Algorithmic Structuring of Cut-free Proofs*

Matthias Baaz** Richard Zach***

Technische Universität Wien, Austria

Abstract. The problem of algorithmic structuring of proofs in the sequent calculi **LK** and $\mathbf{LK}_\mathrm{B}$ (**LK** where blocks of quantifiers can be introduced in one step) is investigated, where a distinction is made between linear proofs and proofs in tree form. In this framework, structuring coincides with the introduction of cuts into a proof. The algorithmic solvability of this problem can be reduced to the question of *k/l-compressibility:*

"Given a proof of $\Pi \to \Lambda$ of length k, and $l \leq k$: Is there is a proof of $\Pi \to \Lambda$ of length $\leq l$?"

When restricted to proofs with universal or existential cuts, this problem is shown to be (1) undecidable for linear or tree-like **LK**-proofs (corresponds to the undecidability of second order unification), (2) undecidable for linear $\mathbf{LK}_\mathrm{B}$-proofs (corresponds to the undecidability of semi-unification), and (3) decidable for tree-like $\mathbf{LK}_\mathrm{B}$-proofs (corresponds to a decidable subproblem of semi-unification).

1 Introduction

Most classical algorithms in proof theory eliminate the structure of given proofs to extract information, e.g., Herbrand disjunctions (as obtained via cut-elimination or the ε-theorem), or normal forms of functional interpretations. The problem of *structuring of proofs* is inverse to these procedures: How to structure a proof by decomposition and introduction of propositions?

In sequent calculi, structuring of proofs can be identified with the insertion of cuts into a proof. This provides us with a general basis for formal approaches to the problem above. All usual cut-elimination procedures for first order logic found in the literature (such as those of Gentzen [1934] and Tait [1968], where substitution is the only operation on terms) produce cut-free proofs of increased term complexity relative to the original proof. If we view the structuring problem as the inverse problem to cut-elimination and restrict ourselves to such procedures, we can of course find a simpler proof with cuts that yields the given proof after cut-elimination if such a proof exists. Such procedures, however, depend on *specific* methods for cut-elimination, and the view of proofs as literal objects.

Since we would actually like to disregard *term* structure in favour of *proof* structure (i.e., we would like to consider proofs as schemata of a certain form, and as equivalent up to substitutions), we take a more general approach here: given a proof and end sequent, we ask for a shorter proof with possibly increased structure. In sequent calculus this corresponds to the introduction of stronger cuts (if the proof cannot be abbreviated trivially, of course). We will be able to solve this problem if we can construct a procedure that solves the following central question:

* in: E. Börger, G. Jäger, H. Kleine Büning, S. Martini, M. M. Richter (Eds.). *Computer Science Logic. Selected papers from CSL'92*, LNCS, Springer, Berlin, 1993, pp. 29–42

** Technische Universität Wien, Institut für Algebra und Diskrete Mathematik E118.2, Wiedner Hauptstraße 8–10, A-1040 Wien, Austria, baaz@logic.tuwien.ac.at

*** Technische Universität Wien, Institut für Computersprachen E185.2, Resselgasse 3/1, A-1040 Wien, Austria, zach@logic.tuwien.ac.at

1.1. k/l-COMPRESSIBILITY Given a proof of $\Pi \to \Lambda$ of length k, and $l \leq k$: Is there is a proof of $\Pi \to \Lambda$ of length $\leq l$?

In what follows, we study proofs in **LK** and $\mathbf{LK}_{\mathrm{B}}$ (**LK** where blocks of quantifiers can be introduced in one step) considered as acyclic graphs (not only tree-like proofs). We restrict ourselves to the fragments with only universal or existential cuts (the cut formulas are pure universal or existential formulas), denoted $\mathbf{LK}^{\Pi\Sigma}$ and $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$, respectively. We show that k/l-compressibility is

(1) undecidable for $\mathbf{LK}^{\Pi\Sigma}$-proofs,
(2) undecidable for linear $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proofs, but is
(3) decidable for tree-like $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proofs.

Since we consider k/l-compressibility as central, and since bounds on cut elimination do only depend on the length of the given proof, it makes no difference whether the given proof is cut-free or not. However, structuring of cut-free proofs is important to computer science, where deduction systems are usually quantifier-free.

In the following, we assume familiarity with BUSS [1991] and KRAJÍČEK and PUDLÁK [1988]

2 Basic definitions

We follow BUSS [1991] in the definition of sequent calculus **LK**, with the exception that axioms and weakenings are restricted to atomic formulas.
The calculus $\mathbf{LK}_{\mathrm{B}}$ is **LK** with the rules ($\forall$:left) and ($\forall$:right) replaced by

$$\frac{A(t_1,\ldots,t_r),\Gamma \to \Delta}{(\forall x_1)\ldots(\forall x_r)A(x_1,\ldots,x_r),\Gamma \to \Delta}\ \forall_B\text{: left}$$

and

$$\frac{\Gamma \to \Delta, A(b_1,\ldots,b_r)}{\Gamma \to \Delta,(\forall x_1)\ldots(\forall x_r)A(x_1,\ldots,x_r)}\ \forall_B\text{: right}$$

respectively (b_1, ..., b_r must not occur in the lower sequent). ($\exists$-left) and ($\exists$-right) are analogously replaced by ($\exists_B$-left) and ($\exists_B$-right).

2.1. DEFINITION A *(linear) proof* is a directed acyclic graph s.t.

(1) every node is labeled with a sequent and the name of a rule of inference,
(2) every node with indegree 0 is labeled by an axiom sequent,
(3) exactly one node has outdegree 0 (labeled by the *end sequent*),
(4) all other nodes have outdegree ≥ 1, and
(5) if an edge connects a node labeled by sequent R to a node labeled by S, then R is a premise to the inference associated with S, and the edge is labeled by L or R according to whether R is the left or right premise of the rule, and unlabeled if the rule has only one premise.

A proof is called *tree-like* if it is a tree, i.e., if every node has outdegree 1. The *length* of a proof is the number of its nodes. For simplicity, we identify nodes with the sequents they are labeled with.

2.2. DEFINITION A *proof analysis* is like a proof except that nodes are only labeled with names of inference rules, and nodes corresponding to axioms and weakenings additionally carry the corresponding predicate symbol.

A proof *realizes* a proof analysis P with end sequent $\Pi \to \Lambda$, if there is a bijection between the nodes and edges in the proof and the proof analysis s.t. corresponding nodes are labeled by the same rule names, axioms and weakening formulas have the predicate symbol determined by the corresponding label in P, corresponding edges have the same labels, and the end sequent of the proof is $\Pi \rightarrow \Lambda$. If there is such a proof, P is called *realizable* with end sequent $\Pi \rightarrow \Lambda$.

The decision problem of whether a given proof analysis with end sequent can be realized by a proof is called the *realizability problem*.

The decision problem of whether there is a proof of a given sequent of length $\leq k$ is called the *k-provability problem*.

2.3. *Remark* It is easily seen that the decidability of realizability implies decidability of k-provability (enumerate all proof analyses up to length k), which in turn implies the decidability of k/l-compressibility, but the converse is not immediately obvious. Consider the class of proof analyses with undecidable realizability problem given in Krajíček and Pudlák [1988], §5: The end sequents $A \rightarrow A, P(s^n 0)$ are trivially derivable by one weakening, and hence k-provability is decidable. To see that the undecidability of k-provability need not imply the undecidability of k/l-compressibility, consider a system of first order logic with all true formulas as axioms and with sound rules: k-provability is undecidable, but k/l-compressibility is decidable.

2.4. *Remark* The restriction to atomic axioms and weakenings makes the use of proof analyses easier, since we can do without a number of case distinctions: In the cut-free case, the end sequent determines the logical form of all formulas, but in the presence of cuts and non-atomic axioms and weakenings, we only have a bound on the logical complexity of the cut-formulas (by Parikh [1973], Theorem 2). Consequently we have to add information on the logical form of cut-formulas to the proof analyses.

3 k/l-Compressibility is undecidable for $\mathbf{LK}^{\Pi\Sigma}$

We derive the undecidability of k/l-compressibility for $\mathbf{LK}^{\Pi\Sigma}$ from the undecidabilty of k-provability: To establish the undecidability of k-provability, we associate with a non-recursive r.e. set $X \subseteq \omega$ a sequence of proof analyses P_i and end sequents $\Pi_i \rightarrow \Lambda_i$, $i \in \omega$, s.t.

$$n \in X \iff P_n \text{ is realizable with end sequent } \Pi_n \rightarrow \Lambda_n,$$

and, furthermore, that all proofs of $\Pi_n \rightarrow \Lambda_n$ for $n \in \omega \setminus X$ are longer than P_n.

In fact, there is a recursive superset X^* of X such that $\Pi_n \rightarrow \Lambda_n$ is *provable* for all $n \in X^*$, since k-provability for *cut-free* proofs is decidable (cf. Krajíček and Pudlák [1988], Theorem 6.1). If $\Pi_n \rightarrow \Lambda_n$ is of the form $\Pi \rightarrow \Lambda, A(s^n(0))$, then X^* is even co-finite.

To show that k/l-compressibility is undecidable, it suffices to bound the length of the proofs of $\Pi_n \rightarrow \Gamma_n$. This is the statement of the following theorem, which can be gathered from Buss [1991]:

3.1. Theorem *For every r.e. set $X \neq \emptyset$ there is a formula $A_X(c)$ and $k \in \omega$ s.t. $n \in X$ iff $\rightarrow A_X(s^n(0))$ has an* **LK**- *(by construction* $\mathbf{LK}^{\Pi\Sigma}$*-) proof of length k and $\rightarrow A(s^n(0))$ has an* **LK**- *(by construction* $\mathbf{LK}^{\Pi\Sigma}$*-) proof of length $k+1$ for all $n \in \omega$.*

Proof. Every r.e. set $X \subseteq \omega$ can be represented by a set Ω of partial substitution equations obeying the special restriction s.t., $n \in X$ iff $\Omega \cup \{\beta_1 = s^n(0)\}$ has a solution (Buss [1991], Theorem 3). The proof of this fact is via Matijacevič's Theorem by encoding diophantine equations as partial substitution equations. Let $\Omega \cup \{\beta_1 = s^n(0)\}$ be the set of equations characterizing the r.e. set X.

In the proof of the Main Theorem of Buss [1991] a formula $A_X(s^n(0))$ and an integer N are constructed s.t. $\rightarrow A_X(s^n(0))$ has an **LK**-proof of $\leq N$ steps iff the above equations have a solution, and is provable in $N+1$ steps, if all but one of the equations have a solution (Section 4, see in particular p. 93, first paragraph). The first part of the theorem now follows from the fact that the system encodes X and hence is solvable iff $n \in X$. For the second part, we replace β_1 by $s^r(0)$ for some $r \in X$, $r \neq n$. Then $s^r(0) = s^n(0)$ is the only equation not satisfied (regardless of whether $n \in X$ or not).

The proofs constructed are all tree-like, use only existential cuts, atomic axioms and atomic weakenings. The central Propositon 8 of Buss [1991] (as noted there) can be adapted to the non-tree-like case. Hence the arguments extend to the case of linear $\mathbf{LK}^{\Pi\Sigma}$-proofs. $\square$

3.2. Corollary *k/l-Compressibility is undecidable for $\mathbf{LK}^{\Pi\Sigma}$-proofs (whether linear or tree-like).*

3.3. *Remark* If the end sequent contains only unary function symbols, k/l-compressibility is decidable: cf. Parikh [1973], Theorem 1 for the case of one and Farmer [1991], Corollary 5.20 for several unary function symbols. It is also decidable if we are looking for shorter proofs with *quantifier-free* cuts (cf. Krajíček and Pudlák [1988], Section 2).

3.4. *Remark* The theorem shows that, in the worst case, we have to pay for introduced structure by a significant—in fact non-recursive—increase in the term structure, *even in decidable subcases.* This situation could be alleviated by taking into account known properties of the function symbols, such as associativity and commutativity.

4 k/l-Compressibility is undecidable for linear $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proofs

To be able to deal with block inferences of quantifiers, we introduce the concept of *semi-unification*:

4.1. Definition (cf. Baaz [1993], Kfoury *et al.* [1990], Pudlák [1988]) A substitution δ is called a *semi-unifier* of the semi-unification problem $\{(s_1, t_1), \ldots, (s_p, t_p)\}$ iff there exist $\sigma_1, \ldots, \sigma_p$ such that $s_1\delta = t_1\delta\sigma_1, \ldots, s_p\delta = t_p\delta\sigma_p$. In other words, a semi-unifier makes the s_i substitution instances of the corresponding t_i.

4.2. Example $\delta = \{f(x, f(x,x))/z\}$ is a semi-unifier of $\big(f(x,z), f(x, f(x,y))\big)$ because

$$f(x,z)\{f(x,f(x,x))/z\} = f(x,f(x,y))\{f(x,f(x,x))/z\}\{f(x,x)/y\}.$$

There is no semi-unifier of $\big(f(x,y), f(x,f(x,y))\big)$, since no simultaneous substitution will make the left side a substitution instance of the right side.

4.3. Theorem *Realizability is undecidable for linear $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-analyses.*

This follows immediately from the undecidability of semi-unification (Kfoury *et al.* [1990]) and the following proposition:

4.4. Proposition *Let the language contain a binary function symbol f. For every semi-unification problem $\Omega = \{(s_1, t_1), \ldots, (s_p, t_p)\}$, there is a proof analysis P_Ω and a sequent $\Pi_\Omega \rightarrow \Lambda_\Omega$, s.t. there is an $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proof realizing P_Ω with end sequent $\Pi_\Omega \rightarrow \Lambda_\Omega$ iff Ω is solvable.*

Proof. First note that the semi-unification problem can be reduced to a semi-unification problem $\{(s_1^*, t), \ldots, (s_p^*, t)\}$ with $s_i^* = f(\cdots f(a_{i_1}, a_{i_2}) \ldots s_i) \ldots a_{i_p})$ and $t = f(\cdots f(t_1, t_2), \ldots t_p)$, where a_{i_j} are new free variables.

Let $A_\Omega(a_1, \ldots, a_n) \equiv P(t) \wedge ((P(s_1^*) \wedge \ldots \wedge P(s_p^*)) \supset Q)$, where all free variables are among $a_1, \ldots, a_n$ and do not occur in Q. We sketch the construction of a proof analysis as follows:

$$
\begin{array}{ll}
 & \left\{ \text{propositional inferences} \right. \\
(a) & A_\Omega(a_1, \ldots, a_n)\delta \to A_\Omega(a_1, \ldots, a_n)\delta \\
(a+1) & \underline{(\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to A_\Omega(a_1, \ldots, a_n)\delta} \\
 & \left\{ \begin{array}{l} \text{propositional inferences including} \\ \text{propositional cuts from } (a+1) \end{array} \right. \\
(b) & (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to P(t)\delta \\
(b+1) & \underline{(\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to (\forall y_1) \ldots (\forall y_m) R(y_1, \ldots, y_m)} \\
 & \left\{ \begin{array}{l} \text{propositional inferences including} \\ \text{propositional cuts from } (a+1) \end{array} \right. \\
(c) & P(s_1^*)\delta, \ldots, P(s_p^*)\delta, (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\
 & \left\{ \begin{array}{l} p\ (\forall_B\text{-left})\text{-inferences, exchanges} \\ \text{and contractions from } (c) \end{array} \right. \\
(d) & (\forall z_1) \ldots (\forall z_s) R'(z_1, \ldots, z_s), (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\
(e) & (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n), (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\
(e+1) & (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q
\end{array}
$$

Here, $(a+1)$ is obtained from (a) by ($\forall_B$:left), $(b+1)$ from (b) by ($\forall_B$:right), (e) from $(b+1)$ and (d) by cut, and $(e+1)$ from (e) by contraction. Note that $(\forall y_1) \ldots (\forall y_m) R(y_1, \ldots, y_m) \equiv (\forall z_1) \ldots (\forall z_s) R'(z_1, \ldots, z_s)$ by the cut rule and hence δ is forced to be a semi-unifier. The label $(a+1)$ is ancestor of *both* sides of the cut, the skeleton is therefore *not* in tree form. (The length of the skeleton is linear in n.)
□

4.5. *Remark* If $p = 1$, then the realizability of this analysis is decidable (cf. PUDLÁK [1988], Theorem (i)).

4.6. *Remark* Note that we do not, and indeed cannot, have a result like this:

For every r.e. set $X \subseteq \omega$ there is a proof analysis P_X and a sequent $\Pi_X \to \Lambda_X, A_X(a)$ s.t. there is an $\mathbf{LK}_B^{\Pi\Sigma}$-proof realizing P_X with end sequent $\Pi_X \to \Lambda_X, A_X(s^n(0))$ iff $n \in X$.

This follows from the fact that for every proof analysis P and every sequent $\Pi \to \Lambda$ with free variable a, there is a semi-unification problem

$$\Omega = \{(s_1(a), t_1(a)), \ldots, (s_p(a), t_p(a))\}$$

s.t. P is realizable by an $\mathbf{LK}^{\Pi\Sigma}$-proof with end sequent $(\Pi \to \Lambda)\{s^n(0)/a\}$ iff $\Omega\{s^n(0)/a\}$ has a solution.

But $\Omega\{s^n(0)/a\}$ is either solvable for all $n \geq m$ and unsolvable for $n < m$, or for only one n. To see this, calculate the most general semi-unifier δ of

$$\{(f(s_1, a), f(t_1, a)), \ldots, (f(s_p, a), f(t_p, a))\}$$

(see below, Proposition 5.4). δ assigns to a either a term of the form $s^m(0)$ (one solution for $n = m$) or one of the form $s^m(b)$ (a solution for every $n \geq m$) (cf. Baaz [1993]).

For $\mathbf{LK}^{\Pi\Sigma}$, such an undecidable proof analysis exists, cf. Krajíček and Pudlák [1988], Section 5.

4.7. Theorem *k/l-Compressibility is undecidable for linear $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proofs.*

Proof. We exhibit a class $\mathcal{C}$ of semi-unification problems whose solvability is undecidable and then show that for $\Omega \in \mathcal{C}$ there is a sequent $\Pi_\Omega \to \Lambda_\Omega$ s.t.

(1) $\Pi_\Omega \to \Lambda_\Omega$ has a proof (with cut) of length l iff Ω has a solution, and
(2) $\Pi_\Omega \to \Lambda_\Omega$ has a proof of length $l + C$.

Let $\mathcal{C}$ consist of $\Omega = \{(s_1, t), (s_2, t)\}$ where

(1) $(\forall x_1, \ldots, x_n) A_\Omega(x_1, \ldots, x_n) \to Q$ is valid for $A_\Omega \equiv P(t) \wedge \big(P(s_1) \wedge P(s_2) \supset Q\big)$,
(2) s, t_1, t_2 are pairwise not unifiable.

We have to prove that $\mathcal{C}$ has the desired property that the proof analysis in Proposition 4.4 describes an optimal proof of $(\forall \bar{x}) A_\Omega(\bar{x}) \to Q$ if Ω is solvable, and that proofs are longer if Ω has no solution. Then we construct a longer proof analysis that is realizable by an $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proof with the same end sequent for all $\Omega \in \mathcal{C}$.

First of all, $\mathcal{C}$ is undecidable because of the following: (a) By Theorem (ii) of Pudlák [1988], every semi-unification problem can be translated into a problem of the form $\Psi = \{(s_1', t'), (s_2', t')\}$. Every such problem can in turn be rewritten as $\Psi' = \big\{\big(f(g(a), s_1), f(a, t)\big), \big(f(h(a), s_2), f(a, t)\big)\big\}$, where a is a new variable. Ψ' obviously has the same solutions as Ψ, but the components of the two equations are pairwise not unifiable.

(b) Validity of $(\forall \bar{x}) A_\Omega(\bar{x}) \to Q$ is decidable. This follows from the fact that the following resolution proof exists iff $(\forall \bar{x}) A_\Omega(\bar{x}) \to Q$ is valid:

$$\dfrac{\dfrac{\{P(t)\sigma_2\} \qquad \dfrac{\{P(t)\sigma_1\} \quad \{\neg P(s_1), \neg P(s_2), Q\}}{\{\neg P(s_2)\delta_1, Q\}}\,\delta_1}{\{Q\}}\,\delta_2 \qquad \{Q\}}{\square}\,id$$

where σ_1, σ_2 are renamings of variables. Consequently the following equations hold:

$$\begin{aligned} P(t)\sigma_1\delta_1\delta_2 &= P(s_1)\delta_1\delta_2 \\ (\text{since } P(t)\sigma_1\delta_1 &= P(s_1)\delta_1) \\ P(t)\sigma_2\delta_2 &= P(s_2)\delta_1\delta_2 \end{aligned}$$

The crucial point for the encoding of semi-unification problems by the proof analysis and end sequent $(\forall \bar{x}) A_\Omega(\bar{x}) \to Q$ is that $(\forall \bar{x}) A_\Omega(\bar{x})$ is "produced" only once, i.e., that $(a+1)$ is ancestor to both premises of the cut (d). We can force this to be the case by replacing $A_\Omega(\bar{a})$ by $\neg^{2r} A_\Omega(\bar{a})$, where r is sufficiently large to make a separate deduction—by copying the part of the analysis above $(a+1)$—too costly.

Let $(\forall \bar{x}) \neg^{2r} A_\Omega(\bar{x}) \to A'$ be the sequent at $(a+1)$. We have (1) $\neg^{2r} A_\Omega(\bar{x})\delta \to A'$ for some δ and (2) Q has to be derived from A'. Take the shortest derivations of (1) and (2). The shortest derivation of Q must contain a quantified cut, since s_1, s_2, t are pairwise not unifiable. If $\big\{(s_1, t), (s_2, t)\big\}$ is not semi-unifiable, one universal or existential cut is not sufficient. The universal cut in the analysis given in the proof of Proposition 4.4 is the simplest possible one(This is intuitively clear, a rigorous proof would use analoga to Propositions 4–9 of Buss [1991]).

Now we show that there *is* a uniform way of deriving valid sequents

$$(\forall \bar{x})\neg^{2r} A_{\Omega}(\bar{x}) \to Q$$

(which of course is longer than the one using the solution to the semi-unification problem Ω). Given σ_1, σ_2, δ_1, δ_2 from the above resolution deduction, the following gives a proof:

$$\begin{array}{ll}
 & \Big\{ \text{propositional inferences} \\
(a) & \neg^{2r} A(a_1, \ldots, a_n) \to A(a_1, \ldots, a_n) \\
(a+1) & \underline{(\forall x_1) \ldots (\forall x_n)\neg^{2r} A(x_1, \ldots, x_n) \to A(a_1, \ldots, a_n)} \\
 & \Big\{ \text{propositional inferences including propositional cuts from } (a+1) \\
(b) & (\forall x_1) \ldots (\forall x_n)\neg^{2r} A(x_1, \ldots, x_n) \to P(t) \\
(b+1) & \underline{(\forall x_1) \ldots (\forall x_n)\neg^{2r} A(x_1, \ldots, x_n) \to (\forall y_1) \ldots (\forall y_m) P(t)} \\
(\alpha) & P(t)\sigma_1\delta_1\delta_2 \to P(t)\sigma_1\delta_1\delta_2 \\
(\alpha+1) & (\forall x_1) \ldots (\forall x_n) P(t) \to P(t)\sigma_1\delta_1\delta_2 \\
(\beta) & P(t)\sigma_2\delta_2 \to P(t)\sigma_2\delta_2 \\
(\beta+1) & (\forall x_1) \ldots (\forall x_n) P(t) \to P(t)\sigma_2\delta_2 \\
(\gamma) & \underline{(\forall x_1) \ldots (\forall x_n) P(t) \to P(t)\sigma_1\delta_1\delta_2 \wedge P(t)\sigma_2\delta_2} \\
 & \Big\{ \text{propositional inferences including propositional cuts from } (a+1) \\
(c) & P(s_1) \wedge P(s_2), (\forall x_1) \ldots (\forall x_n)\neg^{2r} A_{\Omega}(x_1, \ldots, x_n) \to Q \\
(c+1) & \underline{(\exists x_1) \ldots (\exists x_n)\big(P(s_1) \wedge P(s_2)\big), (\forall x_1) \ldots (\forall x_n)\neg^{2r} A_{\Omega}(x_1, \ldots, x_n) \to Q} \\
 & \Big\{ \text{propositional inferences} \\
(\delta) & P(s_1)\delta_1\delta_2 \wedge P(s_2)\delta_1\delta_2 \to P(s_1)\delta_1\delta_2 \wedge P(s_2)\delta_1\delta_2 \\
(\delta+1) & P(s_1)\delta_1\delta_2 \wedge P(s_2)\delta_1\delta_2 \to (\exists x_1) \ldots (\exists x_n)\big(P(s_1) \wedge P(s_2)\big) \\
 & \Big\{ \text{cut from } (\gamma) \text{ and } (\delta+1) \\
(\varepsilon) & (\forall x_1) \ldots (\forall x_n) P(t) \to (\exists x_1) \ldots (\exists x_n)\big(P(s_1) \wedge P(s_2)\big) \\
 & \Big\{ \text{two cuts from } (b+1),\ (c+1),\ (\varepsilon) \\
(e) & (\forall x_1) \ldots (\forall x_n)\neg^{2r} A_{\Omega}(x_1, \ldots, x_n), (\forall x_1) \ldots (\forall x_n)\neg^{2r} A_{\Omega}(x_1, \ldots, x_n) \to Q \\
(e+1) & (\forall x_1) \ldots (\forall x_n)\neg^{2r} A_{\Omega}(x_1, \ldots, x_n) \to Q
\end{array}$$

For the cut resulting in (ε), recall that $P(t)\sigma_1\delta_1\delta_2 = P(s_1)\delta_1\delta_2$ and $P(t)\sigma_2\delta_2 = P(s_2)\delta_1\delta_2$. $\square$

5 k/l-Compressibility is decidable for tree-like $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proofs

For tree-like $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-analyses there is a procedure to decide realizability, given the analysis and end sequent. This procedure uses special semi-unification problems to determine the term structure of the proof. These problems are decidable, and furthermore a most general solution can be found, which guarantees term-minimal proofs.

5.1. Definition A semi-unifier σ of a semi-unification problem Ω is called *most general semi-unifier*, if every semi-unifier σ' of Ω can be written as $\sigma\delta$, for some substitution δ. The most general semi-unifier is unique up to renaming of variables.

In contrast to second order unification, semi-unification has the property that most general semi-unifiers exist, if any exist at all:

5.2. Proposition *There is an algorithm computing the most general semi-unifier of a given semi-unification problem Ω if any semi-unifier for Ω exists.*

See Baaz [1993] or Kfoury *et al.* [1990] for details. The algorithm works roughly as follows: Let $\{(s_1, t_1), \ldots, (s_n, t_n)\}$ be the given semi-unification problem, and let α_i be disjoint canonical renamings of the variables in t_i. Unify $t_i\alpha_i$ with s_i. Apply the resulting unifier to the problem and repeat the process, until the unifier is only a renaming of variables or until unification fails, in which case there is no semi-unifier. The procedure will not always terminate, since semi-unification is undecidable, but will produce a most general semi-unifier if there is any semi-unifier. In what follows we will only use a decidable class of semi-unification problems for which the algorithm terminates after one step:

5.3. Definition Let t be a term and $a_1, \ldots, a_n$ be a sequence of variables.

$$t * \langle a_1, \ldots, a_n\rangle := f(\ldots f(f(t, a_1), a_2) \ldots a_n)$$

5.4. Proposition *Let Ω be a semi-unification problem of the form*

$$\big\{\big(s_1 * \langle a_1, \ldots, a_n\rangle, t_1 * \langle a_1, \ldots, a_n\rangle\big), \ldots, \big(s_r * \langle a_1, \ldots, a_n\rangle, t_r * \langle a_1, \ldots, a_n\rangle\big)\big\},$$

where the variables in $s_1, \ldots, s_r$ are among $a_1, \ldots, a_n$, and let α_i be disjoint canonical renamings of the variables in t_i. Let σ be the most general unifier of

$$\big\{\big(s_1 * \langle a_1, \ldots, a_n\rangle, t_1 * \langle a_1, \ldots, a_n\rangle\alpha_1\big), \ldots, \big(s_r * \langle a_1, \ldots, a_n\rangle, t_r * \langle a_1, \ldots, a_n\rangle\alpha_r\big)\big\},$$

If σ exists, then σ is also a most general semi-unifier of Ω, otherwise Ω is unsolvable.

Proof. σ is also a most general unifier of $\{(s_1, t_1\alpha'_1), \ldots, (s_r, t_r\alpha'_r)\}$, where α'_i is a renaming of the variables occuring in t_i *other than* $a_1, \ldots, a_n$. Let $t_i \equiv t_i(a_1, \ldots, a_n, b_1, \ldots, b_m)$. Then

$$t_i\sigma = t_i(a_1\sigma, \ldots, a_n\sigma, b_1, \ldots, b_m)$$

($b_1, \ldots, b_m$ do not occur in $s_1, \ldots, s_r$!) and

$$s_i\sigma = t_i(a_1\sigma, \ldots, a_n\sigma, b_1\alpha'_i\sigma, \ldots, b_m\alpha'_i\sigma). \quad \Box$$

5.5. Proposition *Let P be a tree-like proof analysis with given end sequent. If there is an $\mathbf{LK}_\mathrm{B}$-proof D realizing P, then there also is a proof D' with the following properties:*

(1) D' is regular (no two strong quantifier inferences have the same eigenvariable and eigenvariables do not occur in the end sequent).

(2) *If P contains a sequence of applications of ($\forall_{\mathrm{B}}$:left) to the same formula, then D' introduces all quantifiers in the first of these applications, and all following ($\forall_{\mathrm{B}}$:left) inferences in the sequence are empty introductions. Similarly for ($\exists_{\mathrm{B}}$:right)*

(3) *If P contains a sequence of applications of ($\forall_{\mathrm{B}}$:right) to the same formula, then D' introduces all quantifiers in the last of these applications, and all preceding ($\forall_{\mathrm{B}}$:right) inferences in the sequence are empty introductions. Similarly for ($\exists_{\mathrm{B}}$:left)*

Proof. (1) In a tree-like proof, eigenvariables can be renamed to ensure regularity. (2), (3) If strong quantifier inferences are moved downwards and weak quantifier inferences are moved upwards in a regular proof tree, the eigenvariable conditions can be protected by renaming. □

5.6. THEOREM *Realizability is decidable for tree-like $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-proof analyses.*

Proof. Given a tree-like proof analysis P and an end sequent $\Pi \to \Lambda$, we construct a *preproof* $\Psi(P, \Pi \to \Lambda)$. A preproof is an assignment of formulas to the nodes of the analysis P such that all inferences except quantifier inferences introducing cut-formulas are in correct form (i.e., valid applications of the rules), and a substitution for free variables will "correct" the cuts as well. Ψ is term-minimal, i.e., if D is a proof realizing P, then D can be written as $\Psi\sigma$, for some substitution σ. The construction is similar to the construction of cut-free term-minimal tree-like proofs in KRAJÍČEK and PUDLÁK [1988], Section 2.

Constructing a preproof Since $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$-analyses contain the names of predicates in axioms and weakenings, the logical structure of a proof is uniquely determined (cf. Proposition 5.5) except for the quantifier prefix of the cut formulas in universal and existential cuts. We index the universal and existential cuts by α_1, α_2, ...

(1) Determine the propositional structure of Ψ from P. Use different free variables for *every* term position in the predicates. For quantifier prefixes use special *quantifier prefix variables* ($\forall_{\mathrm{B}}$-α_i), ($\exists_{\mathrm{B}}$-α_i).
(2) Unify the end sequent of Ψ with $\Pi \to \Lambda$, and proceed upwards in the proof tree as follows:
   (a) Unify conclusions of propositional inferences, exchanges, contractions, and weakenings with the respective premises.
   (b) In strong quantifier inferences not introducing cut formulas, e.g.,

$$\frac{\Gamma' \to \Delta', A'}{\Gamma \to \Delta, (\forall x_1)\ldots(\forall x_n)A(x_1,\ldots,x_n)}\ (\forall_B\text{:right})$$

   unify Γ, Δ with Γ',Δ', and $A(c_1,\ldots,c_n)$ with A', where c_1, ..., c_n are new free variables *which are handled as constants* to avoid substitution into eigenvariables, similarly for ($\exists_B$:left).
   (c) In weak quantifier inferences not introducing cut formulas, e.g.,

$$\frac{A', \Gamma' \to \Delta'}{(\forall x_1)\ldots(\forall x_n)A(x_1,\ldots,x_n), \Gamma \to \Delta}\ (\forall_B\text{:left})$$

   unify Γ, Δ with Γ',Δ', and $A(z_1,\ldots,z_n)$ with A', where z_1, ..., z_n are new variables, similarly for ($\exists_B$:right).
   (d) Unify A and A' in axioms $A \to A'$ and unify the cut formulas in the premises of a cut.

As can easily be seen, the steps in the construction are all as general as possible and the restrictions imposed by the unifications are all necessary. If the procedure fails to find a preproof (i.e., one of the unifications fails or eigenvariable conditions are violated), P is not realizable with end sequent $\Pi \rightarrow \Lambda$.

To complete the preproof to a proof we now have to determine the quantifier prefixes and the term structure of the universal and existential cut formulas. We first illustrate this:

5.7. EXAMPLE

$$
\dfrac{
\dfrac{
\dfrac{
\begin{matrix}
\dfrac{\begin{matrix}\vdots \\ \Gamma_1 \rightarrow \Delta_1, A_1\end{matrix}}{\Gamma_1 \rightarrow \Delta_1, (\forall_{\mathrm{B}}\text{-}\alpha)A}\ * \\ \vdots \\ \Gamma_2 \rightarrow \Delta_2, (\forall_{\mathrm{B}}\text{-}\alpha)A, A_2
\end{matrix}
}{\Gamma_2 \rightarrow \Delta_2, (\forall_{\mathrm{B}}\text{-}\alpha)A, (\forall_{\mathrm{B}}\text{-}\alpha)A}\ **
}{\Gamma_2 \rightarrow \Delta_2, (\forall_{\mathrm{B}}\text{-}\alpha)A}
\qquad
\begin{matrix}
\dfrac{\begin{matrix}\vdots \\ A_3, \Gamma_3 \rightarrow \Delta_3\end{matrix}}{(\forall_{\mathrm{B}}\text{-}\alpha)A, \Gamma_3 \rightarrow \Delta_3}
\quad
\dfrac{\begin{matrix}\vdots \\ A_4, \Gamma_4 \rightarrow \Delta_4\end{matrix}}{(\forall_{\mathrm{B}}\text{-}\alpha)A, \Gamma_4 \rightarrow \Delta_4} \\ \vdots \\ (\forall_{\mathrm{B}}\text{-}\alpha)A, \Gamma_5 \rightarrow \Delta_5
\end{matrix}
}{\Gamma_2, \Gamma_5 \rightarrow \Delta_2, \Delta_5}
$$

Let P_1 (P_2) denote the part of the preproof above the end sequent and below $*$ ($**$). If σ is an extension of the preproof to a proof, then (a) the eigenvariables of ($*$) do not occur in $P_1\sigma$ and (b) the eigenvariables of ($**$) do not occur in $P_2\sigma$. This leads to the semiunification problem

$$\big\{(A_2 * \langle\bar{a}\rangle, A_1 * \langle\bar{a}\rangle), (A_3 * \langle\bar{a}\rangle, A_1 * \langle\bar{a}\rangle), (A_4 * \langle\bar{a}\rangle, A_1 * \langle\bar{a}\rangle)\big\},$$

where $\bar{a}$ are the free variables in P_1. Let δ_1 be the most general semi-unifier. Next, determine the most general semi-unifier δ_2 of

$$\big\{(A_3\delta_1 * \langle\bar{b}\rangle, A_1\delta_1 * \langle\bar{b}\rangle), (A_4\delta_1 * \langle\bar{b}\rangle, A_1\delta_1 * \langle\bar{b}\rangle)\big\},$$

where $\bar{b}$ are the free variables in $P_2\delta_1$. We obtain:

$$
\begin{aligned}
A_1\delta_1\delta_2 &= A(c_1, \ldots, c_r) \\
A_2\delta_1\delta_2 &= A(g_1(d_1, \ldots, d_s), \ldots, g_r(d_1, \ldots, d_s)) \\
A_3\delta_1\delta_2 &= A(g_1(t_1, \ldots, t_s), \ldots, g_r(t_1, \ldots, t_s)) \\
A_4\delta_1\delta_2 &= A(g_1(t'_1, \ldots, t'_s), \ldots, g_r(t'_1, \ldots, t'_s))
\end{aligned}
$$

Since the c_i do not occur in $P_2\delta_1\delta_2$, c_i can be replaced by $g_i(d'_1, \ldots, d'_s)$. Finally, replace $(\forall_B\text{-}\alpha)A$ by $(\forall z_1 \ldots z_s)A(g_1(z_1, \ldots, z_s), \ldots, g_r(z_1, \ldots, z_s))$. (Any permutation of $z_1 \ldots z_s$ can be chosen.)

Correction of cuts To correct cuts in the general case, we associate with each universal or existential cut α_i the set of strong propositional premises $\mathrm{Prm}_s(\alpha_i)$ and weak propositional premises $\mathrm{Prm}_w(\alpha_i)$. Recall that $\forall$ ($\exists$)-introduction is strong (weak) on the right side and weak (strong) on the left side. Thus, $\mathrm{Prm}_s(\alpha_i)$ is the set of those formulas A_j that are ancestors to the cut formula on the strong side of the cut (A_1, A_2 in Example 5.7), and $\mathrm{Prm}_w(\alpha_i)$ is the set of those formulas A_j that are ancestors to the cut formula on the weak side of the cut (A_4, A_5). Let $\mathcal{D} = \bigcup_{\alpha_i} \mathrm{Prm}_s(\alpha_i)$

Define a partial order $\leq$ on $\mathcal{D}$, according to where in the proof A_j is quantified to yield the cut formula $(\forall_{\mathrm{B}}\text{-}\alpha_i)A$: $A_j \leq A_k$ if A_j is quantified below A_k ($A_2 \leq A_1$). The *exclusion area* $D(A_j)$ of the proof corresponding to A_j is the part above the end sequent and below the premise of this quantifier inference ($D(A_1) = P_1$, $D(A_2) = P_2$).

Balancing cuts Select a maximal element $A_j \in \mathcal{D}$ and compute the most general semi-unifier σ_j of the problem

$$\begin{aligned}&\big\{(A_k * \langle a_1, \ldots, a_n\rangle, A_j * \langle a_1, \ldots, a_n\rangle) \bigm| A_k \in \mathrm{Prm}_w(\alpha_i)\big\} \cup \\ \cup &\big\{(A_l * \langle a_1, \ldots, a_n\rangle, A_j * \langle a_1, \ldots, a_n\rangle) \bigm| A_l \in \mathrm{Prm}_s(\alpha_i), A_j \not\leq A_l\big\}\end{aligned}$$

where $A_j \in \mathrm{Prm}_s(\alpha_i)$ and $a_1, \ldots, a_n$ are the free variables in $D(A_j)$. Apply σ_j to the preproof and repeat this process for $\mathcal{D} := (\mathcal{D} \setminus A_j)\sigma_j$ until $\mathcal{D} = \emptyset$.

Call a free variable in A_j *critical for* A_j if it does not occur in $D(A_j)$ and let $\mathrm{crit}(A_j)$ be the set of all free variables critical for A_j. A variable is *critical for the cut* α_i if it is critical for one of its strong premises.

The critical variables of a strong premise A_j of α_j are the potential eigenvariables for the introduction of quantifiers on A_j: The above semi-unifications make all strong and weak premises A' in $D(A_j)$ corresponding to the same cut as A_j substitution instances of A_j (A_2 is a substitution instance of A_1, and A_3, A_4 are substitution instances of both A_1, A_2). By the *-construction in the semi-unification problems above, if $A' = A_j\delta$ for some substitution δ, then δ only acts on $\mathrm{crit}(A_j)$. Note that the critical variables fulfill the eigenvariable condition.

If A_j and A_k are two premises of the cut α_i, then the critical variables of A_j do not occur in A_k and vice versa (If $c \in \mathrm{crit}(A_j)$ and $A_j \leq A_k$ then c occurs in $D(A_k)$ and hence cannot be critical for A_k. If c would occur in A_k, then it would also occur in a weak premise of the cut (by the above semi-unifications), but this premise is in $D(A_j)$. If, on the other hand, A_k is in $D(A_j)$, then c does not occur in A_k by definition). Critical variables for one cut premise are not critical variables for any other cut (For any two premises A_j and A_k, either A_j is in $D(A_k)$ or vice versa).

Unifying premises Now let $A_j(c_1, \ldots, c_s)$ be one of the possibly several $\leq$-minimal strong premises of the cut α_i, where $c_1, \ldots, c_s$ are the critical variables of A_j. A_j is the least general of the strong premises and therefore determines the term structure of the cut formula (A_2 in the example). Unify every other premise A' of α_i with $A_j\delta$, where δ is a a disjoint canonical renaming of the critical variables of A_j. The unifier acts only on *critical* variables of *this cut*. This makes all strong premises of α_i equal up to renaming of critical variables. Recall that the weak premises are substitution instances of A_j and hence, are now of the form $A_j(t_1, \ldots, t_s)$. Replace the cut formula $(\forall_{\mathrm{B}}\text{-}\alpha_i)A$ by $(\forall v_1) \ldots (\forall v_s)A(v_1, \ldots, v_s)$ ($(\exists_{\mathrm{B}}\text{-}\alpha_i)A$ by $(\exists v_1) \ldots (\exists v_s)A(v_1, \ldots, v_s)$). Repeat this step for every cut in the preproof. The resulting proof is uniquely determined up to the order of the quantifiers in cut formulas.

The unifying of premises may influence other cuts, but since critical variables are disjoint for different cuts, this has no effect on other cuts being balanced or unified. All correction steps with exception of the last one are most general and forced by the information provided by the proof analysis and end sequent. Hence, if the correction fails at any step, or if eigenvariable conditions on variables introduced in the construction of the preproof are violated, there is no proof extending the preproof. $\square$

5.8. Corollary *k-Provability is decidable for $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$.*

5.9. Corollary *k/l-Compressibility is decidable for $\mathbf{LK}_{\mathrm{B}}^{\Pi\Sigma}$.*

5.10. *Remark* The term depth d' of the constructed proof can be very roughly bounded by $d' \leq d \cdot 2^{m \cdot l^l}$, where d is the maximal term depth and m the number of quantified variables in the given end sequent $\Pi \to \Lambda$, and l is the length of the proof analysis.

The construction of the preproof for $\Pi \to \Lambda$ introduces at most m new variables in each step, and at most ml overall. The correction of a strong premise introduces at most $(l-1)v$ variables, where v is the current number of variables. The disappearance of a variable in a unification step increses the term depth at most by a factor of 2. If every bound variable occurs only once in the end sequent, then $d' = d$.

6 Conclusion

Two fundamental distinctions have been made in this paper:

(a) The distinction between systems that introduce one (or any fixed number) quantifier and systems that introduce blocks (an unknown number) of quantifiers of the same type in one introduction. Our results show that a committment on the *form* of these blocks of quantifiers, while irrelevant for cut elimination, is disadvantageous for the algorithmic introduction of cuts into a given proof. This is generally the case with constructions that depend on operations on the term structure, e.g. when generalizing proofs, and is essentially due to the fact that second order unification problems (that correspond to single introduction of quantifiers) do not have most general solutions, in contrast to semi-unification problems (that correspond to block introduction of quantifiers, cf. Baaz [1993])

(b) The distinctions between linear and tree-like ways to write proofs. Until the 1950s, linear notation of proofs was commonplace in logic, but since then has almost disappeared. In computer science, linear proofs have been reintroduced, cf. resolution deductions where one and the same clause is used several times. The more space efficient linear notation, however, has serious drawbacks when the relationship between quantifiers in a given proof is investigated.

The problem of structuring of proofs itself will be of importance to computer science, since it is closely related to structuring of *programs*. If we conceive of proof complexity as the degree of entanglement (e.g., as the topological genus of the proof analysis, cf. Statman [1974]), then structuring means algorithmic simplification.

For proof theory, the significance of the problem is that it enables us to separate model-theoretically indistinguishable systems according to their structural properties (cf. (a), (b) above). For a detailed discussion of this aspect, cf. G. Kreisel's postscript to Baaz and Pudlák [1993].

References

Baaz, M.

[1993] Note on the existence of most general semi-unifiers. In *Arithmetic, Proof Theory and Computational Complexity*, P. Clote and J. Krajíček, editors, pp. 19–28. Oxford University Press.

Baaz, M. and P. Pudlák.

[1993] Kreisel's conjecture for $L\exists_1$. In *Arithmetic, Proof Theory and Computational Complexity*, P. Clote and J. Krajíček, editors, pp. 29–59. Oxford University Press.

Buss, S. R.

[1991] The undecidability of k-provability. *Ann. Pure Appl. Logic*, **53**, 75–102.

Farmer, W. M.

[1991] A unification-theoretic method for investigating the k-provability problem. *Ann. Pure Appl. Logic*, **51**, 173–214.

Gentzen, G.

[1934] Untersuchungen über das logische Schließen I–II. *Math. Z.*, **39**, 176–210, 405–431.

Kfoury, A. J., J. Tiuryn, and P. Urzyczyn.

[1990] The undecidability of the semi-unification problem. In *Proc. 22nd ACM STOC*, pp. 468–476. journal version to appear in *Inf. Comp.*

KRAJÍČEK, J. and P. PUDLÁK.
[1988] The number of proof lines and the size of proofs in first order logic. *Arch. Math. Logic*, **27**, 69–84.

PARIKH, R. J.
[1973] Some results on the length of proofs. *Trans. Am. Math. Soc.*, **177**, 29–36.

PUDLÁK, P.
[1988] On a unification problem related to Kreisel's conjecture. *Comm. Math. Univ. Carol.*, **29**(3), 551–556.

STATMAN, R.
[1974] *Structural Complexity of Proofs*. PhD thesis, Stanford University.

TAIT, W. W.
[1968] Normal derivability in classical logic. In *The Syntax and Semantics of Infinitary Languages*, J. Barwise, editor, pp. 204–236. Springer, Berlin.