$. For a set S of substitutions, $\mathrm{dom}(S) := \bigcup_{\sigma \in S} \mathrm{dom}(\sigma)$ and $\mathrm{vrge}(S) := \bigcup_{\sigma \in S} \mathrm{vrge}(\sigma)$. For σ and θ being substitutions call σ *right-independent of* θ if $\mathrm{dom}(\sigma) \cap \mathrm{dom}(\theta) = \emptyset$ and $\mathrm{vrge}(\sigma) \cap \mathrm{dom}(\theta) = \emptyset$; σ and θ are called *independent* if σ is right-independent of θ and θ is right-independent of σ. The (right-)independence of substitutions is a useful technical property for carrying out rearrangements of substitution sequences which will be used throughout this paper.

Lemma 1. *If σ is right-independent of $\theta = [x_1 \backslash t_1, \ldots, x_n \backslash t_n]$, then $\theta\sigma = \sigma[x_1 \backslash t_1\sigma, \ldots, x_n \backslash t_n\sigma]$. If σ and θ are independent, then $\theta\sigma = \sigma\theta$.*

A substitution σ is called *base substitution* if $|\mathrm{dom}(\sigma)| = 1$. A set S of base substitutions is called *functional* if for all $\sigma_1, \sigma_2 \in S$: $\mathrm{dom}(\sigma_1) = \mathrm{dom}(\sigma_2) \Rightarrow \sigma_1 = \sigma_2$. For substitutions σ, θ write $\sigma <^1 \theta$ if $\mathrm{vrge}(\sigma) \cap \mathrm{dom}(\theta) \neq \emptyset$. A set S of substitutions is called *acyclic* if the directed graph $(S, <^1)$ does not contain a directed cycle. For a set S of substitutions write $\sigma <_S \theta$ if there is a directed path from σ to θ in $(S \cup \{\sigma, \theta\}, <^1)$ and $\leq_S$ for its reflexive closure. This ordering of substitutions will play an important role, it is convenient to extend it also to other objects as follows: For variables x, y write $x \leq_S y$ if $x = y$ or there are $\sigma, \theta \in S$ s.t. $\sigma \leq_S \theta$ and $x \in \mathrm{dom}(\sigma)$ and $y \in \mathrm{vrge}(\theta)$. For a set V of variables write $V \leq_S y$ if there is an $x \in V$ s.t. $x \leq_S y$, for a term t write $t \leq_S y$ if t contains a variable x s.t. $x \leq_S y$ and for a formula F write $F \leq_S y$ if F contains a free variable α s.t. $\alpha \leq_S y$.

Definition 1. *Let S be a finite, acyclic, functional set of base substitutions. A list $\sigma_1, \ldots, \sigma_n$ is called* linearisation of S *if for every $\sigma \in S$ there is exactly one $i \in \{1, \ldots, n\}$ s.t. $\sigma_i = \sigma$ and whenever $\sigma_i <_S \sigma_j$, then $i < j$.*

Lemma 2. *Let S be a finite, acyclic, functional set of base substitutions. Let $\sigma_{i_1}, \ldots, \sigma_{i_n}$ and $\sigma_{j_1}, \ldots, \sigma_{j_n}$ be linearisations of S. Then $\sigma_{i_1} \cdots \sigma_{i_n} = \sigma_{j_1} \cdots \sigma_{j_n}$.*

Proof. By induction on n.

Therefore, each finite, acyclic, functional set S of base substitutions induces a unique substitution $\sigma_1 \cdots \sigma_n$ for $\sigma_1, \ldots, \sigma_n$ being any linearisation of S. We denote this substitution by S°. This description of a substitution is particularly natural in the context of cut-elimination because a global substitution is computed successively by composing base substitutions. This point of view is the design principle behind $\mathbf{LK^s}$.

Definition 2. *A sequent is a pair of multisets of formulas. An $\mathbf{LK^s}$-proof is a pair (π, S) s.t. S is a finite, acyclic, functional set of base substitutions containing free variables only and π is built up from the following axioms and rules:*

$$A_1 \to A_2 \quad \text{if } A_1 S^\circ = A_2 S^\circ$$

$$\frac{\Gamma \to \Delta, A \quad \Pi \to \Lambda, B}{\Gamma, \Pi \to \Delta, \Lambda, A \wedge B}\ \wedge_{\mathrm{r}} \qquad \frac{A, \Gamma \to \Delta \quad B, \Pi \to \Lambda}{A \vee B, \Gamma, \Pi \to \Delta, \Lambda}\ \vee_{\mathrm{l}}$$

$$\frac{A, B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ \wedge_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A, B}{\Gamma \to \Delta, A \vee B}\ \vee_{\mathrm{r}} \qquad \frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta}\ \neg_{\mathrm{l}} \qquad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}\ \neg_{\mathrm{r}}$$

$$\frac{A[x\backslash t], \Gamma \to \Delta}{\forall x\, A, \Gamma \to \Delta}\ \forall_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A[x\backslash\alpha]}{\Gamma \to \Delta, \forall x\, A}\ \forall_{\mathrm{r}} \qquad \frac{A[x\backslash\alpha], \Gamma \to \Delta}{\exists x\, A, \Gamma \to \Delta}\ \exists_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A[x\backslash t]}{\Gamma \to \Delta, \exists x\, A}\ \exists_{\mathrm{r}}$$

where $\alpha \notin \mathrm{dom}(S)$ and t does not contain a variable that is bound in A

$$\frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}\ \mathrm{c}_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A}\ \mathrm{c}_{\mathrm{r}} \qquad \frac{\Gamma \to \Delta}{A, \Gamma \to \Delta}\ \mathrm{w}_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A}\ \mathrm{w}_{\mathrm{r}}$$

$$\frac{\Gamma \to \Delta, A_1 \quad A_2, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut} \quad \text{if } A_1 S^\circ = A_2 S^\circ$$

Furthermore, the following global variable condition *must be fulfilled: For every $\forall_{\mathrm{r}}$- and $\exists_{\mathrm{l}}$-inference ι with an eigenvariable α and every $\beta \leq_S \alpha$: β occurs in π only above ι.*

We have thus relaxed the usual identity constraints on axioms and cuts and replaced it by the weaker constraint of *unifiability* by S°. An even more liberal calculus could be used instead where also the identity constraints on contractions and even on the context of rules are replaced by unifiability. However, our aim here is the analysis of cut-elimination in $\mathbf{LK}$ and the above calculus $\mathbf{LK^s}$ is sufficiently flexible for that purpose. This calculus also bears some resemblance to deduction modulo [8, 9] in relaxing identity constraints, its focus however is rather different as proofs modulo are typically considered w.r.t some fixed background theory, in $\mathbf{LK^s}$ however we will rather start from $S = \emptyset$ and fill S by cut-elimination.

Example 1. Let $\pi =$

$$\dfrac{\dfrac{P(f(\alpha),g(\alpha)) \to P(f(\alpha),g(\alpha))}{P(f(\alpha),g(\alpha)) \to \exists x\, P(f(\alpha),g(x))}\,\exists_{\mathrm{r}} \quad \dfrac{\dfrac{P(\beta,g(\gamma)) \to P(\beta,\delta)}{P(\beta,g(\gamma)) \to \exists y\, P(\beta,y)}\,\exists_{\mathrm{r}}}{P(\beta,g(\gamma)) \to \exists x \exists y\, P(x,y)}\,\exists_{\mathrm{r}}}{\exists x\, P(\beta,g(x)) \to \exists x \exists y\, P(x,y)}\,\exists_{\mathrm{l}}\ \mathrm{cut}$$
$$\dfrac{P(f(\alpha),g(\alpha)) \to \exists x \exists y\, P(x,y)}{\exists x\, P(f(x),g(x)) \to \exists x \exists y\, P(x,y)}\,\exists_{\mathrm{l}}$$

and $S = \{[\beta \backslash f(\alpha)], [\delta \backslash g(\gamma)]\}$. Then (π, S) is an $\mathbf{LK^s}$-proof.

It should be noted that this transition from a calculus $\mathbf{K}$ to a calculus $\mathbf{K^s}$ where syntactic identity is replaced by unifiability is conceivable in a very broad setting: it depends neither on $\mathbf{K}$ being a sequent calculus nor on working in first-order classical logic. The analysis carried out in this paper is therefore also extendable to other proof systems with quantifiers, e.g. to sequent calculi or natural deduction systems for intuitionistic or higher-order logic.

An $\mathbf{LK}$-proof is called regular if different strong quantifier inferences (i.e. $\forall_{\mathrm{r}}$- and $\exists_{\mathrm{l}}$-inferences) have different eigenvariables. $\mathbf{LK^s}$ is complete as every regular $\mathbf{LK}$-proof π can be regarded as an $\mathbf{LK^s}$-proof $(\pi, \emptyset)$. For soundness we need the following

Proposition 1. *If (π, S) is an $\mathbf{LK^s}$-proof, then πS° is a regular $\mathbf{LK}$-proof.*

Proof. The rules remain correct under substitution, the eigenvariable condition of πS° being implied by the global variable condition of (π, S). For regularity, suppose there are strong quantifier inferences ι_1 and ι_2 with the same eigenvariable. By the global variable condition applied to ι_1 and ι_2, ι_1 must be above ι_2 and ι_2 must be above ι_1 and thus $\iota_1 = \iota_2$, so πS° is regular.

3 Cut-Elimination

In this section, we describe cut-elimination for $\mathbf{LK^s}$. The proof reduction steps will be based on those of $\mathbf{LK}$. There are however two crucial differences: upon reduction of a quantifier, the substitution will *not* be applied to the proof but rather be stored in S and secondly variable renamings have to be carried out in S as well. The basic idea behind this procedure, namely to not carry out all substitutions immediately, bears some resemblance to calculi of explicit substitutions, see e.g. [19] for a recent survey. However, $\mathbf{LK^s}$ differs from calculi of explicit substitutions as it does not consider substitutions as part of the object level and does not extend the standard proof reductions by reductions that deal with substitutions.

For the reader's convenience we first recall the reduction of a universal quantifier in **LK**. Let π be an **LK**-proof. If it contains a subproof of the form

$$\psi \quad = \quad \dfrac{\dfrac{\overset{(\psi_1)}{\Gamma \to \Delta, A[x\backslash\alpha]}\ \forall_{\mathrm{r}} \quad \dfrac{\overset{(\psi_2)}{A[x\backslash t], \Pi \to \Lambda}}{\forall x\, A, \Pi \to \Lambda}\ \forall_{\mathrm{l}}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}\ ,$$

we denote this by $\pi = \pi[\psi]$ and define

$$\psi' \quad := \quad \dfrac{\overset{(\psi_1[\alpha\backslash t])}{\Gamma \to \Delta, A[x\backslash t]} \quad \overset{(\psi_2)}{A[x\backslash t], \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}$$

and $\pi[\psi] \to \pi[\psi']$ where $\pi[\psi']$ denotes the proof π where the subproof ψ has been replaced by ψ'. This reduction is adapted to $\mathbf{LK^s}$ in the following sense.

Lemma 3. *Let (π, S) be an $\mathbf{LK^s}$-proof where π contains a subproof*

$$\psi = \dfrac{\dfrac{\overset{(\psi_1)}{\Gamma \to \Delta, A_1[x\backslash\alpha]}\ \forall_{\mathrm{r}} \quad \dfrac{\overset{(\psi_2)}{A_2[x\backslash t], \Pi \to \Lambda}}{\forall x\, A_2, \Pi \to \Lambda}\ \forall_{\mathrm{l}}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}$$

and let

$$\psi' := \dfrac{\overset{(\psi_1)}{\Gamma \to \Delta, A_1[x\backslash\alpha]} \quad \overset{(\psi_2)}{A_2[x\backslash t], \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}\ .$$

Then there is an S' s.t. $(\pi[\psi'], S')$ is an $\mathbf{LK^s}$-proof.

Proof. If x does not appear in A_1, then it also does not appear in A_2 since $A_1 S^\circ = A_2 S^\circ$ and S contains only free variables. In this case, let $S' = S$ and observe that $(\pi[\psi'], S')$ is an $\mathbf{LK^s}$-proof. If x does appear in A_1, let $S' = S \cup \{[\alpha\backslash t]\}$. S' is obviously finite; it is also functional as the $\forall_{\mathrm{r}}$-side condition ensures that $\alpha \notin \mathrm{dom}(S)$. Suppose S' is cyclic, then the cycle in S' must contain $[\alpha\backslash t]$ and thus $t \leq_S \alpha$ which, as t occurs outside of ψ_1 contradicts the global variable assumption of (π, S).

Let $[\alpha_1\backslash t_1], \ldots, [\alpha_n\backslash t_n]$ be a linearisation of S. Then there is a $k \in \{0, \ldots, n\}$ s.t. $S'^\circ = \sigma_l[\alpha\backslash t]\sigma_r$ for $\sigma_l = [\alpha_1\backslash t_1] \cdots [\alpha_k\backslash t_k]$ and $\sigma_r = [\alpha_{k+1}\backslash t_{k+1}] \cdots [\alpha_n\backslash t_n]$. Then

$$A_1[x\backslash\alpha]S'^\circ = A_1\sigma_l\sigma_r[x\backslash t\sigma_r, \alpha\backslash t\sigma_r] = A_2\sigma_l\sigma_r[x\backslash t\sigma_r, \alpha\backslash t\sigma_r] = A_2[x\backslash t]S'^\circ.$$

Let ι be a $\forall_{\mathrm{r}}$- or $\exists_{\mathrm{l}}$-inference in $\pi[\psi']$ with eigenvariable β and let γ be a variable with $\gamma \leq_{S'} \beta$. If $[\alpha\backslash t]$ does not appear in the substitution path $\gamma \leq_{S'} \beta$, then $\gamma \leq_S \beta$ and the global variable condition of $(\pi[\psi'], S')$ follows from that of $(\pi[\psi], S)$. If $[\alpha\backslash t]$ does appear, it does so exactly once for suppose it would appear

twice, then $t \leq_S \alpha$ contradicting acyclicity of S, hence $\gamma \leq_S \alpha$ and $t \leq_S \beta$. By $\gamma \leq_S \alpha$, γ occurs only in ψ_1 and by $t \leq_S \beta$, ι is below the reduced cut and thus γ appears only above ι.

Finally, the remaining identity constraints in $(\pi[\psi'], S')$ are satisfied as they are closed under substitution and the side conditions of the quantifier rules are fulfilled too.

A technical aspect of cut-elimination is to keep track of the names of eigenvariables. The traditional solution of this problem is to work on regular proofs. An alternative would be to use additional constructs for local binding of these variables. In order to keep the object-level formalism as simple as possible, we opted for the first solution. The elimination of a contraction is the only reduction rule where this aspect has to be dealt with. Let V be a set of variables. A substitution ρ is called *fresh-variable renaming for* V if $\rho = [\alpha_i \backslash \alpha'_i]_{i=1}^n$, ρ is injective and none of the α'_i occurs in V. We say that ρ is a fresh-variable renaming for an expression e if it is one for $\mathrm{V}(e)$. If an **LK**-proof π contains a subproof of the form

$$\psi \quad = \quad \dfrac{\dfrac{(\psi_1)}{\Gamma \to \Delta, A, A}\,\mathrm{c_r} \qquad \dfrac{(\psi_2)}{A, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\,\mathrm{cut},$$

define $\psi' :=$

$$\dfrac{\dfrac{\dfrac{(\psi_1)}{\Gamma \to \Delta, A, A} \qquad \dfrac{(\psi_2\rho')}{A, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda, A}\,\mathrm{cut} \qquad \dfrac{(\psi_2\rho'')}{A, \Pi \to \Lambda}}{\dfrac{\Gamma, \Pi, \Pi \to \Delta, \Delta, \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}\,\mathrm{c^*}}\,\mathrm{cut}$$

where $\{\alpha_1, \ldots, \alpha_k\}$ are the eigenvariables of ψ_2 and $\rho' := [\alpha_i \backslash \alpha'_i]_{i=1}^k$, $\rho'' := [\alpha_i \backslash \alpha''_i]_{i=1}^k$ are fresh-variable renamings for π. Define $\pi[\psi] \to \pi[\psi']$. For simplifying the comparison with $\mathbf{LK^s}$ we assume that the above variables α'_i and α''_i have been chosen in such a way that they are not only fresh for the proof currently under consideration but also for the whole cut-elimination sequence up to the current proof. Given a substitution $\sigma = [\beta_j \backslash s_j]_{j=1}^m$, ρ is a fresh-variable renaming for σ if it is one for $V = \mathrm{dom}(\sigma) \cup \mathrm{vrge}(\sigma)$. In this case, define $\sigma^\rho := [\beta_j \rho \backslash s_j \rho]_{j=1}^m$. Given a set S of substitutions, ρ is a fresh-variable renaming for S if it is one for all $\sigma \in S$; in this case, define $S^\rho := \{\sigma^\rho \mid \sigma \in S\}$. For the reduction of a contraction in $\mathbf{LK^s}$ we have to extend the renaming to all variables which depend on eigenvariables of the duplicated proof.

Lemma 4. *Let (π, S) be an $\mathbf{LK^s}$-proof where π contains a subproof*

$$\psi \quad = \quad \dfrac{\dfrac{(\psi_1)}{\Gamma \to \Delta, A_1, A_1}\,\mathrm{c_r} \qquad \dfrac{(\psi_2)}{A_2, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\,\mathrm{cut}.$$

Let $\alpha_1, \ldots, \alpha_k$ be the eigenvariables of ψ_2 and let $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha \mid \alpha \leq_S \alpha_i$ for an $i \in \{1, \ldots, k\}\}$. Let $\alpha'_1, \alpha''_1, \ldots, \alpha'_n, \alpha''_n$ be distinct variables s.t. $\rho' := [\alpha_i \backslash \alpha'_i]_{i=1}^n$ and $\rho'' := [\alpha_i \backslash \alpha''_i]_{i=1}^n$ are fresh-variable renamings for π and S. Then, by the global variable condition, $\psi_2\rho'$ and $\psi_2\rho''$ end with $A_2, \Pi \to \Lambda$. Let $\psi' :=$

$$\dfrac{\dfrac{\dfrac{(\psi_1)}{\Gamma \to \Delta, A_1, A_1} \quad \dfrac{(\psi_2\rho')}{A_2, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda, A_1}\ \text{cut} \quad \dfrac{(\psi_2\rho'')}{A_2, \Pi \to \Lambda}}{\dfrac{\Gamma, \Pi, \Pi \to \Delta, \Lambda, \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}\ \text{c}^*}\ \text{cut}$$

and $S' := S^{\rho'} \cup S^{\rho''}$, then $(\pi[\psi'], S')$ is an $\mathbf{LK^s}$-proof.

Having established the reductions of quantifiers and contractions above we have a cut-elimination relation for $\mathbf{LK^s}$.

Definition 3. *We will write $(\pi, S) \to (\pi', S')$ if π, S, π', S' are as in Lemma 3 or in Lemma 4 above (including the symmetric variants for $\exists$ and contraction-left). Furthermore we also write $(\pi, S) \to (\pi', S)$ if π reduces to π' by a standard* **LK***-reduction of a propositional connective, a weakening, an axiom or the rank of a cut-formula. The reader interested in technical details is invited to consult [16] for a comprehensive list of all reduction rules for this calculus. For* **LK***-proofs π, π' we write $\pi \to \pi'$ for the standard reduction. We will also use $\to$ to denote a sequence of the above reduction steps for both* **LK** *and* $\mathbf{LK^s}$.

Note that we do not impose any restriction on the strategy that can be applied. Therefore this set of reduction rules is not confluent, see [4] for a strongly non-confluent example. It is also not strongly normalising by allowing the double-contraction example found e.g. in [7] and in a similar form in [25]. It is however weakly normalising which follows from known results about **LK**. The rationale for considering this liberal cut-elimination relation lies in the fact that each restriction by a strategy limits the obtainable normal forms. From the point of view of obtaining a confluent calculus, see e.g. [7, 23], to be used as a programming language this effect is intended. However, from the foundational point of view that asks for the constructive content of a mathematical proof in classical logic it has the unfortunate consequence of strongly reducing the degree of generality in which the original proof is considered, see [4].

4 Relation to LK

We can now reduce an **LK**-proof π using either the standard **LK**-reductions to obtain a cut-free **LK**-proof π^* or the $\mathbf{LK^s}$-reductions to obtain a proof (ψ, S) where ψ is cut-free. For a regular **LK**-proof π we define

$$\begin{aligned} \mathrm{NF}_{\mathrm{LK}}(\pi) &:= \{\pi^* \mid \pi \to \pi^*, \pi^* \text{ cut-free}\} \quad \text{and} \\ \mathrm{NF}_{\mathrm{LK^s}}(\pi) &:= \{(\psi, S) \mid (\pi, \emptyset) \to (\psi, S), \psi \text{ cut-free}\}. \end{aligned}$$

In this section we will show that **LK** and $\mathbf{LK^s}$ have the same normal forms. In order to compare the normal forms of $\mathbf{LK^s}$ with those of **LK** we consider the set $(\mathrm{NF}_{\mathrm{LK^s}}(\pi))^\circ$ where, for a set P of $\mathbf{LK^s}$-proofs, we define $P^\circ := \{\psi S^\circ \mid (\psi, S) \in P\}$. First we need some auxiliary commutation properties.

Lemma 5. *Let V be a set of variables, ρ be a fresh-variable renaming for V and σ a substitution with $\mathrm{dom}(\sigma) \subseteq V$ and $\mathrm{vrge}(\sigma) \subseteq V$. Then $(\sigma\rho)|_V = (\rho\sigma^\rho)|_V$.*

Lemma 6. *Let S be a finite, acyclic, functional set of base substitutions and let ρ be a fresh-variable renaming for S. Then $(S^\rho)^\circ = (S^\circ)^\rho$.*

Proposition 2. *Let $\pi \to \pi^*$ be a cut-elimination sequence in **LK**. Then there is a cut-elimination sequence $(\pi, \emptyset) \to (\psi, S)$ in $\mathbf{LK^s}$ s.t. $\psi S^\circ = \pi^*$.*

Proof. By induction on the length of $\pi \to \pi^*$; the case of the empty sequence is trivial. So assume given a sequence $\pi \to \pi' \to \pi^*$ where $\pi' \to \pi^*$ consists of exactly one reduction. By induction hypothesis there is an $\mathbf{LK^s}$-proof (ψ', S') s.t. $\psi' S'^\circ = \pi'$. Note that the inferences in π' are in 1-1 correspondence with those in ψ', so the cut-reduction step $\pi' \to \pi^*$ uniquely induces one in (ψ', S') which we use to define (ψ^*, S^*). It remains to prove $\psi^* S^{*\circ} = \pi^*$. This is easy for the reduction of axioms, propositional connectives, weakening and the rank reductions as $S' = S^*$ in these cases.

For the reduction of a quantifier, let $[\alpha\backslash t]$ be the substitution and π_1 be the subproof of π' to which the substitution is applied in the reduction step $\pi' \to \pi^*$. Then, for some term s we have $S^* = S' \cup \{[\alpha\backslash s]\}$ where, as $\psi' S'^\circ = \pi'$, also $sS'^\circ = t$. Let $[\alpha_1\backslash t_1], \ldots, [\alpha_k\backslash t_k], [\alpha\backslash s], [\alpha_{k+1}\backslash t_{k+1}], \ldots, [\alpha_n\backslash t_n]$ be a linearisation of S', then $[\alpha_1\backslash t_1], \ldots, [\alpha_n\backslash t_n]$ is a linearisation of S. Abbreviating $\sigma_l = [\alpha_1\backslash t_1] \cdots [\alpha_k\backslash t_k]$ and $\sigma_r = [\alpha_{k+1}\backslash t_{k+1}] \cdots [\alpha_n\backslash t_n]$ we thus have $t = s\sigma_r$. Letting ψ_1 be the subproof of ψ' that corresponds to π_1 we have $\pi_1[\alpha\backslash t] = \psi_1\sigma_l\sigma_r[\alpha\backslash s\sigma_r]$. But now, for $i \in \{k+1, \ldots, n\}$, $\alpha \notin \mathrm{V}(t_i)$ by the linearisation property and $\alpha \neq \alpha_i$ by the $\forall_\mathrm{r}$-side condition in ψ, so σ_r is right-independent of $[\alpha\backslash s]$ and thus by Lemma 1: $\pi_1[\alpha\backslash t] = \psi_1 S^{*\circ}$. If F is a formula in ψ^* outside of ψ_1, then $FS'^\circ = FS^{*\circ}$ because $F \not\leq_S \alpha$ by the global variable condition of ψ' and therefore $\psi^* S^{*\circ} = \pi^*$.

For the reduction of contraction, let $\alpha_1, \ldots, \alpha_k$ be the eigenvariables of the subproof π_2 of π' that is duplicated in the reduction $\pi' \to \pi^*$. Then $\alpha_1, \ldots, \alpha_k$ are also the eigenvariables of the subproof ψ_2 of ψ' corresponding to π_2. Let $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha \mid \alpha \leq_{S'} \alpha_i \text{ for an } i \in \{1, \ldots, k\}\}$, then the variables α'_1, α''_1, $\ldots, \alpha'_k, \alpha''_k$ are fresh for ψ' and S' because they are fresh for $\pi \to \pi'$. For the $\mathbf{LK^s}$-step, they are extended to $\alpha'_1, \alpha''_1, \ldots, \alpha'_n, \alpha''_n$ which are also fresh for ψ' and S'. Define $\rho = [\alpha_i\backslash\alpha'_i]_{i=1}^n$, $\hat{\rho} = [\alpha_i\backslash\alpha'_i]_{i=1}^k$, $\sigma = [\alpha_i\backslash\alpha''_i]_{i=1}^n$ and $\hat{\sigma} = [\alpha_i\backslash\alpha''_i]_{i=1}^k$. As $\psi_2\rho$ does not contain any α''_i we have $\psi_2\rho S^{*\circ} = \psi_2\rho(S'^\rho)^\circ$. By Lemma 6: $\psi_2\rho(S'^\rho)^\circ = \psi_2\rho(S'^\circ)^\rho$. Letting $V := \mathrm{dom}(S') \cup \mathrm{vrge}(S') \cup \mathrm{V}(\psi_2)$ and observing that ρ is fresh for V, apply Lemma 5 to obtain $\psi_2\rho(S'^\circ)^\rho = \psi_2 S'^\circ\rho$. Now by induction hypothesis $\psi_2 S'^\circ = \pi_2$ and as $\alpha_{k+1}, \ldots, \alpha_n$ do not appear in π_2, we have $\pi_2\rho = \pi_2\hat{\rho}$ and thus $\psi_2\rho S^{*\circ} = \pi_2\hat{\rho}$. Analogously we obtain $\psi_2\sigma S^{*\circ} = \pi_2\hat{\sigma}$. If F is a formula in ψ^* outside of $\psi_2\rho$ and $\psi_2\sigma$, then for all $i \in \{1, \ldots, n\}$: $F \not\leq_{S'} \alpha_i$ by the global variable condition, so $FS'^\circ = FS^{*\circ}$ and therefore $\psi^* S^{*\circ} = \pi^*$.

Theorem 1. *Let π be a regular* **LK***-proof, then* $\mathrm{NF}_{\mathrm{LK}}(\pi) = (\mathrm{NF}_{\mathrm{LK}^{\mathrm{s}}}(\pi))^{\circ}$.

Proof. The direction $\subseteq$ follows from the above Proposition 2, the direction $\supseteq$ from Proposition 1 and the observation that for $(\psi, S) \to (\psi', S')$ being an $\mathbf{LK^s}$-step, $\psi S^{\circ} \to \psi' S'^{\circ}$ is an **LK**-step.

So $\mathbf{LK^s}$ is equivalent to **LK** from an extensional point of view. It is however different from an intensional point of view, a property that will be exploited in the next two sections to demonstrate that $\mathbf{LK^s}$ is an advantageous mechanism for implementing cut-elimination and a useful tool for carrying out a more fine-grained analysis of **LK**.

5 Implementation and Complexity

It is a well-known observation going back to Kreisel that proof-theoretic methods for consistency-proofs like Gentzen's cut-elimination, Hilbert's ε-calculus or Gödel's Dialectica-interpretation can be applied to concrete mathematical proofs in order to extract constructive information, e.g. bounds or programs, from them. An example for this kind of mathematical application of cut-elimination is Girard's analysis of the Fürstenberg-Weiss proof of van der Waerden's theorem on arithmetic progressions [14, annex 4.A]. A central motivation for implementing cut-elimination thus lies in, at least partially, automating such analyses. The `ceres`-system[1] is an implementation of the cut-elimination method [6] based on resolution and has been applied to concrete proof analyses, see e.g. [5]. In this section we will argue that $\mathbf{LK^s}$ is a useful mechanism for the implementation of the standard cut-elimination as the implicit term representation allows for exponentially shorter normal forms.

The *size* of a term, formula or **LK**-proof is the number of symbols it contains, the size of a set S of substitutions is $\sum_{\sigma \in S} \mathrm{size}(\sigma)$, the size of an $\mathbf{LK^s}$-proof (ψ, S) is $\mathrm{size}(\psi) + \mathrm{size}(S)$. We consider a language containing the constant symbol 0, the function symbols $s(\cdot), +, 2^{\cdot}$ and the binary predicate symbol $=$ with $\mathbb{N}$ as intended interpretation. A numeral is a term of the form $s^n(0)$ for some $n \in \mathbb{N}$; for ease of notation we identify a numeral with the number it denotes. Furthermore the language contains a constant symbol a and a binary function symbol f formalising a data-structure, e.g. binary trees as well as a unary function symbol $|\cdot|$ whose intended interpretation is the number of leaves in a tree built up by f and a. Accordingly, we define the following set $\mathcal{A}$ of axioms, some of which are assigned abbreviations:

$$
\begin{aligned}
& 1 = 2^0 \\
P \;\equiv\; & \forall x\, 2^x + 2^x = 2^{s(x)} \\
& |a| = 1 \\
S \;\equiv\; & \forall x \forall y\, |f(x,y)| = |x| + |y| \\
T \;\equiv\; & \forall x \forall y \forall z\, (x = y \supset y = z \supset x = z) \\
C \;\equiv\; & \forall x \forall y \forall y' \forall z \forall z'\, (x = y + z \supset y = y' \supset z = z' \supset x = y' + z')
\end{aligned}
$$

[1] `http://www.logic.at/ceres/`

where the implication $F \supset G$ is an abbreviation for $\neg F \vee G$ and is right-associative. The sequences of proofs we are going to consider will prove $\exists x\,|x| = 2^n$ from $\mathcal{A}$. When writing down proofs, a list of rule names next to an inference line denotes the application of this list in bottom-up order. We also use the above letters P, S, T, C for denoting a macro-inference which consists of an application of the respective axiom, i.e. one contraction to make a working copy of the axiom, instantiating all quantifiers and removing all implications by axioms on the left so that only the head atom remains. Let

$$\pi_0 \quad := \quad \dfrac{\dfrac{|a| = 2^0 \to |a| = 2^0}{|a| = 2^0 \to \exists x\,|x| = 2^0}\ \exists_{\mathrm{r}}}{\mathcal{A} \to \exists x\,|x| = 2^0}\ T, \mathrm{w}^*$$

which, in expanded form, is

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{|a| = 2^0 \to |a| = 2^0}{|a| = 2^0 \to \exists x\,|x| = 2^0}\ \exists_{\mathrm{r}}}{P, S, |a| = 2^0, T, C \to \exists x\,|x| = 2^0}\ \mathrm{w}^* \quad 1 = 2^0 \to 1 = 2^0}{1 = 2^0, P, S, 1 = 2^0 \supset |a| = 2^0, T, C \to \exists x\,|x| = 2^0}\ \supset_{\mathrm{l}} \quad |a| = 1 \to |a| = 1}{1 = 2^0, P, |a| = 1, S, |a| = 1 \supset 1 = 2^0 \supset |a| = 2^0, T, C \to \exists x\,|x| = 2^0}\ \supset_{\mathrm{l}}}{1 = 2^0, P, |a| = 1, S, T, T, C \to \exists x\,|x| = 2^0}\ \forall_{\mathrm{l}(3\times)}}{1 = 2^0, P, |a| = 1, S, T, C \to \exists x\,|x| = 2^0}\ \mathrm{c}_{\mathrm{l}}$$

Let furthermore $\pi_{n+1} :=$

$$\dfrac{\dfrac{(\pi_n)}{\mathcal{A} \to \exists x\,|x| = 2^n} \quad \dfrac{(\xi_n)}{|\alpha_n| = 2^n, \mathcal{A} \to \exists x\,|x| = 2^{s(n)}}\ \exists_{\mathrm{l}}}{\exists x\,|x| = 2^n, \mathcal{A} \to \exists x\,|x| = 2^{s(n)}}\ \mathrm{cut}}{\mathcal{A}, \mathcal{A} \to \exists x\,|x| = 2^{s(n)}}\ \mathrm{c}^*$$

Let $t_0 := a$, $t_{n+1} := f(\alpha_n, \alpha_n)$ and define $\xi_n :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{|t_{n+1}| = 2^{s(n)} \to |t_{n+1}| = 2^{s(n)}}{|t_{n+1}| = 2^{s(n)} \to \exists x\,|x| = 2^{s(n)}}\ \exists_{\mathrm{r}}}{|t_{n+1}| = 2^n + 2^n, \mathcal{A} \to \exists x\,|x| = 2^{s(n)}}\ P, T, \mathrm{w}^*}{|t_{n+1}| = |\alpha_n| + |\alpha_n|, |\alpha_n| = 2^n, \mathcal{A} \to \exists x\,|x| = 2^{s(n)}}\ \mathrm{c}_{\mathrm{l}}, C}{|\alpha_n| = 2^n, \mathcal{A} \to \exists x\,|x| = 2^{s(n)}}\ S$$

Now, due to the numerals, $\mathrm{size}(\xi_n) = O(n)$ and $\mathrm{size}(\pi_{n+1}) = \mathrm{size}(\pi_n) + \mathrm{size}(\xi_n) + O(n)$ hence $\mathrm{size}(\pi_n) = O(n^2)$. For describing the cut-elimination of π_n we define the following additional proofs. Let $S_n := \{[\alpha_1 \backslash t_1], \ldots, [\alpha_n \backslash t_n]\}$. Write $\mathcal{A}^n$ for n copies of $\mathcal{A}$. For all $n \geq 0$, define a derivation

$$\dfrac{|a| = 2^0, \mathcal{A}^n \to \exists x\,|x| = 2^n}{\mathcal{A}^{n+1} \to \exists x\,|x| = 2^n}\ (\chi_n^0)$$

by the succession T, w^* as used in π_0. For $1 \leq k \leq n$, define a derivation

$$\begin{array}{c} |t_k| = 2^k, \mathcal{A}^{n-k} \to \exists x\, |x| = 2^n \\ (\chi_n^k) \\ |t_{k-1}| = 2^{k-1}, \mathcal{A}^{n-(k-1)} \to \exists x\, |x| = 2^n \end{array}$$

by the succession $S, \mathrm{c_l}, C, P, T, \mathrm{w}^*$ as used in ξ_n and for $n \geq 0$, define the proof

$$\psi_n \quad := \quad \dfrac{\dfrac{\dfrac{|t_n| = 2^n \to |t_n| = 2^n}{|t_n| = 2^n \to \exists x\, |x| = 2^n}\ \exists_{\mathrm{r}}}{\begin{array}{c}(\chi_n^n)\\ \vdots \\ (\chi_n^0)\end{array}}}{\dfrac{\mathcal{A}^{n+1} \to \exists x\, |x| = 2^n}{\mathcal{A} \to \exists x\, |x| = 2^n}\ \mathrm{c}^*}$$

We have $\mathrm{size}(\chi_n^k) = O(n)$ hence $\mathrm{size}(\psi_n) = c + \sum_{k=0}^{n} \mathrm{size}(\chi_n^k) = O(n^2)$ and as $\mathrm{size}(S_n) = O(n)$ finally $\mathrm{size}(\psi_n, S_n) = O(n^2)$.

Theorem 2. *There is a sequence $(\pi_n)_{n\geq 0}$ of regular* **LK***-proofs with* $\mathrm{size}(\pi_n) = O(n^2)$ *s.t.*

1. *every sequence $(\pi_n^*)_{n\geq 0}$ of* **LK***-normal forms has* $\mathrm{size}(\pi_n^*) = \Omega(2^n)$ *and*
2. *there is a sequence $(\psi_n, S_n)_{n\geq 0}$ of* $\mathbf{LK^s}$*-normal forms with* $\mathrm{size}(\psi_n, S_n) = O(n^2)$*. Furthermore, the reduction sequences $(\pi_n, \emptyset) \to (\psi_n, S_n)$ have length $O(n^2)$ and contain only proofs of size $O(n^2)$.*

Proof. Let π_n, ψ_n and S_n be as above. For 1 note that the intended interpretation of our language shows that every cut-free proof of $\mathcal{A} \to \exists x\, |x| = 2^n$ must contain a witness term for x that has 2^n occurrences of a.

For 2 we have to show that $(\pi_n, \emptyset) \to (\psi_n, S_n)$. We proceed by induction on n: the base case $n = 0$ is fulfilled by the empty reduction sequence. To treat the case $n + 1$, first apply the induction hypothesis which costs $O(n^2)$ reductions steps, then apply $O(n)$ rank reductions to transform $(\pi_{n+1}, \emptyset)$ to the proof

$$\dfrac{\dfrac{\dfrac{\dfrac{|t_n| = 2^n \to |t_n| = 2^n}{|t_n| = 2^n \to \exists x\, |x| = 2^n}\ \exists_{\mathrm{r}} \quad \dfrac{(\xi_n)}{\dfrac{|\alpha_n| = 2^n, \mathcal{A} \to \exists x\, |x| = 2^{s(n)}}{\exists x\, |x| = 2^n, \mathcal{A} \to \exists x\, |x| = 2^{s(n)}}\ \exists_{\mathrm{l}}}}{|t_n| = 2^n, \mathcal{A} \to \exists x\, |x| = 2^{s(n)}}\ \mathrm{cut}}{\begin{array}{c}(\chi_{n+1}^n)\\ \vdots \\ (\chi_{n+1}^0)\end{array}}}{\dfrac{\mathcal{A}^{n+2} \to \exists x\, |x| = 2^{s(n)}}{\mathcal{A} \to \exists x\, |x| = 2^{s(n)}}\ \mathrm{c}^*}$$

with S_n as set of substitutions. This $\mathbf{LK^s}$-proof in turn reduces to (ψ_{n+1}, S_{n+1}) in a constant number of reduction steps.

In total, this sums up to $O(n^2)$ reduction steps for $(\pi_n, \emptyset) \to (\psi_n, S_n)$. All proofs in the reduction sequence have size $O(n^2)$ as rank reductions do not change the size and the quantifier reductions only add $[\alpha_1 \backslash t_1], \ldots, [\alpha_n \backslash t_n]$ to the set of base substitutions.

Note that the length of the reduction sequence to $\psi_n S_n^\circ$ in **LK** is also $O(n^2)$ so the above result is an improvement w.r.t. proof size. The above compression cannot be obtained by sharing mechanisms that work on the level of the proof because the redundancy lies at the formula level. Also note that this result is reminiscent of the situation known from first-order unification that, while the unifiability problem is decidable in linear time, the size of the most general unifier is exponential [3].

The above result shows that $\mathbf{LK^s}$ is an advantageous mechanism for implementing cut-elimination because it avoids to unfold terms as long as possible. In addition, it should be noted that due to the simplicity of the used data structure – a set – implementing $\mathbf{LK^s}$ does not require more effort than implementing **LK**. The global substitution which is explicitly computed by $\mathbf{LK^s}$ represents the full cut-elimination in a concise way and can also be applied to structures derived from the original proof π with cuts: for example to a short tautology [17] read off from π to obtain a Herbrand-disjunction or to the characteristic clause set [6] to obtain a propositionally refutable clause set.

6 $\mathbf{LK^s}$ as tool for analysing LK

Carrying out the above analysis of sharing mechanisms on the proof-theoretic instead of on the implementational level has the benefit that it can be used for theoretical analyses as well. An investigation of the form of witness terms obtainable by cut-elimination has been carried out in [16] by different means. One of the central results obtained there is a characterisation of the form of terms obtainable by cut-elimination by regular tree grammars. In this section we will provide a simple proof of this result by observing that it is a corollary of cut-elimination in $\mathbf{LK^s}$.

A *regular tree grammar* [11] is a quadruple $G = (\alpha, N, F, R)$ composed of an axiom α, a set N of non-terminal symbols with $\alpha \in N$, a set F of terminal symbols with $F \cap N = \emptyset$ and a set R of production rules of the form $\beta \to t$ where $\beta \in N$ and t is a term built from $F \cup N$. Given a regular tree grammar $G = (\alpha, N, F, R)$, the derivation relation $\to_G$ associated to G is defined as $s \to_G t$ if there is a production rule $\beta \to u$ and a context $r[]$ s.t. $s = r[\beta]$ and $t = r[u]$. Furthermore, $\twoheadrightarrow_G$ is the reflexive and transitive closure of $\to_G$. The language $\mathrm{L}(G)$ generated by G is the set of all terms containing only symbols from F which can be reached by a derivation path from α.

For the sake of comparability with Section 5, we describe a slightly more general setting than in [16] by working on proofs of Σ_1-sentences in a unviersal theory T. For a proof π of a Σ_1-sentence $F = \exists x_1 \ldots \exists x_n\, A$ with A quantifier-free from axioms of T, let $\mathrm{H}(\pi)$ be the set of auxiliary formulas of $\exists_\mathrm{r}$-inferences introducing $\exists x_n$ in π. Note that $\mathrm{H}(\pi)$ is quantifier-free, that T proves the existential

closure of $\bigvee \mathrm{H}(\pi)$, if π is cut-free, then T proves $\bigvee \mathrm{H}(\pi)$ and if, in addition, T is the empty theory, then $\bigvee \mathrm{H}(\pi)$ is a tautology, the Herbrand-disjunction induced by π.

Let π be a proof and Q be a quantifier occurrence in π. Define a set of terms $\mathrm{t}(Q)$ associated with Q as follows: if Q occurs in the main formula of a weakening, then $\mathrm{t}(Q) := \emptyset$. If Q is introduced by a quantifier inference from a term t or a variable x, then $\mathrm{t}(Q) := \{t\}$ or $\mathrm{t}(Q) := \{x\}$ respectively. If Q occurs in the main formula of a contraction and Q_1, Q_2 are the two corresponding quantifiers in the auxiliary formulas of the contraction, then $\mathrm{t}(Q) := \mathrm{t}(Q_1) \cup \mathrm{t}(Q_2)$. In all other cases Q has exactly one immediate ancestor Q' and $\mathrm{t}(Q) := \mathrm{t}(Q')$.

Let π be a proof, c be a cut in π. Write $\mathrm{Q}(c)$ for the set of pairs (Q, Q') of quantifier occurrences where Q is a strong occurrence in one cut-formula of c and Q' the corresponding weak occurrence on the other side of the cut. Define the set of base substitutions of c as $\mathrm{B}(c) := \bigcup_{(Q,Q')\in \mathrm{Q}(c)} \{[x\backslash t] \mid x \in \mathrm{t}(Q), t \in \mathrm{t}(Q')\}$. For $c_1, \ldots, c_n$ being the cuts in π define the base substitutions of π as $\mathrm{B}(\pi) := \bigcup_{i=1}^{n} \mathrm{B}(c_i)$. A proof then induces a grammar as follows.

Definition 4. *The grammar* $\mathrm{G}(\pi) = (\varphi, N, F, R)$ *is defined by setting* $N = \{\varphi, \alpha_1, \ldots, \alpha_n\}$ *where* $\{\alpha_1, \ldots, \alpha_n\}$ *are the eigenvariables of* π*,* φ *is a new symbol,* F *is the signature of* π *plus the propositional connectives* $\neg, \vee, \wedge$ *and*

$$R = \{\varphi \to F \mid F \in \mathrm{H}(\pi)\} \cup \{\alpha \to t \mid [\alpha\backslash t] \in \mathrm{B}(\pi)\}.$$

Example 2. For the proofs π_n of Section 5 we obtain $\mathrm{G}(\pi_n) = (\varphi, N, F, R)$ where

$$\begin{aligned} N &= \{\varphi, \alpha_0, \ldots, \alpha_{n-1}\}, \\ F &= \{\neg, \vee, \wedge, 0, s, +, 2^{\cdot}, =, a, f, |\cdot|\}, \text{ and} \\ R &= \{\varphi \to |f(\alpha_{n-1}, \alpha_{n-1})| = 2^{s^n(0)}, \\ &\qquad \alpha_{n-1} \to f(\alpha_{n-2}, \alpha_{n-2}), \ldots, \alpha_1 \to f(\alpha_0, \alpha_0), \alpha_0 \to a\}. \end{aligned}$$

One of the central results of [16] is

Theorem 3. *Let* π *be an* **LK***-proof of a* Σ_1*-sentence from universal axioms, then there is a regular tree grammar* $\mathrm{G}(\pi)$ *s.t. for every cut-free* π^* *with* $\pi \to \pi^*$*:* $\mathrm{H}(\pi^*) \subseteq \mathrm{L}(\mathrm{G}(\pi))$.

The importance of this result lies in the fact that the grammar provides a characterisation of all possibly obtainable witness terms that depends only on the original proof π and not on the chosen cut-elimination strategy. In [16] this result has been obtained by considering structured terms which use an additional tree structure for representing substitutions applied to terms. We can now give a simple proof based on cut-elimination in $\mathbf{LK^s}$.

Proof. By Proposition 2 there is a cut-elimination sequence $(\pi, \emptyset) \to (\psi, S)$ in $\mathbf{LK^s}$ s.t. $\psi S^\circ = \pi^*$. Given a variable α in (ψ, S) we write $\iota(\alpha)$ for the unique variable in π that has been renamed to α. The function ι is extended to terms and formulas in the obvious way. By induction on the length of the cut-elimination sequence, it is then straighforward to show (i) $\iota(\mathrm{H}(\psi)) \subseteq \mathrm{H}(\pi)$ and (ii) $\iota(S) \subseteq$

$\mathrm{B}(\pi)$ where ι is needed for contraction- and $\subseteq$ for weakening-reduction. As $\psi S^\circ = \pi^*$ also $\mathrm{H}(\pi^*) = \mathrm{H}(\psi)S^\circ$ and as π^* is a cut-free proof of a Σ_1-sentence from universal axioms, $\mathrm{H}(\pi^*) = \iota(\mathrm{H}(\pi^*))$. Let now $H \in \mathrm{H}(\psi)$ and $\sigma_1, \ldots, \sigma_n$ be a linearisation of S. We will show $\varphi \twoheadrightarrow_{\mathrm{G}(\pi)} \iota(HS^\circ)$ by induction on n. For $n = 0$, $\varphi \twoheadrightarrow_{\mathrm{G}(\pi)} \iota(H)$ by (i). For $n > 0$ let $\sigma_n = [\alpha\backslash t]$, then by (ii) $[\iota(\alpha)\backslash\iota(t)] \in \mathrm{B}(\pi)$ and by applying the production rule $\iota(\alpha) \to \iota(t)$ to all positions of α in $H\sigma_1 \cdots \sigma_{n-1}$ we obtain $\iota(H\sigma_1 \cdots \sigma_{n-1}) \twoheadrightarrow_{\mathrm{G}(\pi)} \iota(H\sigma_1 \cdots \sigma_n)$.

The author is convinced that $\mathbf{LK^s}$ will be a useful tool for obtaining stronger results of the above kind which is left to future work.

7 Conclusion

We have introduced the calculus $\mathbf{LK^s}$ which differs from standard sequent calculus by presenting a proof in a two-layered form: its abstract deductive structure on the one hand and a unifier which renders this structure a proof on the other hand. It has been shown that cut-elimination in $\mathbf{LK^s}$ is equivalent to $\mathbf{LK}$ in the sense that the same set of normal forms is produced. The implicit term representation provided by $\mathbf{LK^s}$ can be used for an implementation that provides an exponential compression of normal forms as well as for a fine-grained theoretical analysis of $\mathbf{LK}$.

Acknowledgements. The author would like to thank Delia Kesner, Alexander Leitsch, Dale Miller, Daniel Weller and the anonymous referees for useful comments on this work.

This research was supported by INRIA and by a Marie Curie Intra European Fellowship within the 7th European Community Framework Programme.

References

1. Andrews, P.B.: Theorem Proving via General Matings. Journal of the ACM 28(2), 193–214 (1981)
2. Asperti, A., Guerrini, S.: The Optimal Implementation of Functional Programming Languages. No. 45 in Cambridge Tracts in Theoretical Computer Science, Cambridge University Press (1998)
3. Baader, F., Snyder, W.: Unification Theory. In: Robinson, A., Voronkov, A. (eds.) Handbook of Automated Reasoning, pp. 445–533. Elsevier (2001)
4. Baaz, M., Hetzl, S.: On the non-confluence of cut-elimination, to appear in the Journal of Symbolic Logic, preprint available at `http://www.logic.at/people/hetzl/`
5. Baaz, M., Hetzl, S., Leitsch, A., Richter, C., Spohr, H.: CERES: An Analysis of Fürstenberg's Proof of the Infinity of Primes. Theoretical Computer Science 403(2–3), 160–175 (2008)
6. Baaz, M., Leitsch, A.: Cut-elimination and Redundancy-elimination by Resolution. Journal of Symbolic Computation 29(2), 149–176 (2000)
7. Danos, V., Joinet, J.B., Schellinx, H.: A New Deconstructive Logic: Linear Logic. Journal of Symbolic Logic 62(3), 755–807 (1997)

8. Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. Journal of Automated Reasoning 31, 33–72 (2003)
9. Dowek, G., Werner, B.: Proof normalization modulo. The Journal of Symbolic Logic 68(4), 1289–1316 (December 2003)
10. Farmer, W.M.: A unification-theoretic method for investigating the k-provability problem. Annals of Pure and Applied Logic 51, 173–214 (1991)
11. Gécseg, F., Steinby, M.: Tree Languages. In: Rozenberg, G., Salomaa, A. (eds.) Handbook of Formal Languages: Volume 3: Beyond Words, pp. 1–68. Springer (1997)
12. Geuvers, H., Loeb, I.: Natural Deduction via Graphs: Formal Definition and Computation Rules. Mathematical Structures in Computer Science 17(3), 485–526 (2007)
13. Geuvers, H., Loeb, I.: Deduction Graphs with Universal Quantification. Electronic Notes in Theoretical Computer Science 203(1), 93–108 (2008)
14. Girard, J.Y.: Proof Theory and Logical Complexity. Elsevier (1987)
15. Goldfarb, W.D.: The undecidability of the second-order unification problem. Theoretical Computer Science 13(2), 225–230 (1981)
16. Hetzl, S.: On the form of witness terms, to appear in the Archive for Mathematical Logic, preprint available at `http://www.logic.at/people/hetzl/`
17. Hetzl, S.: Describing proofs by short tautologies. Annals of Pure and Applied Logic 159(1–2), 129–145 (2009)
18. Huet, G.: A Mechanization of Type Theory. In: Third Interational Joint Conference on Articifical Intelligence (IJCAI). pp. 139–146 (1973)
19. Kesner, D.: A Theory of Explicit Substitutions with Safe and Full Composition. Logical Methods in Computer Science 5(3:1), 1–29 (2009)
20. Krajíček, J., Pudlák, P.: The Number of Proof Lines and the Size of Proofs in First Order Logic. Archive for Mathematical Logic 27, 69–84 (1988)
21. Miller, D., Nadathur, G., Pfenning, F., Scedrov, A.: Uniform proofs as a foundation for logic programming. Annals of Pure and Applied Logic 51(1–2), 125–157 (1991)
22. Orevkov, V.: Reconstruction of a proof by its analysis (russian). Doklady Akademii Nauk 293(3), 313–316 (1987)
23. Parigot, M.: $\lambda\mu$-Calculus: An Algorithmic Interpretation of Classical Natural Deduction. In: Voronkov, A. (ed.) Logic Programming and Automated Reasoning,International Conference LPAR'92, Proceedings. Lecture Notes in Computer Science, vol. 624, pp. 190–201. Springer (1992)
24. Robinson, J.A.: A Machine-Oriented Logic Based on the Resolution Principle. Journal of the ACM 12(1), 23–41 (1965)
25. Zucker, J.: The Correspondence Between Cut-Elimination and Normalization. Annals of Mathematical Logic 7, 1–112 (1974)