Towards Algorithmic Cut-Introduction*

Stefan Hetzl[1], Alexander Leitsch[2], and Daniel Weller[1]

[1] Institut für Diskrete Mathematik und Geometrie, Technische Universität Wien
[2] Institut für Computersprachen, Technische Universität Wien

Abstract. We describe a method for abbreviating an analytic proof in classical first-order logic by the introduction of a lemma. Our algorithm is based on first computing a compressed representation of the terms present in the analytic proof and then a cut-formula that realizes such a compression. This method can be applied to the output of automated theorem provers, which typically produce analytic proofs.

1 Introduction

Computer-generated proofs are typically analytic, i.e. they only contain logical material that also appears in the theorem shown. This is due to the fact that analytic proof systems have a considerably smaller search space which makes proof-search practically feasible. In the case of the sequent-calculus, proof-search procedures work on the cut-free fragment only. But also resolution is essentially analytic as all clauses derive from the formula that is shown.

One interesting property of non-analytic proofs is their considerably smaller length. The exact difference depends on the logic (or theory) under consideration, but it is typically enormous. In (classical and intuitionistic) first-order logic there are proofs with cut of length n whose theorems have only cut-free proofs of length 2_n (where $2_0 = 1$ and $2_{n+1} = 2^{2_n}$). The length of a proof plays an important role in many situations such as human readability, space requirements and time requirements for proof checking (also in applications such as proof carrying code). For most of these situations general-purpose data compression methods cannot be used as the compressed representation is not a proof any more. It is therefore of high practical interest to develop proof-search methods which produce non-analytic and hence potentially much shorter proofs. The difficulty in devising such methods is that it seems impossible to come up with a method for finding useful cut-formulas *during proof search*. In this paper we take a different angle at the problem: we start with a cut-free proof and abbreviate it by computing useful cuts based on a structural analysis of the cut-free proof.

There is another, more theoretical, motivation which derives from the foundations of mathematics: most of the central mathematical notions have developed from the observation that many proofs share common structures and steps of

* This work was supported by a Marie Curie Intra European Fellowship within the 7th European Community Framework Programme and by the projects P-22028-N13 and I-603 N18 of the Austrian Science Fund (FWF).

N. Bjørner and A. Voronkov (Eds.): LPAR-18, LNCS 7180, pp. 228–242, 2012.

reasoning. Encapsulating those leads to a new abstract notion, like that of a group or a vector space. Such a notion then builds the base for a whole new theory whose importance stems from the pervasiveness of its basic notions in mathematics. From a logical point of view this is the introduction of cuts into an existing proof database. While we cannot claim to contribute much to the understanding of such processes by the current technical state of the art, this second motivation is still worthwhile to keep in mind, if only to remind ourselves that we are dealing with a difficult problem here.

Work on cut-introduction can be found at a number of different places in the literature. Closest to our approach are [14] which is an algorithm for the introduction of atomic cuts that is capable of exponential proof compression and the method [2] for propositional logic which is shown to never increase the size of proofs more than polynomially. The work [1] is studying a different approach to cut-introduction which is based on filling a so-called proof skeleton with formulas in order to obtain a proof with cuts. Yet another approach to the compression of first-order proofs by introduction of definitions is [13]. A way to use focusing to avoid proving atomic subgoals twice which results in a proof with atomic cuts can be found in [8].

In this paper we consider classical first-order logic and treat the problem of introducing a cut that contains a single quantifier. While this is a modest class, the present algorithm is to the best of our knowledge the first for the introduction of quantified non-analytic cuts. The class being simple has the further advantage of allowing a clear exposition of the basic principles of the algorithm. After some preparation in Sections 2 and 3 we describe in Section 4 a calculus that allows to compute compressed representation ("decompositions") of the terms present in a cut-free proof. In Section 5 we show how to find a cut-formula that realizes such a decomposition and in Section 6 we discuss how to further improve the choice of the cut-formula. Some of the proofs are left out from this paper; the reader interested in all details is referred to the technical report [6].

2 Proofs and Herbrand-Sequents

A *sequent* is an ordered pair of sets of formulas (Γ, Δ) written as $\Gamma \rightarrow \Delta$. We use the sequent calculus $\mathbf{G3c} + \mathrm{Cut}_{\mathrm{cs}}$[1] from [12] and denote it by **LK**. An *instance* of $\forall x_1 \cdots \forall x_n\, A$ or $\exists x_1 \cdots \exists x_n\, A$ (for A quantifier-free) is a formula of the form $A[x_1\backslash t_1, \ldots, x_n\backslash t_n]$. A *strong quantifier* is a $\forall$ ($\exists$) quantifier with positive (negative) polarity. We distinguish some important subsets of sequents.

Definition 1. *A* prenex sequent *is a sequent containing only prenex formulas. A prenex sequent without strong quantifiers is called a* Σ_1-sequent. *A* Σ_1*-sequent in which every formula has at most one quantifier is called a* simple sequent.

The notion of instance extends in a straightforward way to Σ_1-sequents. In this section, we will primarily work with Σ_1-sequents which does not constitute

[1] $\mathbf{G3c} + \mathrm{Cut}_{\mathrm{cs}}$ has no structural rules and all its rules are invertible.

a substantial restriction as one can transform every sequent into a validity-equivalent Σ_1-sequent by skolemisation and prenexification.

Definition 2. *Let $\Gamma \rightarrow \Delta$ be a Σ_1-sequent. Then $\Gamma' \rightarrow \Delta'$ is called* Herbrand-sequent of $\Gamma \rightarrow \Delta$ *if it is a tautology and consists of instances of $\Gamma \rightarrow \Delta$. The* complexity of a Herbrand-sequent *is defined as $|\Gamma' \rightarrow \Delta'| = |\Gamma'| + |\Delta'|$, where $|\ |$ denotes cardinality.*

Example 1. Consider the language containing a constant symbol a, a unary function symbol f and a unary predicate symbol P and the sequent

$$Pa, \forall x\,(Px \supset Pfx) \rightarrow Pf^m a$$

in this language (we omit parentheses around the argument of a unary symbol). This sequent has a Herbrand-sequent

$$Pa, Pa \supset Pfa, \ldots, Pf^{m-1}a \supset Pf^m a \rightarrow Pf^m a$$

of complexity $m+2$. Note that this Herbrand-sequent is of minimal complexity.

The length of a proof π, written as $|\pi|$, is defined as the number of inferences. The following result is shown in [3].

Theorem 1. *Let $s\colon \Gamma \rightarrow \Delta$ be a Σ_1-sequent and π a cut-free proof of s. Then there is a Herbrand-sequent $s'\colon \Gamma' \rightarrow \Delta'$ of s s.t. $|s'| \leq |\pi|$.*

Note that given an Herbrand-sequent s' of s one can find a cut-free proof of s from s' by quantifier introductions. Combining this with a propositional proof of s' one obtains a cut-free proof of s. Assuming that π is cut-free is essential for the above theorem to hold. The well-known non-elementary growth of cut-elimination [9,11,10] shows that it cannot be true if π contains cuts. We generalize the concept of Herbrand-sequent to extended Herbrand-sequents which correspond to proofs with cuts (similarly to [4]): define a $\forall$-*cut* to be a cut with cut-formula $\forall x\ A$, where A is quantifier-free. There are efficient algorithms for extracting Herbrand-sequents from cut-free proofs, see e.g. [7].

Definition 3. *Let $\Gamma \rightarrow \Delta$ be a Σ_1-sequent, let A be a quantifier-free formula, α be a variable not appearing in $\Gamma \cup \Delta \cup \{A\}$ and $s_1, \ldots, s_k$ be terms. A sequent of the form*

$$A[x\backslash\alpha] \supset \bigwedge_{j=1}^{k} A[x\backslash s_j], \Gamma' \rightarrow \Delta'$$

is called extended Herbrand-sequent *if it is a tautology and $\Gamma' \rightarrow \Delta'$ consists of instances of $\Gamma \rightarrow \Delta$. The* complexity *of the above extended Herbrand-sequent s is defined as $|s| = k + |\Gamma'| + |\Delta'|$.*

Proposition 1. *If π is a proof of a Σ_1-sequent $\Gamma \rightarrow \Delta$ and the only cut of π is a $\forall$-cut, then there is an extended Herbrand-sequent s of $\Gamma \rightarrow \Delta$ with $|s| \leq |\pi|$.*

Proof. W.l.o.g. the strong universal quantifier in the cut is introduced from a single eigenvariable α. Obtain a propositional proof π' of an extended Herbrand-sequent by replacing the introductions of the weak universal quantifier by $\land_\mathrm{l}$-inferences and omitting all inferences that introduce quantifiers into the end-sequent.

Example 2. Consider the sequent $Pa, \forall x\,(Px \supset Pfx) \rightarrow Pf^{n^2}a$ for $n \geq 1$. It can be derived by a proof π_n using one $\forall$-cut as follows:

$$\dfrac{\dfrac{\overset{(\chi_1^n)}{\forall x\,(Px \supset Pfx) \rightarrow P\alpha \supset Pf^n\alpha}}{\forall x\,(Px \supset Pfx) \rightarrow \forall x\,(Px \supset Pf^n x)}\,\forall_\mathrm{r} \qquad \overset{(\chi_2^n)}{\forall x\,(Px \supset Pf^n x), Pa \rightarrow P(f^{n^2}a)}}{Pa, \forall x\,(Px \supset Pfx) \rightarrow Pf^{n^2}a}\,\mathrm{cut}$$

where χ_1^n uses the instances $\alpha, f\alpha, \ldots, f^n\alpha$ of the successor-axiom to prove the cut formula and χ_2^n uses instances $a, f^n a, \ldots, f^{(n-1)n}a$ of the cut formula to prove the claim. The extended Herbrand-sequent of this proof is

$$C, Pa, P\alpha \supset Pf\alpha, \ldots, Pf^{n-1}\alpha \supset Pf^n\alpha \rightarrow Pf^{n^2}a$$

where

$$C \;=\; (P\alpha \supset Pf^n\alpha) \supset \bigwedge_{j=0}^{n-1} (Pf^{jn}a \supset Pf^{(j+1)n}a)$$

so it has complexity $2(n+1)$.

We have seen in example 1 that the complexity of the minimal Herbrand-sequent is $n^2 + 2$. So by introducing the cut above we get a quadratic compression. For the case of a single universal quantifier this bound is sharp. As in the cut-free case, one can construct a proof with cut from an extended Herbrand-sequent.

Lemma 1. *If π is a proof of $A \supset B, \Gamma \rightarrow \Delta$, then there are proofs π_1 of $B, \Gamma \rightarrow \Delta$ and π_2 of $\Gamma \rightarrow \Delta, A$ with $|\pi_1| \leq |\pi|$ and $|\pi_2| \leq |\pi|$.*

Proof. For obtaining π_1, replace all ancestors of $A \supset B$ by B and the introducing inferences

$$\frac{\Pi \rightarrow \Lambda, A \quad B, \Pi \rightarrow \Lambda}{A \supset B, \Pi \rightarrow \Lambda}\supset_\mathrm{l} \qquad \text{by} \quad B, \Pi \rightarrow \Lambda\ .$$

For π_2 proceed analogously.

Proposition 2. *Let $\Gamma \rightarrow \Delta$ be a Σ_1-sequent, let $s = A[x\backslash\alpha] \supset \bigwedge_{j=1}^{k} A[x\backslash s_j]$, $\Gamma' \rightarrow \Delta'$ be an extended Herbrand-sequent of $\Gamma \rightarrow \Delta$, ψ be a proof of s and l be the maximal length of a quantifier prefix in $\Gamma \rightarrow \Delta$. Then there is a proof π of $\Gamma \rightarrow \Delta$ having exactly one $\forall$-cut, s as extended Herbrand-sequent and satisfies $|\pi| = \mathrm{O}(|\psi| + |\Gamma \rightarrow \Delta| \cdot l)$.*

Proof. By introducing weak quantifiers to derive $\Gamma \rightarrow \Delta$ from $\Gamma' \rightarrow \Delta'$ and by replacing $\bigwedge_{j=1}^{k}$ by universal quantifiers, obtain a proof π_1 of $A[x\backslash\alpha] \supset \forall x\, A, \Gamma \rightarrow \Delta$ with $|\pi_1| \leq |\psi| + |\Gamma \rightarrow \Delta| \cdot l + 1$. By Lemma 1 there are proofs π_2 of $\Gamma \rightarrow \Delta, A[x\backslash\alpha]$ and π_3 of $\forall x\, A, \Gamma \rightarrow \Delta$ with $|\pi_2| \leq |\pi_1|$ and $|\pi_3| \leq |\pi_1|$. Define π as

$$\dfrac{\dfrac{\overset{(\pi_2)}{\Gamma \rightarrow \Delta, A[x\backslash\alpha]}}{\Gamma \rightarrow \Delta, \forall x\, A}\,\forall_{\mathrm{r}} \qquad \overset{(\pi_3)}{\forall x\, A, \Gamma \rightarrow \Delta}}{\Gamma \rightarrow \Delta}\,\mathrm{cut} \quad ,$$

and observe $|\pi| = |\pi_2| + |\pi_3| + 2 \leq 2(|\psi| + |\Gamma \rightarrow \Delta| \cdot l + 2)$.

3 Cut-Elimination and Cut-Introduction

Let $\mathcal{S}\colon \{\sigma_1, \ldots, \sigma_n\}$ be a set of substitutions; then by $(\Gamma \rightarrow \Delta)\mathcal{S}$ we denote the sequent $\Gamma\sigma_1, \ldots, \Gamma\sigma_n \rightarrow \Delta\sigma_1, \ldots, \Delta\sigma_n$.

Proposition 3. *Let $A[x\backslash\alpha] \supset \bigwedge_{j=1}^{k} A[x\backslash s_j], \Gamma' \rightarrow \Delta'$ be an extended Herbrand sequent of a Σ_1-sequent $\Gamma \rightarrow \Delta$, then $(\Gamma' \rightarrow \Delta')\{[\alpha\backslash s_j] \mid 1 \leq j \leq k\}$ is a Herbrand-sequent of $\Gamma \rightarrow \Delta$.*

Proof. Consider the proof π of $\Gamma \rightarrow \Delta$ constructed in the proof of Proposition 2: by reducing the universal quantifier of the cut using any standard method for cut-reduction we obtain a proof π' having only quantifier-free cuts whose Herbrand sequent is $(\Gamma' \rightarrow \Delta')\{[\alpha\backslash s_j] \mid 1 \leq j \leq k\}$.

So we have seen in the previous section that the first-order structure of a Herbrand-sequent corresponds to that of a cut-free proof and that of an extended Herbrand-sequent to that of a proof with a single $\forall$-cut. These observations, together with Proposition 3 that describes cut-elimination on these structures motivates the following statement of the

Cut-introduction Problem for a Single $\forall$-cut: Given a simple sequent $\Gamma \rightarrow \Delta$ and a Herbrand-sequent $\Gamma' \rightarrow \Delta'$ of $\Gamma \rightarrow \Delta$, find an extended Herbrand-sequent $s = A[x\backslash\alpha] \supset \bigwedge_{j=1}^{k} A[x\backslash s_j], \Gamma'' \rightarrow \Delta''$ of $\Gamma \rightarrow \Delta$ s.t.

$$\Gamma' \rightarrow \Delta' \;=\; (\Gamma'' \rightarrow \Delta'')\{[\alpha\backslash s_j] \mid 1 \leq j \leq k\}.$$

In order to describe our solution of the above problem, we first give some definitions. For a sequence of terms $\boldsymbol{t} = t_1, \ldots, t_n$ and a formula $F(x)$ (which may or may not contain x), we write $F(\boldsymbol{t})$ for the sequence of formulas $F(t_1), \ldots, F(t_n)$.

For the rest of this section, we fix a simple sequent $s = \forall x\; F_1(x), \ldots, \forall x\; F_n(x) \rightarrow \exists x\; F_{n+1}(x), \ldots, \exists x\; F_m(x)$ and a Herbrand-sequent $s' = F_1(\boldsymbol{t_1}), \ldots, F_n(\boldsymbol{t_n}) \rightarrow F_{n+1}(\boldsymbol{t_{n+1}}), \ldots, F_m(\boldsymbol{t_m})$ of s where $\boldsymbol{t_i} = t_{i,1}, \ldots, t_{i,n_i}$.

We define the *termset* $T(s, s') = \{t_{i,j} \mid i \leq m, j \leq n_i\}$. The following result shows how the termset can give rise to a solution to the cut-introduction problem.

Proposition 4. *Let $U = \{u_1, \ldots, u_\ell\}$ and $S = \{s_1, \ldots, s_k\}$ be sets of terms such that $T(s, s') = \{u_i[\alpha\backslash s_j] \mid i \leq \ell, j \leq k\}$. Then*

$$s' = (F_1(\boldsymbol{u}), \ldots, F_n(\boldsymbol{u}) \to F_{n+1}(\boldsymbol{u}), \ldots, F_m(\boldsymbol{u}))\{[\alpha\backslash s_j] \mid 1 \leq j \leq k\}$$

Proof. Let s, s' be as above. Since $T(s, s') = \{u_i[\alpha\backslash s_j] \mid i \leq \ell, j \leq k\}$, for every $i \leq m, j \leq n_i$ there exist p, q such that $t_{i,j} = u_p[\alpha\backslash s_q]$. Inversely, for every p, q there are i, j s.t. $t_{i,j} = u_p[\alpha\backslash s_q]$.

The first phase of our approach to cut-introduction for simple sequents consists in determining sets U, S as in Proposition 4. Such sets then induce a schematic extended Herbrand-sequent.

Definition 4. *Let U, S be as in Proposition 4. Then the* induced schematic extended Herbrand-sequent *is*

$$X\alpha \supset \bigwedge_{j=1}^{k} Xs_j, F_1(\boldsymbol{u}), \ldots, F_n(\boldsymbol{u}) \to F_{n+1}(\boldsymbol{u}), \ldots, F_m(\boldsymbol{u})$$

where X is a monadic second-order variable.

Let s'' be the induced schematic Herbrand-sequent corresponding to s, s', U, S. The second phase is then to determine a substitution $\sigma = [X\backslash\lambda x.\psi]$ s.t. $s''\sigma$ is a tautology. We will show that such a substitution σ always exists.

4 A Calculus of Decompositions

We will now describe our algorithmic solution for the first phase. For this whole section we fix a variable α and a set of ground terms $T = \{t_1, \ldots, t_n\}$.

Definition 5. *A* decomposition *of T is a pair of sets of terms, written as $U \circ S$, s.t. $T = \{u[\alpha\backslash s] \mid u \in U, s \in S\}$.*

Of course, every T possesses a trivial decomposition by letting $U = \{\alpha\}$ and $S = T$. Keeping our aim of proof compression in mind we are looking for a decomposition $U \circ S$ with $|U| + |S| < |T|$. We will develop a calculus of decompositions along similar lines as a resolution calculus. For a set of terms W and a term v we write $W[x\backslash v]$ for $\{w[x\backslash v] \mid w \in W\}$ and $v[x\backslash W]$ for $\{v[x\backslash w] \mid w \in W\}$ and $\mathrm{V}(v)$ for the set of variables occurring in v.

Definition 6. *We define the following axioms and rules for the manipulation of decompositions. Axioms are of the form*

$$\frac{}{\{\alpha\} \circ \{t\}}\ \mathrm{ax} \quad \textit{if } t \in T.$$

The rules are

$$\frac{U_1 \circ S \quad U_2 \circ S}{(U_1 \cup U_2) \circ S}\ \mathrm{R} \qquad \frac{U \circ S_1 \quad U \circ S_2}{U \circ (S_1 \cup S_2)}\ \mathrm{L} \qquad \frac{U[\alpha\backslash v] \circ S}{U \circ v[\alpha\backslash S]} \to \qquad \frac{U \circ v[\alpha\backslash S]}{U[\alpha\backslash v] \circ S} \leftarrow$$

for any term v with $\alpha \in \mathrm{V}(v)$.

To simplify the notation, we often omit the braces of singleton sets. The above calculus is sound in the sense that it only derives decompositions of subsets of T. More interestingly, it is also complete in the following sense:

Proposition 5. *If T has a decomposition $U \circ S$ then $U \circ S$ is derivable using* $\mathrm{ax}, \leftarrow, \mathrm{R}, \mathrm{L}$.

Proof. Let $T = \{u_i[\alpha \backslash s_j] \mid 1 \leq i \leq m, 1 \leq j \leq k\}$. First, observe that $u_i \circ s_j$ is derivable by a single left-shift. Secondly, we have

$$\frac{u_1 \circ s_j \quad \cdots \quad u_m \circ s_j}{\{u_1, \ldots, u_m\} \circ s_j}\ \mathrm{R} \cdots \mathrm{R} \quad \text{and finally}$$

$$\frac{\{u_1, \ldots, u_m\} \circ s_1 \quad \cdots \quad \{u_1, \ldots, u_m\} \circ s_k}{\{u_1, \ldots, u_m\} \circ \{s_1, \ldots, s_k\}}\ \mathrm{L} \cdots \mathrm{L} \quad .$$

A search for decompositions in this calculus is not very efficient due to the indeterministic nature of the $\leftarrow$-inferences. Fortunately, it is possible to work with most general forms of decompositions, thereby getting (almost) rid of the shift-rules. The rest of this section is devoted to the development of such a most general calculus and a search procedure for it.

Definition 7. *A decomposition $U \circ S$ is called* right normal *if $U = U'[\alpha \backslash v]$ implies $v = \alpha$.*

A first but essential result is that right normal forms are unique. To show this we need some auxiliary notions.

Definition 8. *For terms t, v with $\alpha \in \mathrm{V}(v) \cap \mathrm{V}(t)$ we write $t \geq v$ if there is w s.t. $t = w[\alpha \backslash v]$.*

It will be convenient to work with an inductive definition of the set of right shift terms of a term.

Definition 9. *Let $\alpha \in \mathrm{V}(t)$ and define a set* $\mathrm{rsterms}(t)$ *as follows:* $\mathrm{rsterms}(\alpha) = \{\alpha\}$ *and* $\mathrm{rsterms}(f(t_1, \ldots, t_n)) = \{\alpha, f(t_1, \ldots, t_n)\} \cup \bigcap_{i=1, \alpha \in \mathrm{V}(t_i)}^{n} \mathrm{rsterms}(t_i)$.

Example 3. $f(c, g(\alpha)) \geq g(\alpha)$ because $f(c, g(\alpha)) = f(c, \alpha)[\alpha \backslash g(\alpha)]$ but on the other hand $f(\alpha, g(\alpha)) \not\geq g(\alpha)$ because every w with $f(\alpha, g(\alpha)) = w[\alpha \backslash g(\alpha)]$ would have to start with f whose first argument can then no longer be filled. Furthermore $t \geq t$ and $t \geq \alpha$ for all terms t. We have $\mathrm{rsterms}(f(c, g(\alpha))) = \{\alpha, g(\alpha), f(c, g(\alpha))\}$ and $\mathrm{rsterms}(f(\alpha, g(\alpha))) = \{\alpha, f(\alpha, g(\alpha))\}$.

Lemma 2. *Let $\alpha \in \mathrm{V}(t)$. Then $v \in \mathrm{rsterms}(t)$ iff $t \geq v$.*

Lemma 3. *$\geq$ is a partial order of the set of terms containing α.*

Note that $\geq$ is not a total order on the set of terms containing α. For example, consider the terms $f(\alpha), g(\alpha)$, then clearly $\alpha \leq f(\alpha)$ and $\alpha \leq g(\alpha)$ but $f(\alpha)$ and $g(\alpha)$ are incomparable. On the other hand:

Lemma 4. *Let $\alpha \in \mathrm{V}(t)$, then $\geq$ is a total order of* $\mathrm{rsterms}(t)$.

For a non-empty set of terms U we define $\mathrm{rsterms}(U) = \bigcap_{u \in U} \mathrm{rsterms}(u)$. Note that $\geq$ on $\mathrm{rsterms}(U)$ is total as well because it is a substructure of $\geq$ on $\mathrm{rsterms}(u)$ for any $u \in U$.

Proposition 6. *Every decomposition has a unique right normal form.*

Proof. Let $U \circ S$ be a decomposition with two different right normal forms $U_1 \circ S_1$ and $U_2 \circ S_2$. Then there are terms v_1, v_2 s.t. $U = U_1[\alpha \backslash v_1] = U_2[\alpha \backslash v_2]$ and

$$\frac{U_1[\alpha \backslash v_1] \circ S}{U_1 \circ v_1[\alpha \backslash S]} \rightarrow \quad \text{and} \quad \frac{U_2[\alpha \backslash v_2] \circ S}{U_2 \circ v_2[\alpha \backslash S]} \rightarrow$$

where $S_1 = v_1[\alpha \backslash S]$ and $S_2 = v_2[\alpha \backslash S]$. As $v_1, v_2 \in \mathrm{rsterms}(U)$ we can apply Lemma 4 to obtain w.l.o.g. $v_1 \geq v_2$. As $U_1 \circ S_1 \neq U_2 \circ S_2$ we have $v_1 \neq v_2$ hence $v_1 > v_2$, i.e. there is a $w \neq \alpha$ s.t. $v_1 = w[\alpha \backslash v_2]$. Therefore $U = U_1[\alpha \backslash v_1] = U_1[\alpha \backslash w][\alpha \backslash v_2] = U_2[\alpha \backslash v_2]$ hence $U_2 = U_1[\alpha \backslash w]$ which is not in right normal form.

In light of the above proposition we will henceforth speak about *the* right normal form of a decomposition. Note that the right normal form of a term t can be obtained from using the maximal element of $\mathrm{rsterms}(t)$ as a right shift term.

Lemma 5 (Lifting Lemma for L). *If*

$$\frac{U \circ S_1 \quad U \circ S_2}{U \circ (S_1 \cup S_2)} \ \mathrm{L}$$

and $U' \circ S_1'$ is the right normal form of $U \circ S_1$ and $U' \circ S_2'$ is the right normal form of $U \circ S_2$, then

$$\frac{U' \circ S_1' \quad U' \circ S_2'}{U' \circ (S_1' \cup S_2')} \ \mathrm{L}$$

where $U' \circ (S_1' \cup S_2')$ is the right normal form of $U \circ (S_1 \cup S_2)$.

Proof. Being in right normal form depends only on the U-part of the decomposition. Therefore, if $U' \circ S_i'$ is in right normal form so is $U' \circ (S_1' \cup S_2')$.

Right normality is more problematic when it comes to the R-rule. Consider the two decompositions $\{f_1(\alpha), f_2(\alpha)\} \circ \{f(g(c))\}$ and $\{\alpha\} \circ \{h(g(c))\}$. Both are right normal and they cannot be combined with a R-rule. However shifting both to the left gives $\{f_1(f(\alpha)), f_2(f(\alpha))\} \circ \{g(c)\}$ and $\{h(\alpha)\} \circ \{g(c)\}$ which can be combined with R yielding $\{f_1(f(\alpha)), f_2(f(\alpha)), h(\alpha)\} \circ \{g(c)\}$ which is again right normal. Note that shifting by $f(g(\alpha))$ and $h(g(\alpha))$ instead would give $\{f_1(f(g(\alpha))), f_2(f(g(\alpha)))\} \circ \{c\}$ and $\{h(g(\alpha))\} \circ \{c\}$ whose combination by R would no longer be right normal. So if a R-combination is made possible by applying left shifts before, the minimal such left shifts are most general in the sense that they yield a right normal conclusion of the R-rule. Let us make this precise:

Definition 10. *For right normal decompositions D_1, D_2, D_3, abbreviate*

$$\dfrac{\dfrac{D_1}{D_1'} \leftarrow \quad \dfrac{D_2}{D_2'} \leftarrow}{D_3}\ \mathrm{R} \qquad \textit{by} \qquad \dfrac{D_1 \quad D_2}{D_3}\ \mathrm{R_{mg}}\ .$$

Lemma 6 (Lifting Lemma for R). *If* $\dfrac{U_1 \circ S \quad U_2 \circ S}{(U_1 \cup U_2) \circ S}\ \mathrm{R}$ *and $U_1' \circ S_1$ is the right normal form of $U_1 \circ S$ and $U_2' \circ S_2$ is the right normal form of $U_2 \circ S$, then* $\dfrac{U_1' \circ S_1 \quad U_2' \circ S_2}{V \circ T}\ \mathrm{R_{mg}}$ *where $V \circ T$ is the right normal form of $(U_1 \cup U_2) \circ S$.*

The calculus consisting of $\mathrm{ax}, \mathrm{R_{mg}}, \mathrm{L}$ is sound in the sense that only right normal forms of subsets of T are derived and complete in the following sense:

Theorem 2. *If T has a decomposition $U \circ S$ then the right normal form of $U \circ S$ is derivable using* $\mathrm{ax}, \mathrm{R_{mg}}, \mathrm{L}$.

Proof. By Proposition 5, there exists a derivation of the right normal form of $U \circ S$ using $\mathrm{ax}, \leftarrow, \mathrm{R}, \mathrm{L}$. We convert this derivation inductively to one using only $\mathrm{ax}, \mathrm{R_{mg}}, \mathrm{L}$ of the same structure bringing every line into right normal form by leaving out the $\leftarrow$-inferences and applying Lemmas 5 and 6 for the L- and R-inferences respectively.

We can observe that w.r.t. the generality of a derivation, the calculus $(\mathrm{ax}, \mathrm{R_{mg}}, \mathrm{L})$ behaves like resolution and $(\mathrm{ax}, \leftarrow, \mathrm{R}, \mathrm{L})$ like ground resolution. It is useful to observe the following algorithmic

Corollary 1. *Let A be the axioms induced by T, let B be the* $\mathrm{R_{mg}}$*-closure of A and let C be the* L*-closure of B. Then C contains the right normal forms of all decompositions of T.*

Proof. By inspection of the completeness proof.

Example 4. The sequent $Pa, \forall x\,(Px \supset Pfx) \rightarrow Pf^{n^2}a$ has a Herbrand-sequent $Pa, Pa \supset Pfa, \ldots, Pf^{n^2-1}a \supset Pf^{n^2}a \rightarrow Pf^{n^2}a$ of size n^2 as in Example 1. For abbreviating it we have to find a decomposition of $T = \{a, fa, \ldots, f^{n^2-1}a\}$. Observe that

$$\frac{\alpha \circ f^{in+0}a \quad \cdots \quad \alpha \circ f^{in+n-1}a}{\{\alpha, f\alpha, \ldots, f^{n-1}\alpha\} \circ f^{in}a}\ \mathrm{R_{mg}}, \ldots, \mathrm{R_{mg}}$$

for all $i \in \{0, \ldots, n-1\}$ and that

$$\frac{\{\alpha, f\alpha, \ldots, f^{n-1}\alpha\} \circ a \quad \cdots \quad \{\alpha, f\alpha, \ldots, f^{n-1}\alpha\} \circ f^{(n-1)n}a}{\{\alpha, f\alpha, \ldots, f^{n-1}\alpha\} \circ \{a, f^n a, \ldots, f^{(n-1)n}a\}}\ \mathrm{L}, \ldots, \mathrm{L}$$

which shows that this final decomposition is in C. This decomposition induces the schematic extended Herbrand-sequent

$$X\alpha \supset \bigwedge_{j=0}^{n-1} Xf^{jn}a, Pa, P\alpha \supset Pf\alpha, \ldots, Pf^{n-1}\alpha \supset Pf^n\alpha \rightarrow Pf^{n^2}a$$

which has complexity $2(n+1)$ and has the structure of the extended Herbrand-sequent of the proof π_n from Example 2.

5 Computing the Propositional Structure

Let

$$s^\star\colon \Gamma, X\alpha \supset \bigwedge_{i=1}^{n} Xs_i \to \Delta$$

be an induced schematic extended Herbrand-sequent (see Definition 4) for some fixed sequents s, s' and a term decomposition of $T(s,s')$ by $U \circ W$. The solution of the second phase consists in finding a substitution $\vartheta\colon \{X \leftarrow \lambda x.F(x)\}$ (where $F(x)$ is a quantifier-free formula which may contain the variable x but no other variable) s.t. the β-normal form of $s^\star\vartheta$ is a valid sequent.

The problem of finding a solution can be simplified by applying our (invertible) version of **LK** to s and decompose the formulas in s down to a set of two sequents of the form

$$\mathcal{S}\colon \{\Gamma \to \Delta, X\alpha;\ Xw_1, \ldots, Xw_n, \Gamma \to \Delta\}.$$

where Γ and Δ are sets of ground formulas, $W\colon \{w_1, \ldots, w_n\}$ is a set of ground terms and α is a constant which does not occur in W. Note that α is basically an eigenvariable, but in this context can be considered as a constant.

Definition 11. *Let s be a sequent, s' a corresponding Herbrand sequent and*

$$s^\star\colon\ \Gamma, X\alpha \supset \bigwedge_{i=1}^{n} Xw_i \to \Delta$$

be a schematic extended Herbrand sequent corresponding to the term decomposition $\mathcal{T}$ of $T(s,s')$ by $U \circ W$ for $W = \{w_1, \ldots, w_n\}$. Then the set of sequents $\mathcal{S}\colon \{s_1, s_2\}$ for

$$s_1 = Xw_1, \ldots, Xw_n, \Gamma \to \Delta,\ s_2 = \Gamma \to \Delta, X\alpha,$$

is called a cut-introduction problem *(CIP) w.r.t. $\mathcal{T}$. s_1 is called the W-sequent, and s_2 the α-sequent of $\mathcal{S}$. The sequent $\mathcal{S}_{\mathrm{const}}\colon \Gamma \to \Delta$ is called the constant part of $\mathcal{S}$.*

Definition 12. *Let $\mathcal{S}$ be a CIP w.r.t. a term decomposition $\mathcal{T}$ and $F(x)$ be a quantifier-free formula s.t. $V(F(x)) \subseteq \{x\}$ and α does not occur in $F(x)$ (we call $F(x)$* admissible *for $\mathcal{S}$). The substitution $\vartheta\colon \{X \leftarrow \lambda x.F(x)\}$ is called a* solution *of $\mathcal{S}$ if $s_1\vartheta\downarrow$ and $s_2\vartheta\downarrow$ are both valid (where $\downarrow$ denotes normalization under β-reduction). $\mathcal{S}$ is called* solvable *if there exists a solution of $\mathcal{S}$.*

Remark 1. The restriction that α does not occur in $F(x)$ is necessary as, in case of solvability, the formula $(\forall x)F(x)$ is the cut-formula of the cut-introduction problem. As α is the eigenvariable of the quantifier-introduction on the left side of the cut, α may not appear in $(\forall x)F(x)$.

From now on we denote by $\mathcal{S}$ a CIP w.r.t. $\mathcal{T}$ where $\mathcal{T}$ is a decomposition of $T(s,s')$ by $U \circ W$ for $W = \{w_1,\dots,w_n\}$, and by $F(x)$ an admissible formula for $\mathcal{S}$.

Definition 13. *Let $s_1 = Xw_1,\dots,Xw_n, A_1,\dots,A_n \rightarrow B_1,\dots,B_m$ and $s_2 = A_1,\dots,A_n \rightarrow B_1,\dots,B_m, X\alpha$ and $\mathcal{S}\colon \{s_1,s_2\}$ be a CIP.*
The formula G: $A_1 \wedge \cdots \wedge A_n \wedge \neg B_1 \wedge \cdots \wedge \neg B_m$ is called the characteristic formula *of $\mathcal{S}$.*
The system $\mathcal{S}'\colon \{Xw_1,\dots,Xw_n, G \rightarrow;\; G \rightarrow X\alpha\}$ is called the characteristic normal form *of $\mathcal{S}$.*

Lemma 7. *ϑ is a solution of a CIP $\mathcal{S}$ iff ϑ solves the characteristic normal form of $\mathcal{S}$.*

Proof. Trivial.

Lemma 8. *Let $\mathcal{S}$ be a CIP w.r.t. $\mathcal{T}$, and let G be the characteristic formula of $\mathcal{S}$. Then $G(w_1),\dots,G(w_n) \rightarrow$ is valid.*

Proof. Let $W = \{w_1,\dots,w_n\}$ and $\mathcal{S} = \{s_1,s_2\}$ such that $s_1 = Xw_1,\dots,Xw_n$, $\Gamma' \rightarrow \Delta'$. By Proposition 4, for the original Herbrand-sequent $\Gamma'' \rightarrow \Delta''$ we have

$$\Gamma'' \rightarrow \Delta'' \subseteq (\Gamma' \rightarrow \Delta')\{\alpha \leftarrow w \mid w \in W\}.$$

Let $\Gamma' = A_1,\dots,A_n$ and $\Delta' = B_1,\dots,B_m$, then $G(\alpha) = A_1 \wedge \cdots A_n \wedge \neg B_1 \wedge \cdots \wedge \neg B_m$. The sequent $G(w_1),\dots,G(w_n) \rightarrow$ can be transformed (via substitution application, and applying $\wedge\colon l$ and $\neg\colon l$ rules backwards) to the equivalent sequent

$$\begin{aligned}&s_1''\colon (A_1,\dots,A_k)\{\alpha \leftarrow w_1\},\dots,(A_1,\dots,A_k)\{\alpha \leftarrow w_n\} \rightarrow\\ &(B_1,\dots,B_m)\{\alpha \leftarrow w_1\},\dots,(B_1,\dots,B_m)\{\alpha \leftarrow w_n\} =\\ &(\Gamma' \rightarrow \Delta')\{\alpha \leftarrow w \mid w \in W\}.\end{aligned}$$

But

$$\Gamma'' \rightarrow \Delta'' = (\Gamma' \rightarrow \Delta')\{\alpha \leftarrow w \mid w \in W\} = s_1'',$$

as $\Gamma'' \rightarrow \Delta''$ is a Herbrand-sequent s_1'' is valid. Therefore $G(w_1),\dots,G(w_n) \rightarrow$ is valid.

Theorem 3. *Let $\mathcal{S}$ be a system in characteristic normal form and let G be the characteristic formula. Then $\mathcal{S}$ is solvable and $\{X \leftarrow \lambda x.G\{\alpha \leftarrow x\}\}$ is a solution of $\mathcal{S}$.*

Proof. Let $\mathcal{S}\colon \{s_1,s_2\}$ be a cut-introduction problem for $s_1 = Xw_1,\dots,Xw_n,\Gamma' \rightarrow \Delta'$, $s_2 = \Gamma' \rightarrow \Delta', X\alpha$, and $\Gamma' = A_1,\dots,A_k$, $\Delta' = B_1,\dots,B_m$, and G be the characteristic formula of the problem. We prove that $\theta = \{X \leftarrow \lambda x.G\{\alpha \leftarrow x\}\}$ is a solution of $\mathcal{S}$.

(a) $s_2'\colon s_2\theta\downarrow$ is valid. In fact,

$$s_2' = A_1,\dots,A_k \rightarrow B_1,\dots,B_m, A_1 \wedge \cdots \wedge A_k \wedge \neg B_1 \wedge \cdots \wedge \neg B_m.$$

Note that $(X\alpha)\{X \leftarrow \lambda x.G\{\alpha \leftarrow x\}\}\downarrow = G$.

(b) $s_1'\colon s_1\theta\downarrow$ is valid:

$$\begin{aligned}&s_1' = (Xw_1)\theta\downarrow, \ldots, (Xw_n)\theta\downarrow, \Gamma' \to \Delta' =\\&(\lambda x.G\{\alpha \leftarrow x\})w_1\downarrow, \ldots (\lambda x.G\{\alpha \leftarrow x\})w_n\downarrow, \Gamma' \to \Delta' =\\&G(w_1), \ldots, G(w_n), \Gamma' \to \Delta'.\end{aligned}$$

Since $G(w_1), \ldots, G(w_n) \to$ is valid by Lemma 8, s_1' is valid.

Corollary 2. *Every cut-introduction problem is solvable.*

Proof. By Lemma 7 and Theorem 3.

In fact, once we have a decomposition of the substitution terms we find a canonical solution for the cut-formula. Roughly speaking this solution encodes the whole sequent $\Gamma' \to \Delta'$.

6 Improving the Canonical Solution

In the previous section, we have shown in Theorem 3 that for any CIP $\mathcal{S}$ there exists a solution $\{X \leftarrow \lambda x.G\{\alpha \leftarrow x\}\}$, where G is the characteristic formula of $\mathcal{S}$, such that $|G| = O(|\mathcal{S}|)$. Still for practical application of the method to the structuring of proofs, it will be important to further simplify the solution if possible, since the solution of the CIP corresponds to the cut-formula that is used to structure the proof. As a motivating example, consider the following.

Example 5. Let $\mathcal{S}$ be the CIP of the running example. Then the characteristic formula of $\mathcal{S}$

$$G(\alpha) = Pa \wedge \bigwedge_{0 \leq i < n} (Pf^i\alpha \supset Pf^{i+1}\alpha) \wedge \neg Pf^{n^2}a$$

gives rise to a solution. But there also exists a solution of constant logical complexity, using

$$H(\alpha) = P\alpha \supset Pf^n\alpha$$

which is preferable over the canonical solution based on $G(\alpha)$. Note that $G(\alpha) \models H(\alpha)$ but $H(\alpha) \not\models G(\alpha)$ and that $H(\alpha)$ only contains atoms that contain α.

We will now show that the observations from this example can be generalized and used to simplify the canonical solution. We will focus on characteristic formulas which are in conjunctive normal form. We will first give a sufficient criterion for simplification of such characteristic formulas, and then present an algorithm based on propositional resolution and validity checking that, given a solution, searches for a smaller one. First, note that the canonical solution is most general.

Proposition 7. *Let $\mathcal{S}$ be a CIP and $\vartheta = \{X \leftarrow \lambda x.F\}$ be a solution for $\mathcal{S}$. Then $G\{\alpha \leftarrow x\} \models F$, where G is the characteristic formula of $\mathcal{S}$.*

Proof. By Lemma 7, ϑ is a solution to the characteristic normal form of $\mathcal{S}$, and hence $(G \supset X(\alpha))\{X \leftarrow \lambda x.F\} = G \supset F\{x \leftarrow \alpha\}$ is valid. Therefore $(G \supset F\{x \leftarrow \alpha\})\{\alpha \leftarrow x\} = G\{\alpha \leftarrow x\} \supset F$ is valid.

Note that the converse does not hold: in general, $G \models \top$ but $\{X \leftarrow \lambda x.\top\}$ is not a solution of the CIP of our running example.

Proposition 8. *Let G be a characteristic formula of the CIP $\mathcal{S}$ and assume that G is in conjunctive normal form. Let G' be obtained from G by removing all clauses that do not contain α. Then $\{X \leftarrow \lambda x.G'\{\alpha \leftarrow x\}\}$ is a solution for $\mathcal{S}$.*

Let F be a formula in conjunctive normal form, i.e. $F = \bigwedge_{i\in\{1,\ldots,m\}} C_i$, with clauses $C_i = \bigvee_{j\in\{1,\ldots,n_i\}} L_{i,j}$, where the $L_{i,j}$ are literals. By $\overline{L}$ we denote the dual of a literal L. For two clauses C_i, C_j, if there exists exactly one pair (k, ℓ) such that $L_{i,k} = \overline{L_{j,\ell}}$, we define their *resolvent*

$$\mathrm{res}(C_i, C_j) = \bigvee_{r\in\{1,\ldots,n_i\}\setminus k} L_{i,r} \vee \bigvee_{q\in\{1,\ldots,n_j\}\setminus \ell} L_{j,q}$$

and leave $\mathrm{res}(C_i, C_j)$ undefined otherwise.

Then define

$$\mathcal{R}(F) = \{\mathrm{res}(C_i, C_j) \wedge \bigwedge_{k\in\{1,\ldots,m\}\setminus\{i,j\}} C_k \mid \mathrm{res}(C_i, C_j) \text{ defined}\}.$$

Note that if $G \in \mathcal{R}(F)$ then $|G| < |F|$. Since $C_i \wedge C_j \supset \mathrm{res}(C_i, C_j)$, we have

Lemma 9. *If $H \in \mathcal{R}(F)$ then $F \supset H$ is valid.*

This directly translates to a result on CIPs:

Proposition 9. *Let $\mathcal{S} = \{Xw_1, \ldots, Xw_n, \Gamma \to \Delta,\ \Gamma \to \Delta, X\alpha\}$ be a CIP and $H \in \mathcal{R}(F)$.*

(1) If $F(w_1), \ldots, F(w_n), \Gamma \to \Delta$ is not valid, then $\{X \leftarrow \lambda x.H(x)\}$ is not a solution for $\mathcal{S}$.

(2) If $\Gamma \to \Delta, F(\alpha)$ and $H(w_1), \ldots, H(w_n), \Gamma \to \Delta$ are valid, then $\{X \leftarrow \lambda x.H(x)\}$ is a solution for $\mathcal{S}$.

Proof. For showing (1), assume that $H(w_1), \ldots, H(w_n), \Gamma \to \Delta$ is valid. Then by Lemma 9, $F(w_1), \ldots, F(w_n), \Gamma \to \Delta$ is valid.

For (2), it suffices to show that $\Gamma \to \Delta, H(\alpha)$ is valid, which follows from the same Lemma.

Propositions 7, 8 and 9 suggest a resolution-based method to find more efficient solutions for a CIP $\{Xw_1, \ldots, Xw_n, \Gamma \to \Delta,\ \Gamma \to \Delta, X\alpha\}$, starting from a canonical solution G in conjunctive normal form: First, apply Proposition 8 to remove unnecessary clauses from G to obtain G'. Then, compute $\mathcal{R}(G')$. Since G' yields a solution, we have $\Gamma \to \Delta, G'(\alpha)$ and hence it suffices to check for

$F \in \mathcal{R}(G')$ whether $F(w_1), \ldots, F(w_n), \Gamma \to \Delta$ is valid to determine whether F yields a solution. If it is valid, we iterate the procedure on F. If it is not valid, then we know that no iteration of $\mathcal{R}$ on F will yield a solution, so we can abort the search on this branch of the search tree. Since on each branch of the search tree, the size of solutions decreases, the search terminates.

Example 6. Let $\mathcal{S}$ be the CIP of the running example for $n = 2$, which has the characteristic formula, written in conjunctive normal form,

$$G(\alpha)\colon\ Pa \wedge (\neg P\alpha \vee Pf\alpha) \wedge (\neg Pf\alpha \vee Pf^2\alpha) \wedge \neg Pf^4a.$$

Application of Proposition 8 yields

$$G'(\alpha)\colon\ (\neg P\alpha \vee Pf\alpha) \wedge (\neg Pf\alpha \vee Pf^2\alpha).$$

We have $\mathcal{R}(G') = \{\neg P\alpha \vee Pf^2\alpha\}$. By (2) of Proposition 9, it suffices to check whether

$$Pa, \neg Pa \vee Pf^2a, \neg Pf^2a \vee Pf^4a \to Pf^4a$$

is valid, which is the case. Since $\mathcal{R}(\neg P\alpha \vee Pf^2\alpha) = \emptyset$, search terminates and we have found a smaller solution. In general, the algorithm obtains the solution $\neg P\alpha \vee Pf^n\alpha$ after a linear number of iterations.

7 Conclusion

We have presented a method for cut-introduction which computes a quantified cut-formula from a structural analysis of a cut-free proof. This paper is a first step towards algorithmically feasible proof compression by cut-introduction.

As further work we plan to extend the method: the introduction of an arbitrary number of ∀-cuts can be dealt with based on the results in [5] using a decomposition calculus where lines have a flexible width. The extension from single quantifiers to blocks of quantifiers consists in replacing a single variable by a vector of variables. The treatment of cuts with quantifier alternations first requires a description of the structure of Herbrand-sequents obtained from such proofs (along the lines of Proposition 3) which is an interesting theoretical problem.

In order to study this method in a realistic context we plan to implement it within the existing `gapt`-project[2] and to apply it to the output of automated theorem provers.

References

1. Baaz, M., Zach, R.: Algorithmic Structuring of Cut-free Proofs. In: Martini, S., Börger, E., Kleine Büning, H., Jäger, G., Richter, M.M. (eds.) CSL 1992. LNCS, vol. 702, pp. 29–42. Springer, Heidelberg (1993)

[2] `http://code.google.com/p/gapt/`

2. Finger, M., Gabbay, D.: Equal Rights for the Cut: Computable Non-analytic Cuts in Cut-based Proofs. Logic Journal of the IGPL 15(5–6), 553–575 (2007)
3. Gentzen, G.: Untersuchungen über das logische Schließen. Mathematische Zeitschrift 39, 176–210, 405–431 (1934–1935)
4. Hetzl, S.: Describing proofs by short tautologies. Annals of Pure and Applied Logic 159(1–2), 129–145 (2009)
5. Hetzl, S.: Applying Tree Languages in Proof Theory. In: Dediu, A.-H., Martín-Vide, C. (eds.) LATA 2012. LNCS, vol. 7183, pp. 301–312. Springer, Heidelberg (2012)
6. Hetzl, S., Leitsch, A., Weller, D.: Towards Algorithmic Cut-Introduction. technical report, `http://www.logic.at/people/hetzl/`
7. Hetzl, S., Leitsch, A., Weller, D., Woltzenlogel Paleo, B.: Herbrand Sequent Extraction. In: Autexier, S., Campbell, J., Rubio, J., Sorge, V., Suzuki, M., Wiedijk, F. (eds.) AISC/Calculemus/MKM 2008. LNCS (LNAI), vol. 5144, pp. 462–477. Springer, Heidelberg (2008)
8. Miller, D., Nigam, V.: Incorporating Tables into Proofs. In: Duparc, J., Henzinger, T.A. (eds.) CSL 2007. LNCS, vol. 4646, pp. 466–480. Springer, Heidelberg (2007)
9. Orevkov, V.P.: Lower bounds for increasing complexity of derivations after cut elimination. Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta 88, 137–161 (1979)
10. Pudlák, P.: The Lengths of Proofs. In: Buss, S. (ed.) Handbook of Proof Theory, pp. 547–637. Elsevier (1998)
11. Statman, R.: Lower bounds on Herbrand's theorem. Proceedings of the American Mathematical Society 75, 104–107 (1979)
12. Troelstra, A.S., Schwichtenberg, H.: Basic Proof Theory, 2nd edn. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press (2000)
13. Vyskočil, J., Stanovský, D., Urban, J.: Automated Proof Compression by Invention of New Definitions. In: Clarke, E.M., Voronkov, A. (eds.) LPAR-16 2010. LNCS, vol. 6355, pp. 447–462. Springer, Heidelberg (2010)
14. Woltzenlogel Paleo, B.: Atomic Cut Introduction by Resolution: Proof Structuring and Compression. In: Clarke, E.M., Voronkov, A. (eds.) LPAR-16 2010. LNCS, vol. 6355, pp. 463–480. Springer, Heidelberg (2010)