On the Elimination of Quantifier-free Cuts[1]

Daniel Weller

Institute of Computer Languages (E185),
Vienna University of Technology,
Favoritenstraße 9, 1040 Vienna, Austria

Abstract

When investigating the complexity of cut-elimination in first-order logic, a natural subproblem is the elimination of quantifier-free cuts. So far, the problem has only been considered in the context of general cut-elimination, and the upper bounds that have been obtained are essentially double exponential. In this note, we observe that a method due to Dale Miller can be applied to obtain an exponential upper bound.

1. Introduction

In propositional logic, every valid formula has a cut-free proof which is at most of exponential size. This trivially gives an exponential upper bound on the complexity of cut-elimination in propositional logic: Given a proof π (with cuts) of a formula φ, throw away π and compute a new cut-free proof ψ of φ which is at most of exponential size. When eliminating quantifier-free cuts from proofs in first-order logic, the situation is different: The size of proofs cannot be recursively bounded in the length of the theorems, hence the argument of propositional logic does not go through.

The impact of cut-elimination theorems with a complexity analysis can be regarded from two points of view: First, a constructive proof gives a method to perform cut-elimination and provides a worst case bound on the complexity of this transformation. Second, such a theorem provides a theoretical bound on the speed-up that can be achieved by *cut-introduction*. From the complexity analysis of general cut-elimination, we know that, in principle, non-elementary speed-ups can be achieved by cut-introduction, though to this date, not much is known on how to actually introduce cuts (see [15] for some preliminary results). It is natural to start investigating this problem by introducing cuts of low complexity, say atomic or quantifier-free cuts, hence from this point of view an investigation of the complexity of the elimination of quantifier-free cuts is well-motivated.

The best known bounds on the problem can be derived from [16, 17, 5, 6]: if $h(\pi)$ is the *height* of a proof, and $c(\pi)$ the maximal logical depth of its cut-

[1]supported by the Austrian Science Fund (project no. P22028-N13)

formulas, then a proof π with arbitrary quantifier-free cuts can be transformed into a cut-free one π' such that $h(\pi') \leq 2^{2^{c(\pi)}h(\pi)}$. Note that this bound was derived from work not concerned with quantifier-free cut-elimination *per se*, but rather with the effect of propositional cut-elimination in the context of full first-order cuts.

When considering the problem of quantifier-free cut-elimination in isolation, the question remains whether this essentially double exponential bound is the best we can do. We show that the elimination of quantifier-free cuts is exponential in both the symbol complexity and in the *length* of the proof. The method used to show this result does not rely on *reductive cut-elimination*, as the technique introduced by Gentzen in [4] has been called, but is based on a modern version of Herbrand's theorem due to Dale Miller [10, 11], which provides a strong link between propositional and first-order logic. Roughly, the quantifier-free cuts are eliminated by reproving the propositional part of the proof, which can be done with an exponential blow-up (see for example [3]). The main data structure to achieve this will be *expansion trees*. Another, similar formalism was independently introduced in [1] and further investigated in [14]. Closely related work can also be found in [7, 9, 8]. Different forms of Herbrand's theorem are discussed in [2].

The complexity gap of quantifier-free cut-elimination is now closed: already in propositional logic there exists a sequence of tautologies that exhibits an exponential blow-up in symbol complexity when going from proofs with atomic cuts to cut-free proofs (see Theorem 5.1 in [13]).

2. Preliminaries

For the sake of simplicity, we restrict our attention to first-order formulas over $\vee, \neg, \forall, \bot$, although the method also applies to higher-order logic, and in the presence of other connectives. The set of formulas will be denoted by $\mathcal{F}$. We use a two-sided sequent calculus for classical logic. It is essentially the calculus **G1c** from [12] with cut restricted to quantifier-free formulas.

Definition 1 (Sequent calculus $\mathbf{LK}_{pc}$)**.** If Γ, Δ are multisets of formulas, then $S = \Gamma \vdash \Delta$ is a *sequent*. Sometimes it will be convenient to treat sequents as formulas, for this purpose we associate the formula $\bigvee \neg\Gamma \vee \bigvee \Delta$ with S. When relating sequents with formulas, we implicitly work modulo associativity and commutativity of $\vee$. The sequent calculus $\mathbf{LK}_{pc}$ consists of the following rules:
Propositional rules:

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B} \vee_r \qquad \frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta} \vee_l$$

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta} \neg_l \qquad \frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \neg_r$$

Quantifier rules:

$$\frac{F\{x \leftarrow t\}, \Gamma \vdash \Delta}{(\forall x)F, \Gamma \vdash \Delta} \forall_l \qquad \frac{\Gamma \vdash \Delta, F\{x \leftarrow \alpha\}}{\Gamma \vdash \Delta, (\forall x)F} \forall_r$$

Structural rules:

$$\frac{F, F, \Gamma \vdash \Delta}{F, \Gamma \vdash \Delta}\ \mathrm{c}_l \qquad \frac{\Gamma \vdash \Delta, F, F}{\Gamma \vdash \Delta, F}\ \mathrm{c}_r$$

$$\frac{\Gamma \vdash \Delta}{F, \Gamma \vdash \Delta}\ \mathrm{w}_l \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, F}\ \mathrm{w}_r$$

$$\frac{\Gamma \vdash \Delta, C \quad C, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathit{cut}$$

where C is a quantifier-free formula (which may contain free variables) and α is not free in F, Γ, Δ. An $\mathbf{LK}_{pc}$*-proof* is a tree formed according to the rules above, with axioms of the form $A \vdash A$, where A is an atom, or $\bot \vdash$.

As our sequents are defined as multisets, to be fully precise we have to distinguish the active formulas of the rules to prevent ambiguity. To avoid proliferation of syntax, we supress this notation.

The main aim of this paper is to give upper bounds on the problem of the elimination of quantifier-free cuts. To this end, we define some notions of complexity:

Definition 2 (Sizes)**.** We define the *logical complexity* $|\cdot|$ and the *symbol complexity* $||\cdot||$ of terms, formulas and proofs. Let t be a term, then we define $||t||$ to be the number of symbols in t. Let F be a formula, then we define $|F|$ to be the number of logical connectives in F, and $||F||$ to be the number of (logical and non-logical) symbols in F.

Let π be an $\mathbf{LK}_{pc}$-proof, and let $S_1, \ldots, S_n$ be the sequents in π. Then $||\pi|| = \sum_{1 \leq i \leq n} ||S_i||$ and $|\pi|$ is the number of axioms and propositional, quantifier, w_l and w_r inferences in π.

3. Elimination of quantifier-free cuts

Our approach to eliminating cuts from an $\mathbf{LK}_{pc}$-proof π of S is the following: First, a "propositional tautology" E is extracted from π which is of linear size (Theorem 1). Then, a cut-free proof ψ of E which has exponential size is constructed (Lemma 2), and finally ψ is converted to a cut-free $\mathbf{LK}_{pc}$-proof ψ' of S with polynomial expense (Lemma 3).

We will now introduce a version of the expansion trees of [11]. They are a data structure which allows an elegant proof-theoretic proof of (a version of) Herbrand's theorem. Their essential task is to keep track of quantifier instantiations and variable dependencies. For $F, G \in \mathcal{F}$, we write $F \approx G$ for "F is G with some positive subformulas replaced by $\bot$" (a subformula is positive if it is dominated by an even number of $\neg$).

Definition 3 (Expansion trees)**.** We define *expansion trees* $\mathcal{E}$, *dual expansion trees* $\mathcal{E}_d$, *selected variables*, *expansion terms*, two functions Sh and Dp from $\mathcal{E} \cup \mathcal{E}_d$ to $\mathcal{F}$, and size functions $|\cdot|$ and $||\cdot||$:

1. If A is an atom or $\bot$, then $A \in \mathcal{E} \cap \mathcal{E}_d$ and $\mathrm{Sh}(A) = \mathrm{Dp}(A) = A$.
2. If $E \in \mathcal{E}$ then $\neg E \in \mathcal{E}_d$, if $E \in \mathcal{E}_d$ then $\neg E \in \mathcal{E}$. In either case,

$$\begin{array}{ll} \mathrm{Sh}(\neg E) = \neg \mathrm{Sh}(E), & \mathrm{Dp}(\neg E) = \neg \mathrm{Dp}(E), \\ |\neg E| = |E| + 1, & ||E|| = ||E|| + 1. \end{array}$$

3. Assume that E_1 and E_2 do not share selected variables. If $E_1, E_2 \in \mathcal{E}$ then $E_1 \vee E_2 \in \mathcal{E}$, if $E_1, E_2 \in \mathcal{E}_d$ then $E_1 \vee E_2 \in \mathcal{E}_d$. In either case,

$$\begin{array}{ll} \mathrm{Sh}(E_1 \vee E_2) = \mathrm{Sh}(E_1) \vee \mathrm{Sh}(E_2), & \mathrm{Dp}(E_1 \vee E_2) = \mathrm{Dp}(E_1) \vee \mathrm{Dp}(E_2), \\ |E_1 \vee E_2| = |E_1| + |E_2| + 1, & ||E_1 \vee E_2|| = ||E_1|| + ||E_2|| + 1. \end{array}$$

4. Assume $E \in \mathcal{E}$, $F \in \mathcal{F}$, and $\mathrm{Sh}(E) \approx F\{x \leftarrow \alpha\}$ for some variable α not selected in E. Let $E' = (\forall x)F +^{\alpha} E$. Then $E' \in \mathcal{E}$, α is a *selected variable of* E' and

$$\begin{array}{ll} \mathrm{Sh}(E') = (\forall x)F, & \mathrm{Dp}(E') = \mathrm{Dp}(E), \\ |E'| = |E| + 1, & ||E'|| = ||E|| + 1. \end{array}$$

5. Let $F \in \mathcal{F}$, $t_1, \ldots, t_n$ be terms, $E_1, \ldots, E_n \in \mathcal{E}_d$ such that the E_i do not share selected variables, and $\mathrm{Sh}(E_i) \approx F\{x \leftarrow t_i\}$. Let $E' = (\forall x)F +^{t_1} E_1 + \ldots +^{t_n} E_n$. Then $E' \in \mathcal{E}_d$, $t_1, \ldots, t_n$ are *expansion terms* of E', and

$$\begin{array}{ll} \mathrm{Sh}(E') = (\forall x)F, & \mathrm{Dp}(E') = \bigwedge_{1 \leq i \leq n} \mathrm{Dp}(E_i), \\ |E'| = \sum_{1 \leq i \leq n} (|E_i| + 1), & ||E'|| = \sum_{1 \leq i \leq n} (||E_i|| + 1). \end{array}$$

We remark that, somewhat unintuitively, $||E||$ ignores the sizes of the expansion terms t_i. There are two reasons for this: first, this definition suffices for the bounds on cut-elimination we want to obtain. Second, t_i will usually occur in E_i (otherwise the quantifier is "vacuous") and hence it would suffice to store a constant-size pointer to t_i.

Now let $E \in \mathcal{E} \cup \mathcal{E}_d$. Observe that if E is a quantifier-free formula, then $|E|$ and $||E||$ are consistent with Definition 2. Note that $\mathrm{Dp}(E)$ is a propositional formula. In the tree representation of E, a quantifier node Q_1 *dominates* another quantifier node Q_2 if both are on a common branch and Q_1 is closer to the root than Q_2.

Let Θ_E be the set of occurrences of expansion terms of E. Define the binary relation $<_E^0$ on Θ_E: $t <_E^0 s$ if there exists a variable α which is selected for a quantifier node dominated by the quantifier node of t such that α is free in s. We write $<_E$ for the transitive closure of $<_E^0$.

Definition 4 (Expansion tree proofs)**.** We say that E is *tautologous* if $\mathrm{Dp}(E)$ is a tautology. E is an *expansion tree for* a formula F, written $E \succ F$, if

1. $\mathrm{Sh}(E) \approx F$, and
2. the free variables of F are not selected in E, and
3. $<_E$ is acyclic.

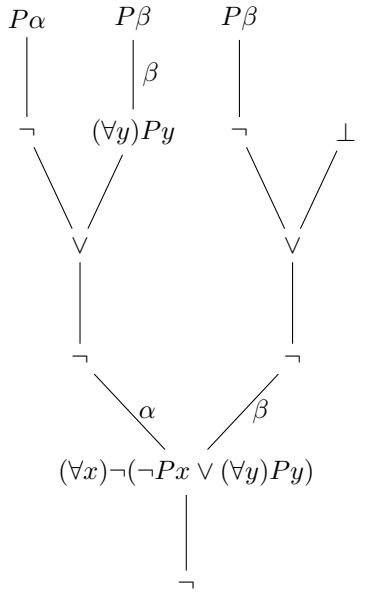
E is an *ET-proof* of a formula F, in symbols $\vdash_E F$, if $E \succ F$ and E is tautologous.

Note that in particular, $\bot \succ F$ for all F.

Example 1. Consider the expansion tree

$$E = \neg[(\forall x)\neg(\neg Px \vee (\forall y)Py) \quad +^{\alpha}\neg(\neg P\alpha \vee [(\forall y)Py +^{\beta} P\beta]) \\ +^{\beta}\neg(\neg P\beta \vee \bot)]$$

More suggestively, E can be drawn as a tree:



Then α, β are expansion terms in E, β is selected, $\alpha <_E \beta$, and

$$\begin{array}{ll} \mathrm{Sh}(E) = \neg((\forall x)\neg(\neg Px \vee (\forall y)Py)), & |E| = 10, \\ \mathrm{Dp}(E) = \neg(\neg(\neg P\alpha \vee P\beta) \wedge \neg(\neg P\beta \vee \bot)), & ||E|| = 16. \end{array}$$

It is easy to verify that $\vdash_E \mathrm{Sh}(E)$.

In order to extract expansion tree proofs from $\mathbf{LK}_{pc}$-proofs, we will need to merge expansion trees:

Lemma 1. *Let $E_1, E_2 \in \mathcal{E}$ (or $E_1, E_2 \in \mathcal{E}_d$). If $E_1 \succ F$ and $E_2 \succ F$ then there exists $E_1 \cup E_2 \in \mathcal{E}$ (or $\in \mathcal{E}_d$) such that $E_1 \cup E_2 \succ F$ and $||E_1 \cup E_2|| \leq ||E_1|| + ||E_2||$ and $|E_1 \cup E_2| \leq |E_1| + |E_2|$ and*

1. *if $E_1, E_2 \in \mathcal{E}$ then $(\mathrm{Dp}(E_1) \vee \mathrm{Dp}(E_2)) \to \mathrm{Dp}(E_1 \cup E_2)$ is a tautology, and*
2. *if $E_1, E_2 \in \mathcal{E}_d$ then $\mathrm{Dp}(E_1 \cup E_2) \to (\mathrm{Dp}(E_1) \wedge \mathrm{Dp}(E_2))$ is a tautology.*

Proof. We only treat the interesting cases. If $E_1 = \bot$ then we take $E_1 \cup E_2 = E_2$ (similarily if $E_2 = \bot$). If $E_1 = (\forall x)F +^{t_1} E_1 + \ldots +^{t_n} E_n$ then $E_2 = (\forall x)F +^{s_1} E'_1 + \ldots +^{s_m} E'_m$ and we take $E_1 \cup E_2 = (\forall x)F +^{t_1} E_1 + \ldots +^{t_n} E_n +^{s_1} E'_1 + \ldots +^{s_m} E'_m$. If $E_1 = (\forall x)F +^{\alpha} E$ then $E_2 = (\forall x)F +^{\alpha} E'$ and we take $E_1 \cup E_2 = (\forall x)F +^{\alpha} (E \cup E')$. □

Even in the presence of quantifier-free cuts, we can extract small expansion tree proofs from sequent calculus proofs:

Theorem 1. *Let π be an $\mathbf{LK}_{pc}$-proof of a sequent S. There exists an expansion tree E such that $\vdash_E S$, $||E|| \leq c||\pi||$, and $|E| \leq d|\pi|$, where c, d are constants.*

Proof. Let ρ be an inference in π with conclusion $\Gamma_S, \Gamma_C \vdash \Delta_S, \Delta_C$, where Γ_S, Δ_S are the end-sequent ancestors and Γ_C, Δ_C are the cut-ancestors. Let $h(\rho)$ be the maximal number of sequents between ρ and an axiom of π. We construct by induction on $h(\rho)$ an expansion tree E such that the expansion tree $E \vee (\Gamma_C \vdash \Delta_C)$ is tautologous and $E \succ (\Gamma_S \vdash \Delta_S)$ and $||E|| \leq c||\pi_\rho||$ and $|E| \leq d|\pi_\rho|$, where π_ρ is the subproof of π ending in ρ. Furthermore, no variable free in the conclusion of ρ is selected in E. Then, by taking ρ as the last rule of π, the desired result follows.

1. ρ is an axiom $A \vdash A$ (the case of $\bot \vdash$ is analogous). We assume that the left occurrence is an end-sequent ancestor and the right occurrence is a cut-ancestor (the other cases are similar; in case all occurrences are cut-ancestors, we take $E = \bot$). We take $E = \neg A$. Hence $E \vee (\Gamma_C \vdash \Delta_C) = \neg A \vee A$ is tautologous, $E \succ \neg A$ and $||E|| \leq ||\pi_\rho||$ and $|E| \leq |\pi_\rho|$.
2. ρ is a $\forall_l$ inference

$$\dfrac{\begin{matrix}(\lambda)\\ G\{x \leftarrow t\}, \Gamma_S, \Gamma_C \vdash \Delta_S, \Delta_C\end{matrix}}{(\forall x)G, \Gamma_S, \Gamma_C \vdash \Delta_S, \Delta_C}\ \forall_l$$

   As all cuts in π are quantifier-free, $(\forall x)G$ and $G\{x \leftarrow t\}$ are end-sequent ancestors. By (IH) there exists E such that $E \succ \neg G\{x \leftarrow t\} \vee (\Gamma_S \vdash \Delta_S)$, $E \vee (\Gamma_C \vdash \Delta_C)$ is tautologous and $||E|| \leq c||\lambda||$ and $|E| \leq d|\lambda|$. Hence $E = \neg E' \vee E''$ such that $\mathrm{Sh}(E') = G\{x \leftarrow t\}$. Let $E^* = (\forall x)G +^t E'$, then $E^+ = \neg E^* \vee E''$ is the desired expansion tree. $<_{E^+}$ remains acyclic since by our inductive assumption, no variable free in t is selected in E. Note that $||E^+|| = ||E|| + 1 \leq c||\pi_\rho||$ and $|E^+| = |E| + 1 \leq d|\pi_\rho|$.
3. ρ is a $\forall_r$ inference. We proceed analogously to $\forall_l$, renaming selected variables if necessary.
4. ρ is a cut

$$\dfrac{\begin{matrix}(\pi_1)\\ \Gamma_{S,1}, \Gamma_{C,1}, \vdash \Delta_{S,1}, \Delta_{C,1}, F\end{matrix} \quad \begin{matrix}(\pi_2)\\ F, \Gamma_{S,2}, \Gamma_{C,2}, \vdash \Delta_{S,2}, \Delta_{C,2}\end{matrix}}{\Gamma_{S,1}, \Gamma_{C,1}, \Gamma_{S,2}, \Gamma_{C,2} \vdash \Delta_{S,1}, \Delta_{C,1}, \Delta_{S,2}, \Delta_{C,2}}\ cut$$

   By (IH) there exist expansion trees E_1, E_2 such that $E_i \succ (\Gamma_{S,i} \vdash \Delta_{S,i})$, and $E_1 \vee (\Gamma_{C,1} \vdash \Delta_{C,2}, F)$ and $(F, \Gamma_{C_2} \vdash \Delta_{C,2}) \vee E_2$ are both tautologous, and such that $|E_i| \leq d|\pi_i|$. We take $E = E_1 \vee E_2$, renaming selected variables if necessary. Note that $||E|| = ||E_1|| + ||E_2|| + 1 \leq c||\pi_\rho||$ and $|E| = |E_1| + |E_2| + 1 \leq d|\pi_\rho|$.

5. ρ is w_r (the case of w_l is analogous). In case an end-sequent ancestor is introduced, $E = E' \vee \bot$, where E' the expansion tree obtained by (IH). In this case, $||E|| = ||E'|| + 2 \leq c||\pi_\rho||$ and $|E| = |E'| + 2 \leq d|\pi_\rho|$. Otherwise we conclude by (IH).
6. ρ is a c_l or c_r inference. If the main formulas are end-sequent ancestors, E is obtained from the expansion tree obtained by (IH) by applying Lemma 1. Otherwise we conclude by (IH).
7. ρ is a propositional inference. If the main formulas are end-sequent ancestors, E is obtained by introducing the appropriate connective. In the case of a binary inference, Lemma 1 is used for the context formulas.

□

The next definition introduces a sequent calculus for expansion trees. It is invertible in the sense that if S is derived from S', then if S is tautologous so is S'.

Definition 5 (Sequent calculus $\mathbf{LK}_E$)**.** We say that a term t is admissible in an expansion tree E if no variable free in t is selected in E. We now consider *expansion sequents* $\Gamma \vdash \Delta$ where Δ (Γ) is multiset of (dual) expansion trees. As with sequents, we will treat expansion sequents as expansion trees when it is convenient. The sequent calculus $\mathbf{LK}_E$ consists of the rules $\vee_l, \vee_r, \neg_l, \neg_r, w_l, w_r$ of $\mathbf{LK}_{pc}$, defined for expansion sequents, and the following expansion rules:

$$\frac{\Gamma \vdash \Delta, E}{\Gamma \vdash \Delta, (\forall x)F +^{\alpha} E}\ \forall_r \qquad \frac{E_1, \Gamma \vdash \Delta}{(\forall x)F +^{t_1} E_1, \Gamma \vdash \Delta}\ \forall_l^1$$

$$\frac{(\forall x)F +^{t_1} E_1 + \ldots +^{t_{i-1}} E_{i-1} +^{t_{i+1}} E_{i+1} + \ldots +^{t_n} E_n, E_i, \Gamma \vdash \Delta}{(\forall x)F +^{t_1} E_1 + \ldots +^{t_n} E_n, \Gamma \vdash \Delta}\ \forall_l$$

In $\forall_l$, t_i must be admissible in $\Gamma \vdash \Delta, (\forall x)F +^{t_1} E_1 + \ldots +^{t_n} E_n$. Similarily in $\forall_l^1$. An $\mathbf{LK}_E$*-proof* is a tree formed according to the rules of $\mathbf{LK}_E$, with axioms of the form $\bot \vdash$ and $A \vdash A$ where A is an atom. For $\mathbf{LK}_E$-proofs π, the logical and symbol complexity measures $|\pi|$ and $||\pi||$ are defined analogously as for $\mathbf{LK}_{pc}$-proofs.

Since the rules of $\mathbf{LK}_E$ except w_l and w_r are invertible, the usual semantic cut-free completeness proof for the sequent calculus for propositional logic as in e.g. [3] can be applied with a slight modification to obtain

Lemma 2. *Let E be a tautologous expansion sequent such that $<_E$ is acyclic. Then there exists an $\mathbf{LK}_E$-proof π of E such that $||\pi|| \leq 2^{||A||}$ and $|\pi| \leq 2^{|A|}$.*

Proof. By induction on E. The difference to the argument for propositional logic is that we have to show that, if all members of E are dual expansion trees of the form $(\forall x)F +^{t_{i,1}} E_1 + \ldots +^{t_{i,n_i}} E_n \in \mathcal{E}_d$, then some $t_{i,j}$ is admissible. This follows straightforwardly from the acyclicity of $<_E$. □

Finally, we convert cut-free proofs of expansion sequents to cut-free proofs in first-order logic.

Lemma 3. *Let π be an $\mathbf{LK}_E$-proof of an expansion sequent S_E such that $S_E \succ S$. Then there exists a cut-free $\mathbf{LK}_{pc}$-proof φ of S such that $||\varphi|| \leq ||\pi||^2$ and $|\varphi| \leq |\pi|$.*

Proof. We first construct a proof ψ of $\mathrm{Sh}(S_E)$ by replacing sequents $\Gamma \vdash \Delta$ in π by $\mathrm{Sh}(\Gamma) \vdash \mathrm{Sh}(\Delta)$, and inferences by their respective $\mathbf{LK}_{pc}$ counterparts. In particular, $\forall_l$ in π is replaced by c_l and $\forall_l$. The eigenvariable condition holds because the terms used in the $\forall_l$ inferences are admissible. Clearly $|\psi| \leq |\pi|$ and $||\psi|| \leq ||\pi||$.

Since $\mathrm{Sh}(S_E) \approx S$, to obtain φ from ψ we may have to replace some positive occurrences of $\bot$ by the correct subformulas of S. This can be done since the axiom $\bot \vdash$ only applies to negative occurrences of $\bot$. We have $|\varphi| \leq |\psi|$ and $||\varphi|| \leq ||\psi||^2$. □

Finally, we can state the main result on the complexity of the elimination of quantifier-free cuts from proofs in first-order logic:

Theorem 2. *Let π be an $\mathbf{LK}_{pc}$-proof of a sequent S. Then there exists a cut-free $\mathbf{LK}_{pc}$-proof ψ of S such that $||\psi|| < 2^{c||\pi||}$ and $|\psi| < 2^{d|\pi|}$, where c, d are constants.*

Proof. By Theorem 1 there exists an expansion tree E such that $\vdash_E S$, $||E|| \leq c_1||\pi||$, and $|E| \leq d_1|\pi|$. By Lemma 2, there exists an $\mathbf{LK}_E$-proof φ of E such that $||\varphi|| \leq 2^{c_1||\pi||}$ and $|\varphi| \leq 2^{d_1|\pi|}$. By Lemma 3, we obtain a cut-free $\mathbf{LK}_{pc}$-proof ψ of S such that $||\psi|| \leq 2^{2c_1||\pi||}$ and $|\psi| \leq 2^{d_1|\pi|}$. □

4. Acknowledgments

The author would like to thank Matthias Baaz for pointing out that the problem addressed in this work was open, and to Matthias Baaz, Stefan Hetzl, and Alexander Leitsch for fruitful discussions and insightful comments on the subject. In particular, the idea to use $\bot$ to handle the weak formulas is due to Stefan Hetzl.

[1] Matthias Baaz and Alexander Leitsch. Skolemization and proof complexity. *Fundamenta Informaticae*, 20(4):353–379, 1994.

[2] Samuel R. Buss. On Herbrand's theorem. In *Logic and Computational Complexity*, volume 960 of *Lecture Notes in Computer Science*, pages 195–209. Springer Berlin, 1995.

[3] Samuel R. Buss. An introduction to proof theory. In *Handbook of Proof Theory*, pages 1–78, 1998.

[4] Gerhard Gentzen. Untersuchungen über das logische Schließen I. *Mathematische Zeitschrift*, 39(1):176–210, dec 1935.

[5] Philipp Gerhardy. Refined complexity analysis of cut elimination. In *Computer Science Logic*, volume 2803 of *Lecture Notes in Computer Science*, pages 212–225. Springer Berlin, 2003.

[6] Philipp Gerhardy. The role of quantifier alternations in cut elimination. *Notre Dame Journal of Formal Logic*, 46(2):165–171, 2005.

[7] Willem Heijltjes. Proof forests with cut-elimination based on Herbrand's theorem. In *Second International Workshop on Classical Logic and Computation*, July 2008.

[8] Stefan Hetzl. Describing proofs by short tautologies. *Annals of Pure and Applied Logic*, 159(1–2):129–145, 2009.

[9] Richard McKinley. Herbrand expansion proofs and proof identity. In *Second International Workshop on Classical Logic and Computation*, July 2008.

[10] Dale Miller. *Proofs In Higher-Order Logic*. PhD thesis, Carnegie Mellon University, Department of Mathematics, 1983.

[11] Dale Miller. A compact representation of proofs. *Studia Logica*, 46(4):347–370, 1987.

[12] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, second edition, 2000.

[13] Alasdair Urquhart. The complexity of propositional proofs. *The Bulletin of Symbolic Logic*, 1(4):425–467, dec 1995.

[14] Bruno Woltzenlogel Paleo. *Herbrand Sequent Extraction*. VDM-Verlag, Saarbruecken, Germany, 2008.

[15] Bruno Woltzenlogel Paleo. *A General Analysis of Cut-Elimination by CERes*. PhD thesis, Vienna University of Technology, 2009.

[16] Wenhui Zhang. Cut elimination and automatic proof procedures. *Theoretical Computer Science*, 91(2):265–284, 1991.

[17] Wenhui Zhang. Depth of proofs, depth of cut-formulas and complexity of cut-formulas. *Theoretical Computer Science*, 129(1):193–206, 1994.