The Journal of Symbolic Logic
Volume 00, Number 0, XXX 0000

ON THE COMPLEXITY OF PROOF DESKOLEMIZATION

MATTHIAS BAAZ, STEFAN HETZL, AND DANIEL WELLER

Abstract. We consider the following problem: Given a proof of the Skolemization of a formula F, what is the length of the shortest proof of F? For the restriction of this question to cut-free proofs we prove corresponding exponential upper and lower bounds.

§1. Introduction.

The Skolemization of formulas is a standard technique in logic. It consists of replacing existential quantifiers by new function symbols whose arguments reflect the dependencies of the quantifier. The Skolemization of a formula is satisfiability-equivalent to the original formula. This transformation has a number of applications, it is for example crucial for automated theorem proving as the resolution calculus is a quantifier-free formalism.

While Skolemization in a model-theoretic context is viewed as transformation of the axioms of a theory, in a proof-theoretic context it is used for transforming a formula that shall be proved. Hence in the context of proof theory, which is the background of this paper, we remove universal quantifiers in favour of new function symbols. Thereby a validity-equivalent formula is obtained (which is sometimes also called the Herbrandization of the original formula).

This transformation of formulas naturally induces a transformation of proofs: if we are given a proof π of some formula F one can obtain a proof π' of the Skolemization of F by simple instantiation of free variables. In fact, the Skolemization of a proof has the effect of decreasing the number of inferences (as some quantifier inferences can be dropped). Now the following question naturally arises: If we are given a proof of the Skolemization of F what is the length of the shortest proof of F? Or in other words: What is the complexity of deskolemization?

This question is of practical interest as resolution-based automated theorem provers output essentially cut-free proofs of skolemized formulas and presenting a proof of the original input formula to a user must therefore involve an algorithm for deskolemization. The historically first deskolemization algorithm for prenex formulas in the cut-free case (via Herbrand-disjunctions) can be found in the proof of the 2nd ε-theorem [8].

The complexity of deskolemization is also of considerable theoretical interest as it concerns the impact on proof length of the addition of new function symbols to

Received by the editors December 27, 2010.

the language. The question of the degree of this impact has been formulated by P. Pudlák (in a slightly different form) as problem 22 in [5]. A partial solution has been given by J. Avigad in [1]: theories that allow the encoding of finite functions have polynomial deskolemization. In this paper we consider a different type of restriction: instead of restricting the theories we restrict the proofs and consider the question of the complexity of deskolemization for *cut-free* proofs. We prove both an exponential upper and a corresponding exponential lower bound. Finally we consider an optimized version of Skolemization that even in the cut-free case has only non-elementary deskolemization.

§2. Preliminaries.

We consider first-order formulas over the logical constants $\neg, \vee, \wedge, \rightarrow, \forall, \exists, \top, \bot$. An occurrence of $\forall$ in a formula F is called *strong* if it occurs in a positive context (i.e. dominated by an even number of negations and left-hand sides of implications), and weak otherwise. An analogous definition is made for $\exists$. The number of strong quantifiers in a formula F is denoted by $\mathrm{qocc}(F)$.

We use a variant of the sequent calculus **G3c** from [11], with the difference that we add the appropriate axiom for $\top$ and that we work in a purely cut-free setting.

Definition 1 (Sequent calculus). *Sequents* are pairs of multisets of formulas, written $\Gamma \vdash \Delta$. An **LK**-proof is a tree built up from the following axioms and rules: axioms are of the form

$$\frac{}{A, \Gamma \vdash \Delta, A}\ \mathrm{ax} \qquad \frac{}{\bot, \Gamma \vdash \Delta}\ \mathrm{ax}\bot \qquad \frac{}{\Gamma \vdash \Delta, \top}\ \mathrm{ax}\top$$

for an atom A. The rules are

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

and analogously for $\wedge$ and $\rightarrow$. Furthermore

$$\frac{\Gamma \vdash \Delta, (\exists x)F, F\{x \leftarrow t\}}{\Gamma \vdash \Delta, (\exists x)F}\ \exists_r \qquad \frac{F\{x \leftarrow \alpha\}, \Gamma \vdash \Delta}{(\exists x)F, \Gamma \vdash \Delta}\ \exists_l$$

where α is a variable which does not occur in F, Γ, Δ, the *eigenvariable* of this rule. The rules for $\forall$ are defined analogously. The notions of *active*, *auxiliary*, and *main formulas*, and the *ancestor relation* are defined as usual. The quantifier rules with eigenvariable conditions are called *strong* quantifier rules, the other quantifier rules are called *weak*.

We will use the standard assumption that our **LK**-proofs are *regular*, that is: for every two distinct $\exists_l$ inferences ρ, σ in an **LK**-proof π, the eigenvariables of ρ and σ are different.

Definition 2 (Proof length). Let π be an **LK**-proof. Then the *length of* π, denoted by $|\pi|$, is the number of sequents in π.

Having set up our calculus, we will now introduce Skolemization (for Skolemization in the context of proofs, see also [2, 3]). We postulate a countably infinite set of *Skolem symbols* $\mathcal{SK} = \{f_n \mid n \in \mathbb{N}\}$ and define an operator for *structural Skolemization* as follows.

Definition 3 (Skolemization operators). Let F be a formula and $n \in \mathbb{N}$. If F does not contain strong quantifiers then $\mathrm{sk}_n(F) = F$. If F does contain strong quantifiers, then

$$\mathrm{sk}_n(F) = \quad \mathrm{sk}_{n+1}(F_{Qy}\{y \leftarrow f_n(x_1, \dots , x_k)\})$$

where F_{Qy} is F after omission of the leftmost strong quantifier occurrence μ of Qy, and $Q_1x_1, \dots Q_kx_k$ are the weak quantifiers appearing in this order in F such that μ is in their scope. We call $t = f_n(x_1, \dots , x_k)$ *Skolem terms* of F, and we say that t *corresponds to* μ and vice-versa.

Finally, we define $\mathrm{sk}(F) = \mathrm{sk}_0(F)$. If $F = \bigwedge \Gamma \to \bigvee \Delta$ and $\mathrm{sk}(F) = \bigwedge \Pi \to \bigvee \Lambda$ we define $\mathrm{sk}(\Gamma \vdash \Delta) = \Pi \vdash \Lambda$.

The following theorem on proof Skolemization is well-known:

Theorem 1. *Let π be an* **LK**-*proof of S, then there exists an* **LK**-*proof π' of* $\mathrm{sk}(S)$ *such that* $|\pi'| \leq |\pi|$.

Proof. The proof from [3] readily adapts to our version of **LK**: eigenvariables are replaced by Skolem terms. ⊣

It is also well-known that in the case of F being a prenex formula, from an **LK**-proof of $\mathrm{sk}(F)$ we can easily construct an **LK**-proof of F:

Proposition 1. *Let F be a prenex formula and π an* **LK**-*proof of* $\vdash \mathrm{sk}(F)$. *Then there exists an* **LK**-*proof ψ of* $\vdash F$ *such that* $|\psi| \leq |\pi| * (\mathrm{qocc}(F) + 1)$.

Proof. First, we apply Gentzen's midsequent theorem [6] to π to obtain an **LK**-proof φ of $\vdash \mathrm{sk}(F)$ such that φ contains a sequent S such that above S, only propositional inferences are applied and below S, only weak quantifier inferences are applied. Further, $|\varphi| \leq |\pi|$. The quantifier inferences can then be reordered such that the strong quantifier inferences (corresponding to the quantifiers that were removed by Skolemization) can be introduced without violating any eigenvariable conditions. The reordering does not increase proof size since all quantifier inferences are unary, and at most $\mathrm{qocc}(F) * |\pi|$ strong quantifier inferences have to be introduced. This yields the desired **LK**-proof ψ of $\vdash F$. ⊣

Note that this proof, going back to the 2nd ε-theorem [8], does not work in the more general setting where the quantifiers in F may appear at arbitrary positions: the mid-sequent theorem does not apply anymore, and the reordering of quantifier inferences may be more expensive since binary inferences are involved. It is this problem that we will consider in the next two sections.

§3. The upper bound.

A central technique for the upper bound will be to collect instances of a formula that appear in a proof. To that aim we will use a variant of expansion trees, introduced by D. Miller in [9] in the setting of higher-order logic. In fact, what we are going to define as expansion below corresponds most closely to the Skolem expansion trees of [9]. In order to simplify the notation we do not use the connective $\wedge$ and $\to$ explicitely in this section, their treatment being analogous to that of $\vee$ and $\neg$.

Definition 4. 1. An atom A is an expansion of itself.

2. If E_1 is an expansion of A_1 and E_2 is an expansion of A_2, then $E_1 \vee E_2$ is an expansion of $A_1 \vee A_2$.
3. If E is an expansion of A, then $\neg E$ is a dual expansion of $\neg A$.
4. If $\{t_1, \ldots, t_n\}$ is a set of terms and $E_1, \ldots, E_n$ are expansions of $A\{x \leftarrow t_1\}, \ldots, A\{x \leftarrow t_n\}$, then $\exists x\, A +^{t_1} E_1 + \ldots +^{t_n} E_n$ is an expansion of $\exists x\, A$.
5. If f is a Skolem symbol and E is an expansion of $A\{x \leftarrow f(t_1, \ldots, t_n)\}$, then $\forall x\, A +^{f(t_1,\ldots,t_n)} E$ is an expansion of $\forall x\, A$.
6. $\bot$ is an expansion of every formula.

Dual expansions are defined as above switching *expansion* and *dual expansion*, $\bot$ and $\top$ as well as $\forall$ and $\exists$. In addition, an expansion or dual expansion E must satisfy the following two global conditions:

A. Each strong quantifier in A induces an equivalence class of sub-expansions of E of the form of 5 by considering E_1 and E_2 as equivalent if they correspond to the same strong quantifier in A. All elements in an equivalence class use the same function symbol f which must not appear in A and must be different from the function symbol of any other equivalence class.

B. Every strong quantifier node in E has the form $E_0 = Qx\, A' +^{f(\bar{s},t_1,\ldots,t_n)} E_1$, for some Skolem symbol f, where the terms $t_1, \ldots, t_n$ are exactly those introduced for weak quantifiers on the path from the root of E to E_0 in this order and $\bar{s} = s_1, \ldots, s_m$ is a fixed list of variable-free terms, called the *parameters* of E.

Often the parameters will be irrelevant, if they are not we will mention them explicitely. For an expansion or dual expansion E, the set of Skolem terms $\mathrm{SkTerms}(E)$ is the set of terms $f(t_1, \ldots, t_n)$ that are contained in E at nodes of the form $Qx\, A' +^{f(t_1,\ldots,t_n)} E'$ pertaining to strong quantifiers. If E is an expansion or dual expansion of a formula A with parameters $\bar{s}$ and $f(\bar{s}, t_1, \ldots, t_n) \in \mathrm{SkTerms}(E)$, then there is a unique strong quantifier node in E with $f(\bar{s}, t_1, \ldots, t_n)$ as Skolem term. For suppose there would be two such quantifier nodes, then the paths from the root of E to these two nodes would split on either a $\vee$- or an $\exists$-node. The former is impossible because, by condition A, the Skolem symbol f designates a unique strong quantifier in A and the latter is impossible because, by condition B, the terms $t_1, \ldots, t_n$ designate a unique subexpansion of their respective weak quantifier nodes.

Remark 1. Our expansions differ from Miller's Skolem expansion trees at several points: our convention on naming Skolem symbols corresponds directly to Skolemization of formulas, we allow $\bot$ and $\top$ to accomodate weakening conveniently, at weak quantifiers we consider a set of terms and we work in the setting of first-order logic.

In addition to considering expansions of formulas we will also consider expansions of sequents. If $S = A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ is a sequent, $E_1, \ldots, E_n$ are dual expansions of $A_1, \ldots, A_n$ and $F_1, \ldots, F_m$ are expansions of $B_1, \ldots, B_m$, then $E_1, \ldots, E_n \vdash F_1, \ldots, F_m$ is called expansion of S if every $t \in \mathrm{SkTerms}(E_1, \ldots, E_n \vdash F_1, \ldots, F_m)$ corresponds to exactly one strong quantifier node in $E_1, \ldots, E_n \vdash F_1, \ldots, F_m$.

Definition 5. If E is an expansion or dual expansion, then the formula $\mathrm{Sh}(E)$ and the quantifier-free formula $\mathrm{Dp}(E)$ are defined as follows:

$$\begin{aligned}\mathrm{Sh}(E) &= E \text{ for an atom } E\\ \mathrm{Sh}(\neg E) &= \neg\mathrm{Sh}(E)\\ \mathrm{Sh}(E_1 \vee E_2) &= \mathrm{Sh}(E_1) \vee \mathrm{Sh}(E_2)\\ \mathrm{Sh}(Qx\, A +^{t_1} E_1 + \ldots +^{t_n} E_n) &= Qx\, A.\end{aligned}$$

$$\begin{aligned}\mathrm{Dp}(E) &= E \text{ for an atom } E\\ \mathrm{Dp}(\neg E) &= \neg\mathrm{Dp}(E)\\ \mathrm{Dp}(E_1 \vee E_2) &= \mathrm{Dp}(E_1) \vee \mathrm{Dp}(E_2)\\ \mathrm{Dp}(\exists x\, A +^{t_1} E_1 + \ldots +^{t_n} E_n) &= \bigvee_{i=1}^{n} \mathrm{Dp}(E_i), \text{ and}\\ \mathrm{Dp}(\forall x\, A +^{t_1} E_1 + \ldots +^{t_n} E_n) &= \bigwedge_{i=1}^{n} \mathrm{Dp}(E_i).\end{aligned}$$

If $S = E_1, \ldots, E_n \vdash F_1, \ldots, F_m$ is the expansion of a sequent, then $\mathrm{Dp}(S) = \neg\mathrm{Dp}(E_1) \vee \ldots \vee \neg\mathrm{Dp}(E_n) \vee \mathrm{Dp}(F_1) \vee \ldots \vee \mathrm{Dp}(F_m)$.

Note that, if E is an expansion of A, then in general $\mathrm{Sh}(E) \neq A$ but by replacing positive occurrence of $\bot$ and negative occurrences of $\top$ in $\mathrm{Sh}(E)$ by subformulas of A, the formula A can be recovered. An expansion E is called tautological if $\mathrm{Dp}(E)$ is a tautology.

Example 1. $E_0 = \forall y\,(P(c) \to P(y)) +^{f(c)} P(c) \to P(f(c))$ is an expansion of $\forall y\,(P(c) \to P(y))$ with parameter c and Skolem symbol f.
$E_1 = \exists x \forall y\,(P(x) \to P(y)) +^{c} E_0$ as well as $E_2 =$

$$\exists x\forall y(P(x) \to P(y)) +^{c} E_0$$
$$+^{f(c)} (\forall y(P(f(c)) \to P(y)) +^{f(f(c))} P(f(c)) \to P(f(f(c))))$$

are expansions of $\exists x\forall y\,(P(x) \to P(y))$ but only E_2 is tautological.

Definition 6. For an expansion or dual expansion E its logical complexity $|E|$ is defined as

$$\begin{aligned}|E| &= 0 \text{ for an atom } E\\ |\neg E| &= |E| + 1\\ |E_1 \vee E_2| &= |E_1| + |E_2| + 1\\ |Qx\, A +^{t_1} E_1 \ldots +^{t_n} E_n| &= \sum_{i=1}^{n}(|E_i| + 1) \text{ for a quantifier } Qx\end{aligned}$$

If $\Pi \vdash \Lambda$ is the expansion of a sequent, then $|\Pi \vdash \Lambda| = \sum_{E \in \Pi\cup\Lambda} |E|$.

For reading out expansions from proofs, the following merge-operation will be useful. For our purposes it is enough to use it on expansions of formulas without strong quantifiers and for the sake of simplicity we restrict our definition to this case.

Definition 7. If E_1 and E_2 are expansions of the same formula A without strong quantifiers, then their union $E_1 \cup E_2$ is again an expansion of A and is defined as follows:

1. If $E_1 = \bot$, then $E_1 \cup E_2 = E_2$. If $E_2 = \bot$, then $E_1 \cup E_2 = E_1$.
2. If $E_1 = E_1' \vee E_1''$ and $E_2 = E_2' \vee E_2''$, then $E_1 \cup E_2 = (E_1' \cup E_2') \vee (E_1'' \cup E_2'')$.
3. If $E_1 = \neg E_1'$ and $E_2 = \neg E_2'$, then $E_1 \cup E_2 = \neg(E_1' \cup E_2')$.
4. If
$$E_1 = \exists x\, A' +^{r_1} E_{1,1} \ldots +^{r_k} E_{1,k} +^{s_1} F_1 \ldots +^{s_l} F_l \text{ and}$$
$$E_2 = \exists x\, A' +^{r_1} E_{2,1} \ldots +^{r_k} E_{2,k} +^{t_1} G_1 \ldots +^{t_m} G_m$$
where $\{s_1, \ldots , s_l\} \cap \{t_1, \ldots , t_m\} = \emptyset$, then
$$\begin{aligned} E_1 \cup E_2 = \exists x\, A' \ & +^{r_1}(E_{1,1} \cup E_{2,1}) \ldots +^{r_k} (E_{1,k} \cup E_{2,k}) \\ & +^{s_1}F_1 \ldots +^{s_l} F_l \\ & +^{t_1}G_1 \ldots +^{t_m} G_m \end{aligned}$$

For dual expansions the analogous definition applies where $\top$ replaces $\bot$ and $\forall$ replaces $\exists$. The union of expansions of sequents is defined by componentwise union.

Note that $|E_1 \cup E_2| \leq |E_1| + |E_2|$ which can be shown by a straightforward induction.

Lemma 1. *Let E_1, E_2 be expansions of the same formula without strong quantifiers, then* $\mathrm{Dp}(E_1) \vee \mathrm{Dp}(E_2) \Rightarrow \mathrm{Dp}(E_1 \cup E_2)$. *For dual expansions E_1, E_2 of the same formula* $\mathrm{Dp}(E_1 \cup E_2) \Rightarrow \mathrm{Dp}(E_1) \vee \mathrm{Dp}(E_2)$ *and for S_1, S_2 being expansions of the same sequent* $\mathrm{Dp}(S_1) \vee \mathrm{Dp}(S_2) \Rightarrow \mathrm{Dp}(S_1 \cup S_2)$.

Proof. The result on sequents follows directly from the results on formulas which are proved simultaneously by a straightforward induction on the structure of the formula of which E_1 and E_2 are expansions. The most interesting case of this induction is that of $\vee$ for dual expansions as it hinders the logical equivalence: For $E_1 = E_1' \vee E_1''$ and $E_2 = E_2' \vee E_2''$ being dual expansions we have $E_1 \cup E_2 = (E_1' \cup E_2') \vee (E_1'' \cup E_2'')$, so

$$\mathrm{Dp}(E_1 \cup E_2) \Leftrightarrow (\mathrm{Dp}(E_1') \wedge \mathrm{Dp}(E_2')) \vee (\mathrm{Dp}(E_1'') \wedge \mathrm{Dp}(E_2''))$$

by induction hypothesis and

$$\mathrm{Dp}(E_1) \wedge \mathrm{Dp}(E_2) \Leftrightarrow (\mathrm{Dp}(E_1') \vee \mathrm{Dp}(E_1'')) \wedge (\mathrm{Dp}(E_2') \vee \mathrm{Dp}(E_2'')).$$

⊣

Lemma 2. *Let π be a cut-free* **LK***-proof of a sequent $\Gamma \vdash \Delta$ which does not contain any strong quantifiers. Then there is a tautological expansion $\Pi \vdash \Lambda$ of $\Gamma \vdash \Delta$ s.t. $|\Pi \vdash \Lambda| \leq |\pi|$.*

Proof. By induction on π: for the case of π being an axiom $A, \Gamma \vdash \Delta, A$, or $\Gamma \vdash \Delta, \top$, or $\bot, \Gamma \vdash \Delta$ let $\Pi \vdash \Lambda$ be $A, \top, \ldots , \top \vdash \bot, \ldots , \bot, A$, or $\top, \ldots , \top \vdash \bot, \ldots , \bot, \top$, or $\bot, \top, \ldots , \top \vdash \bot, \ldots , \bot$ respectively. In any case, $\Pi \vdash \Lambda$ is tautological and $|\Pi \vdash \Lambda| = 0$.

If π has the form

$$\dfrac{\begin{array}{c}(\psi)\\ \Gamma \vdash \Delta, A\end{array}}{\neg A, \Gamma \vdash \Delta}\ \neg_l$$

we obtain a tautological expansion $\Pi \vdash \Lambda, E$ of $\Gamma \vdash \Delta, A$ from the induction hypothesis. Then $\neg E, \Pi \vdash \Lambda$ is a tautological expansion of $\neg A, \Gamma \vdash \Delta$ and

$$|\neg E, \Pi \vdash \Lambda| = |\Pi \vdash \Lambda, E| + 1 \leq |\psi| + 1 = |\pi|.$$

The other unary propositional rules are treated analogously.

If π has the form

$$\dfrac{\begin{array}{c}(\psi_1)\\ A_1, \Gamma \vdash \Delta\end{array} \quad \begin{array}{c}(\psi_2)\\ A_2, \Gamma \vdash \Delta\end{array}}{A_1 \vee A_2, \Gamma \vdash \Delta}\ \vee_l$$

we obtain expansions $E_1, \Pi_1 \vdash \Lambda_1$ and $E_2, \Pi_2 \vdash \Lambda_2$ of $A_1, \Gamma \vdash \Delta$ and $A_2, \Gamma \vdash \Delta$ respectively by induction hypothesis. Let $\Pi \vdash \Lambda$ be $E_1 \vee E_2, \Pi_1 \cup \Pi_2 \vdash \Lambda_1 \cup \Lambda_2$ and observe that, by Lemma 1,

$$\begin{aligned}
\mathrm{Dp}(E_1 \vee E_2,&\Pi_1 \cup \Pi_2 \vdash \Lambda_1 \cup \Lambda_2)\\
&\Leftarrow (\neg E_1 \wedge \neg E_2) \vee \mathrm{Dp}(\Pi_1 \vdash \Lambda_1) \vee \mathrm{Dp}(\Pi_2 \vdash \Lambda_2)\\
&\Leftarrow (\neg E_1 \vee \mathrm{Dp}(\Pi_1 \vdash \Lambda_1)) \wedge (\neg E_2 \vee \mathrm{Dp}(\Pi_2 \vdash \Lambda_2))\\
&\Leftrightarrow \mathrm{Dp}(E_1, \Pi_1 \vdash \Lambda_1) \wedge \mathrm{Dp}(E_2, \Pi_2 \vdash \Lambda_2)
\end{aligned}$$

which is tautological by induction hypothesis. Furthermore

$$|\Pi \vdash \Lambda| = |E_1, \Pi_1 \vdash \Lambda_1| + |E_2, \Pi_2 \vdash \Lambda_2| + 1 \leq |\psi_1| + |\psi_2| + 1 = |\pi|.$$

The other binary propositional rules are treated analogously.

If π is of the form

$$\dfrac{\begin{array}{c}(\psi)\\ \Gamma \vdash \Delta, \exists x\, A, A\{x \leftarrow t\}\end{array}}{\Gamma \vdash \Delta, \exists x\, A}\ \exists_r$$

we obtain an expansion $\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n, E$ of $\Gamma \vdash \Delta, \exists x\, A, A\{x \leftarrow t\}$ by induction hypothesis. Then $\Pi \vdash \Lambda, (\exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n) \cup (\exists x\, A +^{t} E)$ is tautological as by Lemma 1

$$\begin{aligned}
\mathrm{Dp}(\Pi \vdash \Lambda,&(\exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n) \cup (\exists x\, A +^{t} E))\\
&\Leftarrow \mathrm{Dp}(\Pi \vdash \Lambda) \vee \mathrm{Dp}(\exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n) \vee \mathrm{Dp}(\exists x\, A +^{t} E)\\
&\Leftrightarrow \mathrm{Dp}(\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n, E)
\end{aligned}$$

which is tautological by induction hypothesis. Furthermore

$$\begin{aligned}
|\Pi \vdash \Lambda,&(\exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n) \cup (\exists x\, A +^{t} E)|\\
&\leq |\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n| + |E| + 1\\
&= |\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n, E| + 1\\
&\leq |\psi| + 1 = |\pi|.
\end{aligned}$$

The $\forall_l$-rule is treated analogously. $\dashv$

We write sk^{d} for the operator that is dual to sk, i.e. where the roles of strong and weak quantifiers are exchanged. A formula F is satifiability-equivalent to $\mathrm{sk}^{\mathrm{d}}(F)$.

Lemma 3. *Let A be a formula and E be an expansion (or dual expansion) of $A' = \mathrm{sk}(A)$ (or $A' = \mathrm{sk}^{\mathrm{d}}(A)$ respectively), then there is an expansion (a dual expansion) F of A with* $\mathrm{Dp}(E) = \mathrm{Dp}(F)$ *and* $|F| \leq |E|\mathrm{qocc}(A) + |E| + \mathrm{qocc}(A)$.

Proof. By induction on A. If A is an atom let $F := E$.

If $A = A_1 \vee A_2$, then $E = E_1 \vee E_2$ is an expansion of $A' = A_1' \vee A_2'$ and by induction hypothesis we obtain expansions F_1 of A_1 and F_2 of A_2 respectively. Define $F := F_1 \vee F_2$ and observe that $\mathrm{Dp}(F) = \mathrm{Dp}(E)$. Furthermore,

$$\begin{aligned}|F| &\leq |E_1|\mathrm{qocc}(A_1) + |E_1| + \mathrm{qocc}(A_1) + |E_2|\mathrm{qocc}(A_2) + |E_2| + \mathrm{qocc}(A_2) + 1\\ &= \mathrm{qocc}(A) + |E| + |E_1|\mathrm{qocc}(A_1) + |E_2|\mathrm{qocc}(A_2)\\ &\leq \mathrm{qocc}(A) + |E| + |E|\mathrm{qocc}(A).\end{aligned}$$

If $A = \neg A_0$, then $E = \neg E_0$ is an expansion of $A' = \neg A_0'$ and by induction hypothesis we obtain a dual expansion F_0 of A_0. Define $F := \neg F_0$ and observe $\mathrm{Dp}(F) = \mathrm{Dp}(E)$ and

$$\begin{aligned}|F| &\leq |E_0|\mathrm{qocc}(A) + |E_0| + \mathrm{qocc}(A) + 1\\ &= |E|\mathrm{qocc}(A) + |E|.\end{aligned}$$

If $A = \exists x\, A_0$, then $E = \exists x\, A_0' +^{t_1} E_1 \ldots +^{t_n} E_n$ is an expansion of $\exists x\, A_0'$ hence $E_1, \ldots, E_n$ are expansions of $A_0'\{x \leftarrow t_1\}, \ldots, A_0'\{x \leftarrow t_n\}$ which are the Skolemizations of $A_0\{x \leftarrow t_1\}, \ldots, A_0\{x \leftarrow t_n\}$. From the induction hypothesis we obtain expansions $F_1, \ldots, F_n$ of $A_0\{x \leftarrow t_1\}, \ldots, A_0\{x \leftarrow t_n\}$ and define $F := \exists x\, A_0 +^{t_1} F_1 \ldots +^{t_n} F_n$. Observe that $\mathrm{Dp}(F) = \bigvee_{i=1}^{n} \mathrm{Dp}(F_i) = \bigvee_{i=1}^{n} \mathrm{Dp}(E_i) = \mathrm{Dp}(E)$ and that

$$\begin{aligned}|F| &\leq \sum_{i=1}^{n}(|E_i|\mathrm{qocc}(A) + |E_i| + \mathrm{qocc}(A) + 1)\\ &= \sum_{i=1}^{n}(|E_i| + 1)\mathrm{qocc}(A) + \sum_{i=1}^{n}(|E_i| + 1)\\ &= \mathrm{qocc}(A)|E| + |E|.\end{aligned}$$

If $A = \forall x\, A_0$, then E is an expansion of $A_0'\{x \leftarrow f(\bar{t})\}$. We apply the induction hypothesis to $A_0\{x \leftarrow f(\bar{t})\}$ and E to obtain an expansion F_0 of $A_0\{x \leftarrow f(\bar{t})\}$. Define $F := \forall x\, A_0 +^{f(\bar{t})} F_0$ and observe that $\mathrm{Dp}(F) = \mathrm{Dp}(F_0) = \mathrm{Dp}(E)$ and

$$\begin{aligned}|F| &\leq |E|\mathrm{qocc}(A_0\{x \leftarrow f(\bar{t})\}) + |E| + \mathrm{qocc}(A_0\{x \leftarrow f(\bar{t})\}) + 1\\ &= |E|\mathrm{qocc}(A) + \mathrm{qocc}(A).\end{aligned}$$

The dual cases are analogous. ⊣

Lemma 4. *Let S be a sequent and E be an expansion of* $\mathrm{sk}(S)$, *then there is an expansion F of S with* $\mathrm{Dp}(E) = \mathrm{Dp}(F)$ *and* $|F| \leq |E|\mathrm{qocc}(S) + |E| + \mathrm{qocc}(S)$.

Proof. This follows from applying the above Lemma 3 to every formula in S and the additional observation that every $t \in \mathrm{SkTerms}(F)$ designates a unique strong quantifier node in F. For suppose there were two strong quantifier nodes having t as Skolem term, then they must appear in different expansions (or dual expansions) E_1 and E_2. This however is impossible as each Skolem symbol in $\mathrm{sk}(S)$ corresponds to a unique strong quantifier in S. ⊣

Definition 8. The calculus $\mathbf{LK^E}$ works on expansion sequents and is defined as follows: axioms are of the form

$$A, \Pi \vdash \Lambda, A, \quad \Pi \vdash \Lambda, \top, \text{ or } \quad \bot, \Pi \vdash \Lambda$$

for an atom A. The rules are

$$\frac{E_1, \Pi \vdash \Lambda \quad E_2, \Pi \vdash \Lambda}{E_1 \vee E_2, \Pi \vdash \Lambda} \vee_l \quad \frac{\Pi \vdash \Lambda, E_1, E_2}{\Pi \vdash \Lambda, E_1 \vee E_2} \vee_r \quad \frac{\Pi \vdash \Lambda, E}{\neg E, \Pi \vdash \Lambda} \neg_l \quad \frac{E, \Pi \vdash \Lambda}{\Pi \vdash \Lambda, \neg E} \neg_r$$

and analogously for $\wedge$ and $\rightarrow$. Furthermore

$$\frac{\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_{i-1}} E_{i-1} +^{t_{i+1}} E_{i+1} \ldots +^{t_n} E_n, E_i}{\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n} \exists_r$$

$$\frac{E, \Pi \vdash \Lambda}{\exists x\, A +^t E, \Pi \vdash \Lambda} \exists_l$$

and analogously for $\forall_r$ and $\forall_l$.

If ι is an $\exists_r$-inference we write $\mathrm{t}(\iota)$ for t_i and if ι is an $\exists_l$-inference we write $\mathrm{t}(\iota)$ for t. The above calculus will (only) be used for a bottom-up proof construction. The rules of $\mathbf{LK^E}$ are invertible in the sense that, for every unary rule, $\mathrm{Dp}(C) \Rightarrow \mathrm{Dp}(P)$ for C being the conclusion of the rule and P the premise, as well as $\mathrm{Dp}(C) \Rightarrow \mathrm{Dp}(P_1) \wedge \mathrm{Dp}(P_2)$ for P_1, P_2 for the binary rule with premises P_1, P_2. Furthermore, if the conclusion of a rule is an expansion so are its premises (the converse is not true). The depth of a proof π is the maximal number of inferences on a branch of π.

Lemma 5. *Let π be an $\mathbf{LK^E}$-proof of an expansion E, then* $\mathrm{depth}(\pi) \leq |E|$.

Proof. It is easy to check that a premise of a rule has a logical complexity which is strictly smaller than that of its conclusion. ⊣

Definition 9. For an expansion E we define the Skolem term ordering $\prec_E$ as $s \prec_E t$ if

1. s is a proper subterm of t, or
2. E contains a strong quantifier $Qx\, A' +^s E'$ and E' contains a strong quantifier $Qy\, A'' +^t E''$.

Note that the above ordering $\prec_E$ is wellfounded on any set of terms T: let $M \subseteq T$ be the set of terms which is minimal w.r.t. the subterm-ordering (which is well-founded), then there is at least one $t \in M$ which belongs to an outermost strong quantifier. This is a minimal term w.r.t. $\prec_E$ on T. With $\preceq$ we denote the reflexive closure of an ordering $\prec$.

Definition 10. An $\mathbf{LK^E}$-proof is called compatible with a term ordering $\preceq$ if for all quantifier inferences ι_1 and ι_2 where ι_1 is strong and is above ι_2 we have $\mathrm{t}(\iota_1) \not\preceq \mathrm{t}(\iota_2)$.

LEMMA 6. *Every tautological expansion $\Pi \vdash \Lambda$ has an $\mathbf{LK^E}$-proof that is compatible with $\preceq_{\Pi\vdash\Lambda}$.*

PROOF. We proceed by induction on the cardinality of $\mathrm{SkTerms}(\Pi \vdash \Lambda)$. For $\mathrm{SkTerms}(\Pi \vdash \Lambda) = \emptyset$ any bottom-up proof search yields a proof by invertibility of the rules, so let $\mathrm{SkTerms}(\Pi \vdash \Lambda) \neq \emptyset$. By well-foundedness of $\prec_{\Pi\vdash\Lambda}$ there exists a $\prec_{\Pi\vdash\Lambda}$-minimal element in $\mathrm{SkTerms}(\Pi \vdash \Lambda)$, say $f(\bar{s}, \bar{t})$ where $\bar{t} = t_1, \ldots , t_n$. Let Qy be the unique strong quantifier in $\Pi \vdash \Lambda$ that is associated to $f(\bar{s}, \bar{t})$ and let E be the expansion (or dual expansion) that contains Qy. Then the weak quantifiers dominating Qy in E are $Qx_1, \ldots , Qx_n$ with terms $t_1, \ldots , t_n$ respectively. Furthermore Qy is not dominated by a strong quantifier due to $\prec_{\Pi\vdash\Lambda}$-minimality.

A bottom segment of the proof of $\Pi \vdash \Lambda$ is constructed by induction on the depth of Qy in E: if the outermost connective is propositional, the corresponding rule is applied, if the outermost connective is a quantifier, then it is one of the Qx_i for $1 \leq i \leq n$ and the weak quantifier rule is applied to the term t_i. If the outermost connective is a strong quantifier, then by the above observation, it is Qy in which case we apply the corresponding rule yielding the term $f(\bar{s}, \bar{t})$. The leaves $\Pi_1 \vdash \Lambda_1, \ldots , \Pi_m \vdash \Lambda_m$ of the proof segment just constructed are tautological by the invertibility of the rules and have strictly smaller sets of Skolem-terms, so we can complete the proof construction by obtaining proofs $\pi_1, \ldots , \pi_m$ of them by induction hypothesis. It remains to prove compatibility with $\prec_{\Pi\vdash\Lambda}$.

If ι_1 is the inference introducing Qy then as ι_1 is above ι_2, ι_2 is introducing Qx_i for an $i \in \{1, \ldots , n\}$ and in this case $\mathrm{t}(\iota_2) = t_i$ is a proper subterm of $f(\bar{s}, \bar{t}) = \mathrm{t}(\iota_1)$ hence $\mathrm{t}(\iota_1) \not\preceq_{\Pi\vdash\Lambda} \mathrm{t}(\iota_2)$.

If ι_1 is above ι_2 and both are in some π_i, then by induction hypothesis $\mathrm{t}(\iota_1) \not\preceq_{\Pi_i\vdash\Lambda_i} \mathrm{t}(\iota_2)$ hence $\mathrm{t}(\iota_1)$ is not a subterm of $\mathrm{t}(\iota_2)$. Suppose now, for the sake of contradiction, that $\mathrm{t}(\iota_1) \preceq_{\Pi\vdash\Lambda} \mathrm{t}(\iota_2)$, then $\Pi \vdash \Lambda$ must contain a strong quantifier $Qx\, A' +^{\mathrm{t}(\iota_1)} E'$ and E' must contain a strong quantifier $Qy\, A'' +^{\mathrm{t}(\iota_2)} E''$. But as both ι_1 and ι_2 are in π_i also $\Pi_i \vdash \Lambda_i$ must contain $Qx\, A' +^{\mathrm{t}(\iota_1)} E'$ contradicting $\mathrm{t}(\iota_1) \not\preceq_{\Pi_i\vdash\Lambda_i} \mathrm{t}(\iota_2)$.

If ι_1 is in π_i and ι_2 in the bottom segment, then $\mathrm{t}(\iota_1) \neq f(\bar{s}, \bar{t})$ because $f(\bar{s}, \bar{t}) \notin \mathrm{SkTerms}(\Pi_i \vdash \Lambda_i)$. Furthermore both $\mathrm{t}(\iota_1) \prec_{\Pi\vdash\Lambda} f(\bar{s}, \bar{t})$ as well as $\mathrm{t}(\iota_1) \prec_{\Pi\vdash\Lambda} t_j \prec_{\Pi\vdash\Lambda} f(\bar{s}, \bar{t})$ for some $j \in \{1, \ldots , n\}$ would contradict $\prec_{\Pi\vdash\Lambda}$-minimality of $f(\bar{s}, \bar{t})$. ⊣

LEMMA 7. *Let E be an expansion of a sequent S that does not contain Skolem symbols and let π be an $\mathbf{LK^E}$-proof of E which is compatible with $\preceq_E$. Then there is an $\mathbf{LK}$-proof ψ of S with* $\mathrm{depth}(\psi) = \mathrm{depth}(\pi)$.

PROOF. It suffices to construct such a proof ψ of $\mathrm{Sh}(E)$ as a proof of S can then be obtained by replacing positive occurrences of $\bot$ and negative occurrences of $\top$ by subformulas of S which does not change the depth of the proof.

We proceed by induction on π. The translation of axioms, propositional and weak quantifier rules are straightforward, so consider a subproof π_1 of π of the form

$$\frac{\begin{matrix}(\pi_0)\\ E_0, \Pi \vdash \Lambda\end{matrix}}{\exists x\, A +^{f(\bar{t})} E_0, \Pi \vdash \Lambda}\ \exists_l$$

By induction on the depth of π_1 in π, and using the assumption that S does not contain Skolem terms, one can show that

$$\mathrm{SkTerms}(\mathrm{Sh}(\exists x\, A +^{f(\bar{t})} E_0, \Pi \vdash \Lambda)) \subseteq \mathrm{Subterms}(\{\mathrm{t}(\iota_1), \dots, \mathrm{t}(\iota_n)\})$$

where $\iota_1, \dots, \iota_n$ are the quantifier inferences below π_1 in π. By compatibility of π with $\preceq_E$ we have $f(\bar{t}) \not\preceq_E \mathrm{t}(\iota_i)$ hence $f(\bar{t}) \notin \mathrm{Subterms}(\{\mathrm{t}(\iota_1), \dots, \mathrm{t}(\iota_n)\}$.

By induction hypothesis there is an **LK**-proof ψ_0 of $\mathrm{Sh}(E_0, \Pi \vdash \Lambda)$. Let α be a fresh variable and ψ_0' be the result of replacing all occurrences of $f(\bar{t})$ in ψ_0 by α. Let ψ_1 be

$$\frac{\begin{matrix}(\psi_0)\\ \mathrm{Sh}(E_0, \Pi \vdash \Lambda)\end{matrix}}{\mathrm{Sh}(\exists x\, A +^{f(\bar{t})} E_0, \Pi \vdash \Lambda)}\ \exists_l$$

which is a valid rule application as $f(\bar{t}) \notin \mathrm{Terms}(\mathrm{Sh}(\exists x\, A +^{f(\bar{t})} E_0, \Pi \vdash \Lambda))$. ⊣

Theorem 2. *Let S be a sequent that does not contain Skolem symbols and π be an* **LK***-proof of* $\mathrm{sk}(S)$*, then there is an* **LK***-proof ψ of S with* $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$ *and hence* $|\psi| \leq 2^{|\pi|\mathrm{qocc}(S)+|\pi|+\mathrm{qocc}(S)}$.

Proof. By Lemma 2 there is a tautological expansion E of $\mathrm{sk}(S)$ s.t. $|E| \leq |\pi|$. By Lemma 4 there is a tautological expansion F of S with $|F| \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$. By Lemma 6 there is an $\mathbf{LK^E}$-proof χ of F which is compatible with $\preceq_F$ and, by Lemma 5, has $\mathrm{depth}(\chi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$. Finally, by Lemma 7, we obtain an **LK**-proof ψ of S with $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$. ⊣

The above upper bound refers to cut-free proofs only. However one can use this result to obtain a similar upper bound on a class of proofs with cuts as follows. For the rest of this section, we augment our calculus **LK** by the following cut-rule:

$$\frac{\Gamma \vdash \Delta, A \quad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\ \mathrm{cut}$$

Let π be an **LK**-proof, let $\alpha_1, \dots, \alpha_n$ be the eigenvariables of π and let $T = \{t_1 = \alpha_1, \dots, t_n = \alpha_n, t_{n+1}, \dots, t_m\}$ be a set of terms. Denote by $\check{\pi}^T$ the cut-free proof obtained from π by replacing every cut by an $\rightarrow_l$-inference followed by $\forall_l$-inferences to bind all occurrences of terms from T (this is a slightly more general version of proof transformations that also appear in [2, 4]). If the endsequent of π is $\Gamma \vdash \Delta$, then the endsequent of $\check{\pi}^T$ is $\Sigma, \Gamma \vdash \Delta$ where

$$\Sigma \ = \ \forall x_1 \dots \forall x_m\, (A_1 \rightarrow A_1), \dots, \forall x_1 \dots \forall x_m\, (A_k \rightarrow A_k)$$

and $A_1\{x_i \leftarrow t_i\}_{i=1}^m, \dots, A_k\{x_i \leftarrow t_i\}_{i=1}^m$ are the cut formulas of π. As there are at most $|\pi|$ many cuts we add at most $|\pi||T|$ new inferences and obtain $|\check{\pi}^T| \leq (|T| + 1)|\pi|$.

Conversely, if χ is a proof of a sequent $\Sigma, \Gamma \vdash \Delta$ with Σ of the above form, denote with $\hat{\chi}$ the proof of $\Gamma \vdash \Delta$ which is obtained from replacing every $\rightarrow_l$-inference pertaining to an $(A_j \rightarrow A_j)\{x_i \leftarrow t_{j,i}\}_{i=1}^{n}$ by a cut and removing the $\forall_l$-inferences. If an ancestor path of a formula in Σ does not contain an $\rightarrow_l$-inference, it starts with weakening and is removed without increasing the depth of the proof, hence $\mathrm{depth}(\hat{\chi}) \leq \mathrm{depth}(\chi)$.

Corollary 1. *Let S be a sequent that does not contain Skolem symbols and π be an* **LK***-proof of* $\mathrm{sk}(S)$ *s.t. every term that starts with a Skolem symbol and appears in a cut formula of π does not contain a bound variable. Let $A_1, \dots, A_k$ be the cut formulas of π and let c be the number of quantifiers in $\{A_1, \dots, A_k\}$. Then there is an* **LK***-proof ψ of S s.t.* $\mathrm{depth}(\psi) \leq (|\pi|^2 \mathrm{qocc}(S) + |\pi| + 1)(c + \mathrm{qocc}(S) + 1)$ *and hence* $|\psi| \leq 2^{(|\pi|^2 \mathrm{qocc}(S)+|\pi|+1)(c+\mathrm{qocc}(S)+1)}$.

Proof. Let $S = \Gamma \vdash \Delta$ and $\mathrm{sk}(S) = \Gamma' \vdash \Delta'$. Let $T = \{t_1 = \alpha_1, \dots, t_n = \alpha_n, t_{n+1}, \dots, t_m\}$ where $\{\alpha_1, \dots, \alpha_n\}$ are the eigenvariables of π and $\{t_{n+1}, \dots, t_m\}$ are all Skolem terms of π that do not contain bound variables. Now $|T| \leq |\pi| \mathrm{qocc}(\Gamma \vdash \Delta)$ because every Skolem term $t \in T$ starts with a certain Skolem symbol f of which there are $\mathrm{qocc}(\Gamma \vdash \Delta)$ many. Furthermore, for each f the number of different $f(\bar{t})$'s is bound by the number of paths of weak quantifier inferences corresponding to the weak quantifiers that bind variables in $f(\bar{x})$ in $\Gamma \vdash \Delta$, i.e. by the number of weak quantifier inferences which are uppermost in such paths, i.e. by $|\pi|$.

Now $\psi_0 = \check{\pi}^T$ is a cut-free proof of $\Sigma, \Gamma' \vdash \Delta'$ and Σ does not contain Skolem symbols. Let ψ_1 be the proof of $\Sigma', \Gamma' \vdash \Delta'$ obtained from skolemizing ψ_0. Note that $\Sigma', \Gamma' \vdash \Delta'$ is a skolemization of $\Sigma, \Gamma \vdash \Delta$ which does not contain Skolem symbols. Therefore we can apply Theorem 2 to obtain a cut-free proof ψ_2 of $\Sigma, \Gamma \vdash \Delta$ with

$$\begin{aligned} \mathrm{depth}(\psi_2) &\leq |\psi_1| \mathrm{qocc}(\Sigma, \Gamma \vdash \Delta) + |\psi_1| + \mathrm{qocc}(\Sigma, \Gamma \vdash \Delta) \\ &\leq (|\pi|^2 \mathrm{qocc}(S) + |\pi| + 1)(c + \mathrm{qocc}(S) + 1) \end{aligned}$$

Finally $\psi = \hat{\psi_2}$ is a proof of $\Gamma \vdash \Delta$ with $\mathrm{depth}(\psi) \leq \mathrm{depth}(\psi_2)$. ⊣

The above corollary provides a necessary condition for a super-exponential lower bound: to contain Skolem terms with bound variables. Note that in the context of Skolemization in higher-order logic, a similar condition was formulated in [9]: essentially, it also forbids the application of Skolem symbols to terms containing bound variables. There, the condition was formulated for soundness (without it, the Skolemization of the axiom of choice becomes provable), while in our setting, it concerns complexity.

§4. A lower bound. For our lower bound, we consider the language $\mathcal{L} = \{P_1, P_2, \dots, G_0, G_1, G_2 \dots\}$ where the P_i are one-place predicate symbols and the G_i are zero-place predicate symbols. The following sequence will be central to proving the lower bound:

1. $R_0 = G_0 \rightarrow G_0$.
2. For $N > 0$, $R_N = ((\exists x_N) P_N(x_N) \vee G_N) \rightarrow (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})$.

DEFINITION 11. Let F be a formula, then the size of F, denoted by $||F||$, is defined as the number of (logical and non-logical) symbols in F.

The sizes of the formulas are moderate, but their proofs are long:

PROPOSITION 2. $||R_N|| = 16 * N + 4$.

THEOREM 3. *For all* **LK***-proofs* π *of* $\vdash R_N$, $|\pi| \geq 2^{N+1}$.

PROOF. We proceed by induction on N:

1. $N = 0$. Then π:

$$\frac{G_0 \vdash G_0}{\vdash G_0 \to G_0} \to_r$$

is the shortest **LK** proof of $\vdash R_0$. Note that $|\pi| = 2$.

2. $N > 0$. We will describe the shortest **LK** proof π of R_N, arguing at every step that there is only one way to apply the rules. We will also give countermodels to show that some rules are not applicable, for this purpose we will give interpretations $\mathcal{M}$ with domain $M = \{a, b\}$. The induction hypothesis (IH) is: all proofs ψ of $\vdash R_{N-1}$ are such that $|\psi| \geq 2^N$. π has the form

$$\cfrac{\cfrac{\pi_1 \qquad \pi_2}{(\exists x_N)P_N(x_N) \vee G_N \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})} \vee_l \ (2)}{\vdash ((\exists x_N)P_N(x_N) \vee G_N) \to (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})} \to_r \ (1)$$

because in step (1), only $\to_r$ is applicable. In step (2), $\exists_r$ is not applicable, as $((\exists x_N)P_N(x_N)) \vee G_N \vdash ((P_N(s) \vee G_N) \wedge R_{N-1})$ is not valid for any term s. To see this, set $G_N^{\mathcal{M}} = \mathrm{f}$, and if $s^{\mathcal{M}} = a$ set $P_N^{\mathcal{M}} = \{b\}$ (and analogously if $s^{\mathcal{M}} = b$). Therefore we have to apply $\vee_l$.

π_1 is

$$\cfrac{\cfrac{(\psi)}{P_N(\alpha_N) \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})}}{(\exists x_N)P_N(x_N) \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})} \exists_l \ (3)$$

because in step (3), $\exists_r$ cannot be applied: the countermodel from the previous paragraph is also a countermodel here. So $\exists_l$ has to be applied. We claim that $|\psi| \geq 2^N$. This follows by (IH) and the following:

LEMMA 8. *Let* π *be a proof of* $P_N(\alpha_N) \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})$. *Then there exists a proof* ψ *of* $\vdash R_{N-1}$ *such that* $|\psi| \leq |\pi|$.

which we will prove later. This completes the argument for π_1.

The end-sequent of π_2 is $G_N \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})$. We claim that $|\pi_2| \geq 2^N$. This follows by (IH) and the following:

LEMMA 9. *Let* π *be a proof of* $G_N \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})$. *Then there exists a proof* ψ *of* $\vdash R_{N-1}$ *such that* $|\psi| \leq |\pi|$.

which we will also prove later.

Hence we find that for some constant k,

$$|\pi| = k + |\psi| + |\pi_2| \geq k + 2 * 2^N = k + 2^{N+1} \geq 2^{N+1}.$$

⊣

We will use the following result from [11], which also holds for our modified version of **G3c**:

PROPOSITION 3. *For all* A, Γ, Δ

1. *If* π *is an* **LK**-*proof of* $A, A, \Gamma \vdash \Delta$ *then there exists an* **LK**-*proof* ψ *of* $A, \Gamma \vdash \Delta$ *such that* $|\psi| \leq |\pi|$.
2. *If* π *is an* **LK**-*proof of* $\Gamma \vdash \Delta, A, A$ *then there exists an* **LK**-*proof* ψ *of* $\Gamma \vdash \Delta, A$ *such that* $|\psi| \leq |\pi|$.

Now, we are ready to give the missing proofs:

PROOF OF LEMMA 8. First, note that for all axioms $A, \Gamma \vdash \Delta, A$ in π, it holds that $A \neq G_N$ (because G_N occurs only in one polarity), and if $A = P_N(s)$ for some term s then A occurs in a subproof φ_1 of the form

$$\dfrac{\begin{matrix}(\varphi_1) \\ \Pi \vdash \Lambda, P_N(s) \vee G_N\end{matrix} \qquad \begin{matrix}(\varphi_2) \\ \Pi \vdash \Lambda, R_{N-1}\end{matrix}}{\Pi \vdash \Lambda, (P_N(s) \vee G_N) \wedge R_{N-1}} \wedge_r$$

in π (because the indicated occurrence of $P_N(y_N)$ in the end-sequent is the only positive occurrence of P_N in the end-sequent). Call such subproofs φ_1 of π *degenerate*, and call inferences occuring in degenerate subproofs degenerate. Further, call an occurrence in π *replaceable* if it is an ancestor of the occurrence of $(\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})$ in the end-sequent of π that (still) contains the indicated disjunction.

Let ρ be an inference in π with conclusion $\Gamma \vdash \Delta, \Theta$, where Θ are the replaceable occurrences (note that this is general as replaceable occurrences can only occur on the rhs). By induction on the height of ρ, we will define a proof π_ρ of $\Gamma \vdash \Delta, R_{N-1}, \ldots, R_{N-1}$ if ρ is not degenerate. Otherwise π_ρ is undefined. Hence we only consider inferences ρ which are not degenerate:

1. If ρ is an axiom $A, \Pi \vdash \Lambda, A$, then replaceable occurrences occur at most in Π, Λ (otherwise ρ would be degenerate by the argument given above). Hence we may replace those occurrences by R_{N-1} to obtain a suitable axiom to take for π_ρ.
2. If ρ does not operate on replaceable occurrences then we obtain π_ρ from the proofs π_{ρ_1} (π_{ρ_2}) obtained by induction hypothesis by applying ρ. Note that since ρ is not degenerate by assumption and does not operate on replaceable occurrences, ρ_1 (and ρ_2) are also not degenerate.
3. If ρ is an $\wedge_r$ inference operating on a replaceble occurrence with premises ρ_1, ρ_2, then ρ is of the form:

$$\dfrac{\begin{matrix}(\varphi_1) \\ \Gamma \vdash \Delta, P_N(s) \vee G_N\end{matrix} \qquad \begin{matrix}(\varphi_2) \\ \Gamma \vdash \Delta, \Theta, R_{N-1}\end{matrix}}{\Gamma \vdash \Delta, \Theta, (P_N(s) \vee G_N) \wedge R_{N-1}} \wedge_r$$

Note that φ_2 is degenerate only if the proof ending in ρ is, which is not the case by assumption. Hence we set $\pi_\rho = \pi_{\rho_2}$ which is a proof of $\Gamma \vdash \Delta, R_{N-1}, \ldots, R_{N-1}$ by induction hypothesis.

4. If ρ is an $\vee_r$ inference operating on a replaceable occurrence, then it is degenerate and hence we do not treat this case.
5. If ρ is an $\exists_r$ inference operating on a replaceable occurrence with premise ρ' then ρ is of the form

$$\frac{\overset{(\varphi)}{\Gamma \vdash \Delta, \Theta, (P_N(s) \vee G_N) \wedge R_{N-1}, (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})}}{\Gamma \vdash \Delta, \Theta, (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})} \exists_r$$

   Again φ is degenerate only if the subproof ending in ρ is, which is not the case by assumption. Hence we may set $\pi_\rho = \pi_{\rho'}$ which is a proof of $\Gamma \vdash \Delta, R_{N-1}, \ldots, R_{N-1}$ by induction hypothesis.

Observe that if ρ_0 is the last inference in π then π_{ρ_0} is a proof of $P_N(\alpha_N) \vdash R_{N-1}, \ldots, R_{N-1}$ and by construction, $|\pi_{\rho_0}| \leq |\pi|$. As $P_N(\alpha_N)$ occurs only in one polarity, π_{ρ_0} can easily be transformed into a proof ψ of $\vdash R_{N-1}, \ldots, R_{N-1}$ such that $|\psi| \leq |\pi_{\rho_0}|$. Finally, we apply Proposition 3 multiple times to obtain the desired **LK**-proof of $\vdash R_{N-1}$. ⊣

Lemma 9 is proved analogously.

While R_N has only long proofs, its Skolemization has short proofs. The Skolemization of R_N is S_N^N where for all N and for all $n \leq N$ we define

1. $S_0^N = G_0 \to G_0$.
2. For $n > 0$,

$$S_n^N = (P_n(f_{N-n}(y_N, y_{N-1}, \ldots, y_{n+1})) \vee G_n) \to (\exists y_n)((P_n(y_n) \vee G_n) \wedge S_{n-1}^N)$$

THEOREM 4. *There exists an* **LK** *proof* π *of* $\vdash \mathrm{sk}(R_N)$ *such that* $|\pi| \leq k * N + c$ *for some constants* c, k.

PROOF. Let $N, n \in \mathbb{N}$ such that $N \geq n$. Let

$$\begin{aligned} s_n^N &= \quad f_{N-n}(y_N, y_{N-1}, \ldots, y_{n+1}) \\ \sigma_n^N &= \quad \{y_N \leftarrow s_N^N, y_{N-1} \leftarrow s_{N-1}^N \sigma_{N-1}^N, \ldots, y_{n+1} \leftarrow s_{n+1}^N \sigma_{n+1}^N\}. \end{aligned}$$

Observe that s_N^N is a Skolem constant, and that for all $0 < n < N$, $s_n^N \sigma_n^N$ is a closed term. Therefore the range of σ_n^N consists of closed terms and hence $\sigma_n^N \{y_n \leftarrow s_n^N \sigma_n^N\} = \sigma_{n-1}^N$.

We will construct **LK** proofs π of $\Gamma \vdash \Delta, S_n^N \sigma_n^N$ for all $N \geq n$ and multisets of formulas Γ, Δ, such that $|\pi| \leq k * n + c$, by induction on n. For reasons of clarity, we will (mostly) not write down the contexts Γ, Δ explicitly — they are only needed because our calculus does not have rules for weakening.

1. $n = 0$. Observe that $S_0^0 = G_0 \to G_0 = S_0^0 \sigma$ for all substitutions σ. Take as π

$$\frac{G_0 \vdash G_0}{\vdash G_0 \to G_0} \to_r$$

   and note that $|\pi| = 2$.
2. $n > 0, N > 0$. Let π be

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P_n(s_n^N\sigma_n^N) \vdash \Delta, P_n(s_n^N\sigma_n^N) \qquad G_n \vdash \Delta, G_n}{P_n(s_n^N\sigma_n^N) \vee G_n \vdash \Delta, P_n(s_n^N\sigma_n^N), G_n}\,\vee_l}{P_n(s_n^N\sigma_n^N) \vee G_n \vdash \Delta, (P_n(y_n) \vee G_n)\sigma_{n-1}^N}\,\vee_r \qquad \begin{array}{c}(\pi_{(IH)})\\ \Gamma \vdash \Delta, S_{n-1}^N\sigma_{n-1}^N\end{array}}{P_n(s_n^N\sigma_n^N) \vee G_n \vdash \Delta, ((P_n(y_n) \vee G_n) \wedge S_{n-1}^N)\sigma_n^N\{y_n \leftarrow s_n^N\sigma_n^N\}}\,\wedge_r^c}{P_n(s_n^N\sigma_n^N) \vee G_n \vdash ((\exists y_n)((P_n(y_n) \vee G_n) \wedge S_{n-1}^N))\sigma_n^N}\,\exists_r}{\vdash ((P_n(s_n^N) \vee G_n) \to (\exists y_n)((P_n(y_n) \vee G_n) \wedge S_{n-1}^N))\sigma_n^N}\,\to_r$$

where $\pi_{(IH)}$ is a proof of $\Gamma \vdash \Delta, S_{n-1}^N\sigma_{n-1}^N$ such that $|\pi_{(IH)}| \leq k*(n-1)+c$ obtained by applying the induction hypothesis. Then for some constant $l \leq k$,

$$|\pi| = l + |\pi_{(IH)}| \leq l + k(n-1) + c \leq kn + c.$$

⊣

In the above lower bound, the assumption of working in a cut-free setting is necessary.

Proposition 4. *There are proofs π_N with cuts of $\vdash R_N$ s.t. $|\pi_N| = k*N+c$ for some constants k, c.*

Proof. The sequents

$$(\exists x_N)P_N(x_N) \vee G_N \vdash (\exists z_N)(P_N(z_N) \vee G_N)$$

have constant-length proofs ψ_N. Let π_0 be

$$\dfrac{G_0 \vdash G_0}{\vdash G_0 \to G_0}\,\to_l$$

and π_N for $N > 0$ be

$$\dfrac{\dfrac{\psi_N \qquad \begin{array}{c}\vdots\\ (\exists z_N)(P_N(z_N) \vee G_N) \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})\end{array}}{(\exists x_N)P_N(x_N) \vee G_N \vdash (\exists y_N)((P_N(y_N) \vee G_N) \wedge R_{N-1})}\,\mathrm{cut}}{\vdash R_N}\,\to_r$$

⊣

§5. *sm*-Skolemization.

In this section, we consider an alternative Skolemization that, even in the cut-free case, does not have an elementary elimination of Skolem symbols. This optimized version *sm*-Skolemization of structural Skolemization allows minimization of quantifier scope. This is analogous to the δ^+ rule for free variable semantic tableaux introduced in [7].

Definition 12. We define a rewrite relation $\to_{sm}$ on formulas that "pushes quantifiers down":

$$(\forall x)\neg F \to_{sm} \neg(\exists x)F,$$
$$(\forall x)(F \vee G) \to_{sm} (\forall x)F \vee G, \quad (\forall x)(G \vee F) \to_{sm} G \vee (\forall x)F$$

provided that x is not free in G, and so on for the other cases and connectives. If $F \to_{sm}^* G$ then $\mathrm{sk}(G)$ is an *sm-Skolemization* of F. This definition is extended to sequents in the obvious way.

Clearly, in general sm-Skolemization creates smaller Skolem terms than structural Skolemization. Using results from [2], we show that there may be a non-elementary difference in cut-free proof complexity between a formula and its sm-Skolemization. For this purpose, we define the functions e, s by $e(0,k) = k, e(n+1,k) = 2^{e(n,k)}, s(n) = e(n,1)$.

Theorem 5. *There exist sequences of sequents S_n, M_n and constants c, d such that for all n*

1. *M_n is an sm-Skolemization of S_n, and*
2. *there exists a cut-free proof π_n of M_n s.t. $|\pi_n| \leq e(c,n)$ (i. e. elementary), and*
3. *for all cut-free proofs π_n of S_n, $|\pi_n| \geq s(n-d)$ (i. e. non-elementary).*

Proof. Consider the sequence of sequents T_n Statman uses to show the non-elementary complexity of cut-elimination in [10]. Statman constructs short proofs with cut π_n of T_n. Consider the end-sequent T'_n of $\check{\pi_n}^T$ where T is the set of eigenvariables of π_n. We take $\mathrm{sk}(T'_n)$ for M_n. For S_n we take a certain "bad prenexification" of T'_n, constructed as the witness for e) in Theorem 4.1 in [2]. Since S_n is a prenexification of T'_n, $S_n \rightarrow^*_{sm} T'_n$, which shows 1. Further, 2. follows from d), and 3. follows from e) and c)[1] of the aformentioned Theorem. The bounds there are stated in terms of the Herbrand complexity $\mathrm{HC}(S)$, which is the number of formulas of a minimal Herbrand sequent of S. But since we can (using the techniques described in this paper) go from Herbrand sequents to proofs and back with at most exponential expense, we get the desired bounds. $\dashv$

§6. Conclusion.

We would like to stress that the complexity considerations in this paper do not depend so much on Skolemization per se but rather on the rigidity of the eigenvariable conditions and the form of the proof. The eigenvariable conditions can be more relaxed, e.g. for sequent calculus variants of Hilbert's ε-calculus or a sequent calculus that uses Henkin constants instead of eigenvariables. The length of cut-free proofs in such calculi corresponds to that of skolemized cut-free proofs which allows to repeat the complexity results of this paper. In case the format of the proof is changed from tree-like to dag-like the questions remain open.

The question about the complexity of deskolemization of proofs with cuts in the general case is left open. Among the main obstacles seems to be the difficulty of proving lower bounds for proofs with cuts. Another open question posed in the cut-free and general case is the complexity of deskolemization in presence of identity axioms for the Skolem functions. This question is interesting because it is connected to an assymmetry between model-theoretic and proof-theoretic Skolemization. In model theory identity axioms for Skolem functions are always assumed as one intends to work algebraically in the open extension. In proof theory already existing proofs are skolemized and therefore identity axioms for Skolem functions are never used.

Acknowledgements. The authors would like to thank Bruno Woltzenlogel Paleo for insightful comments on an early draft of this paper.

[1] c) is Statman's result.

REFERENCES

[1] Jeremy Avigad, *Eliminating definitions and skolem functions in first-order logic*, ***ACM Transactions on Computational Logic***, vol. 4 (2003), no. 3, pp. 402–415.

[2] Matthias Baaz and Alexander Leitsch, *Skolemization and proof complexity*, ***Fundamenta Informaticae***, vol. 20 (1994), no. 4, pp. 353–379.

[3] ———, *Cut normal forms and proof complexity*, ***Annals of Pure and Applied Logic***, vol. 97 (1999), pp. 127–177.

[4] Matthias Baaz and Alexander Leitsch, *Cut-elimination and redundancy-elimination by resolution*, ***Journal of Symbolic Computation***, vol. 29 (2000), no. 2, pp. 149–176.

[5] Peter Clote and Jan Krajíček, *Open problems*, ***Arithmetic, proof theory and computational complexity*** (Peter Clote and Jan Krajíček, editors), Oxford University Press, 1993, pp. 1–19.

[6] Gerhard Gentzen, *Untersuchungen über das logische Schließen II*, ***Mathematische Zeitschrift***, vol. 39 (1935), no. 1, pp. 405–431.

[7] Reiner Hähnle and Peter H. Schmitt, *The liberalized δ-rule in free variable semantic tableaux*, ***Journal of Automated Reasoning***, vol. 13 (1994), no. 2, pp. 211–221.

[8] David Hilbert and Paul Bernays, ***Grundlagen der Mathematik II***, 2nd ed., Springer, 1970.

[9] Dale Miller, *A compact representation of proofs*, ***Studia Logica***, vol. 46 (1987), no. 4, pp. 347–370.

[10] Richard Statman, *Lower bounds on Herbrand's theorem*, ***Proceedings of the American Mathematical Society***, vol. 75 (1979), pp. 104–107.

[11] A. S. Troelstra and H. Schwichtenberg, ***Basic proof theory***, second ed., Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, 2000.

INSTITUTE OF DISCRETE MATHEMATICS AND GEOMETRY (E104)
VIENNA UNIVERSITY OF TECHNOLOGY
WIEDNER HAUPTSTRAßE 8-10, 1040 VIENNA, AUSTRIA
E-mail: baaz@logic.at

LABORATOIRE PREUVES, PROGRAMMES ET SYSTÈMES (PPS)
UNIVERSITÉ PARIS DIDEROT – PARIS 7
175 RUE DU CHEVALERET, 75013 PARIS, FRANCE
E-mail: stefan.hetzl@pps.jussieu.fr

INSTITUTE OF COMPUTER LANGUAGES (E185)
VIENNA UNIVERSITY OF TECHNOLOGY
FAVORITENSTRAßE 9, 1040 VIENNA, AUSTRIA
E-mail: weller@logic.at