Arch. Math. Logic (1988) 27: 69–84

Archive for
Mathematical
Logic

The Number of Proof Lines and the Size of Proofs in First Order Logic

Jan Krajíček and Pavel Pudlák

Mathematical Institute, ČSAV, Prague, Žitná 25, 11567, Czechoslovakia

There are two basic ways of measuring the complexity (or length) of proofs:

(1) to count the number of proof lines,

(2) to count the total size of the proof (i.e. to count each symbol). Trivially the size is an upper bound to the number of proof lines. It is much more difficult to bound the size using the number of proof lines. If we consider logic without function symbols a reasonable bound can be proved (see Proposition 3.4). If function symbols are allowed, then the situation is considerably more complicated. In such a case formulas in the proof may contain large terms and it is difficult to find some bounds to the size of these terms using only the information about the number of proof lines. There are still important open problems here which show that the role of terms in the first order logic is not quite well understood.

Some papers about this subject are rather difficult to read, one reason being that they consider general classes of logical calculi. Therefore we decided to consider just one particular calculus, Gentzen's well-known calculus *LK* as presented in [T]. Our results generalize trivially to theories given by a finite set of axioms in *LK*, in particular to LK_e, the calculus *LK* with equality. On the other hand, theories axiomatized by schemata, such as Peano arithmetic, require a different approach.

As mentioned above, our presentation of the results uses the particular formulation of *LK* defined in [T], namely, we use also two different kinds of variables, free and bound, and we assume that terms contain only free variables while semiterms may contain both free and bound ones (cf. [T], p. 6 and p. 35). This distinction is not essential but is useful. The *size* of a formula or a semiterm will be the number of symbols in it. The size of a sequent is the sum of the sizes of formulas in the sequent. Semiterms and formulas in *LK* can be represented as labelled trees. The depth of a semiterm t denoted by $dp(t)$ will be the length of the longest path in the tree corresponding to t.

A proof in *LK* is a particular rooted tree labelled by sequents. The *size of the proof* is the sum of the sizes of the sequents in the proof. The *number of proof lines of the proof* is the number of vertices of the tree. The size of a semiterm or formula or sequent or proof X will be denoted by $|X|$.

The main question that we want to address here is the following. Suppose a sequent $\Gamma \to \Delta$ of size m has a proof with k proof lines in LK. How can we bound the minimal size of a proof of $\Gamma \to \Delta$ in LK using k and m? We think that this is a good test question showing how well (or how poorly) we understand the structure of first order proofs. If the sequent has a *cut-free* proof with k proof lines, then we have an upper bound which is exponential in $k+m$. In general, we have only primitive recursive bound in $k+m$, since we use the cut-elimination theorem. It is an open problem if there is an elementary recursive bound (i.e. a fixed times iterated exponential).

The results are based on a reduction to the unification problem. This reduction is implicit in Parikh's paper [Pa] and was later developed by Farmer [F1, F2]. In the case of cut-free proofs in LK the reduction is very simple which allows us to obtain quite a good bound. The bound is based on an estimate to the depth of a most general unifier proved in Sect. 2.

A similar reduction procedure for proofs with cuts produces only a so called second order unification problem (a general system of equations with free variables for unknown terms). This problem has been shown undecidable [G]. We shall use this fact to show that the problem whether a given sequent $\Gamma \to \Delta$ has a proof with a given proof skeleton (see Sect. 2 for the definition) is undecidable. A result of this type has been announced by Orevkov in [O1] and sketched in [O3]. This shows that in order to obtain a proof of $\Gamma \to \Delta$ of small size from a proof of $\Gamma \to \Delta$ with few proof lines we must in general change the structure, we cannot just replace the terms in the proof by shorter ones. Motivated by a well-known conjecture of Kreisel we prove these results for systems in which there is only one term parameter which has the form $S^n(0)$, $n < \omega$, where S is a unary function symbol.

A related problem has been studied by Farmer [F1, F2]: given k and a formula or a sequent, is it decidable whether it has a proof with k proof lines? In particular he has shown that for cut-free proofs in LK it is decidable. (This follows from the reduction to the unification.) For general proofs in LK it is still open.

The most famous problem in this area is the so called *Kreisel's conjecture* mentioned already above: "Suppose that for some $A(a)$ and $k < \omega$, Peano arithmetic proves every $A(S^n(0))$ by a proof with $\leq k$ proof lines. Then it also proves $\forall x A(x)$".

We could not resist to add at least some simple observations about this conjecture in Sect. 6. A full proof of this conjecture has been announced by M. Baaz.

We assume that the reader is familiar with the system LK as defined in [T]. Throughout the paper "proof", "provable" etc. refers always to this system.

1. Bounds to the Unification

Let Term_L^A be the set of terms with variables from the set A and function symbols from the set L. A *substitution* is a mapping

$$\sigma : A \to \mathrm{Term}_L^A .$$

Given a term t and substitution σ, $\sigma(t)$ is the term obtained from t by substitution σ i.e.

$$\sigma(t) = t(a_1/\sigma(a_1), \ldots, a_m/\sigma(a_m))$$

where t does not contain variables other than $a_1, \dots, a_m$ and we substitute for *all* occurrences of the corresponding variables.

The *unification problem* is to find a substitution σ for a given system U of pairs of terms $(t_1, s_1), \dots, (t_k, s_k)$ such that, for all $i = 1, \dots, k$, $\sigma(t_i) = \sigma(s_i)$. σ is called a *unifier* for $(t_1, s_1), \dots, (t_k, s_k)$. The unification problem arose in connection with the resolution principle. Therefore it is not surprising that other problems in proof theory can be reduced to it. Such reductions were constructed in [F1, F2]. In the next section we shall reduce the problem of finding a proof of a sequent $\Gamma \to \Delta$ with a given skeleton S (defined in Sect. 3) to the unification problem. For this purpose it is not sufficient to have any unifier, since a proof poses some restrictions to the variables occurring in terms. An approach to this problem is based on the concept of a *most general unifier*. Another approach based on trees instead of terms was used in [K1], Sect. 2.

A *most general unifier* for a system U is a unifier σ_0 such that any unifier σ for U can be decomposed into $\sigma = \sigma_1 \sigma_0$ for some substitution σ_1.

The *restrictions* will be of the following type:

(*) for a pair (a, c), a a variable, and c a constant, $\sigma(a)$ must not contain the constant c.

Lemma 1.1. *If there exists a unifier for U which satisfies a set of conditions of type* (*), *then any most general unifier for U satisfies the conditions too.*

Proof – trivial. □

There is a well-known and simple algorithm for finding a most general unifier, see [C–L], p. 77. Using properties of this algorithm we derive bounds to the depth of a most general unifier. We shall use these bounds to derive relations between the number of proof lines and the size of a proof. Part (i) of the next lemma is equivalent to a lemma of [K1], Sect. 2.

Lemma 1.2. *Let U be a system of pairs of terms, let S be the set of terms s_i and t_i occurring in U, let v be the number of different variables occurring in U. Then each most general unifier σ for U satisfies the following inequalities*

(i) $$\max_{t \in S} \mathrm{dp}(\sigma(t)) \leqq \sum_{t \in S} |t|;$$

(ii) $$\max_{t \in S} \mathrm{dp}(\sigma(t)) \leqq (v+1) \cdot \max_{t \in S} \mathrm{dp}(t).$$

Proof. The unification algorithm produces sets of terms $S_0, S_1, \dots, S_k$ such that

(1) $S_0 = S$, $S_k = \{\sigma(t) \mid t \in S\}$, where σ is a most general unifier;

(2) $S_{i+1} = \{t(a/s) \mid t \in S_i\}$, where s is a subterm of some term in S_i and s does not contain the variable a. Since each most general unifier can be obtained from σ by permuting variables, it is sufficient to consider just σ produced by the algorithm. For each $i = 0, \dots, k$, $t \in S_i$ we label the tree $T(t)$ as follows. The labelled tree will be denoted by $\bar{T}(t)$. For $i = 0$ and a vertex w of $T(t)$, the label of w will be the subterm of t corresponding to the vertex w. Thus for instance the leaves of $T(t)$, $t \in S_0$ are labelled by variables and constants. For $t' \in S_{i+1}$, $t' = t(a/s)$ as in (2) above, the vertices of $T(t')$ which correspond to $T(t)$ will have the same labels as in $\bar{T}(t)$, the vertices which correspond to $T(s)$ will have the same labels as in $\bar{T}(s)$, except for the vertices which correspond to the root of $\bar{T}(s)$ [since they have labels from $\bar{T}(t)$].

Claim 1. If $u \neq w$ are on a path from the root to a leave in $\bar{T}(t)$, $t \in S_i$, $0 \leqq i \leqq k$, then they have different labels.

This is a corollary of a stronger Claim 2 which follows easily from the property (2) using induction over i.

Claim 2. Suppose that a vertex u of $\bar{T}(t)$ and vertex w of $\bar{T}(s)$ have the same label, $s, t \in S_i$, $0 \leqq i \leqq k$. Then u and w determine isomorphic labelled subtrees of $\bar{T}(t)$ and $\bar{T}(s)$.

To prove the inequalities consider a maximal path p in some $\bar{T}(t)$, $t \in S_k$. Since there are $\leqq \sum_{t \in S} |t|$ labels and by Claim 1, the length of p is less than or equal to $\sum_{t \in S} |t|$, which proves (i). By the construction of $\bar{T}(t)$, p can be decomposed into paths isomorphic to paths in the trees $\bar{T}(s)$, $s \in S$, each path, except possibly for the last one, ending with a vertex labelled by a variable. For different paths the variables must be different, thus we obtain (ii). □

Remark. The proof above gives in fact the following inequality $\max_{t \in S} \mathrm{dp}(\sigma(\mathrm{t}))$ $\leqq \mathrm{card}\{s \mid s$ a subterm of some $t \in S\}$, which is stronger than (i) if some term occurs more than once as a subterm of some $t \in S$.

2. The Size of Terms in Cut-Free Proofs

In general proofs with few proof lines may contain large terms. In this section we shall show that in cut-free proofs one can replace large terms by terms whose size is bounded where the bound depends only on the number of proof lines and the size of the sequent that we want to prove.

Following Farmer [F1, F2] we define a *proof skeleton* (or just a skeleton) as a rooted tree whose vertices are labelled by the inference rules of *LK*. Further, it is marked on the tree which son of a given vertex is the left one and which is the right one. For the exchange rule the label contains also the number of the pair to which it should be applied. The information which the skeleton *does not* contain are the terms and variables used in quantifier rules. Every proof determines uniquely its skeleton, but we do not require for a skeleton to be determined by some proof. A *cut-free skeleton* is a skeleton in which no vertex is labelled by the cut rule.

Let a cut-free skeleton S and a sequent $\Gamma \rightarrow \Delta$ be given. We want to find a proof of $\Gamma \rightarrow \Delta$ whose skeleton is S. We shall consider only regular proofs (cf. [T]) and show that in this case the problem can be reduced to a unification problem with the restriction of the type (*) of the preceding section (observe that for any proof P there is a regular proof P' of the same end-sequent as P which has the same skeleton as P). We shall divide the reduction procedure into two parts. First we shall show that if there is any proof of $\Gamma \rightarrow \Delta$ with skeleton S, then its logical structure (= everything except for semiterms) is uniquely determined. Then we construct the unification problem.

Let us call a *preproof* any structure which has all the properties of a proof except for the initial sequents which are only required to be of the following form

$$B(s_1, \ldots, s_\ell) \rightarrow B(t_1, \ldots, t_\ell), \quad \text{where} \quad s_1, \ldots, s_\ell, t_1, \ldots, t_\ell \tag{**}$$

are semiterms[1]. To construct a preproof from S and $\Gamma \to \Delta$ we proceed as follows:

(1) assign $\Gamma \to \Delta$ on the root of S,

(2) if a sequent has been assigned to a vertex v of S and v is not a leave, assign sequents to its sons according to the rule assigned to v; in case of the structural and propositional rules these sequents are uniquely determined; in case of the quantifier rules choose always a new free variable and substitute it for the bounded variable.

This procedure may not terminate with preproof sometimes. But clearly we have:

Claim 2.1. If there is a proof of $\Gamma \to \Delta$ with skeleton S, the procedure above constructs a preproof P_0 such that each regular proof P of $\Gamma \to \Delta$ with skeleton S can be obtained from P_0 by substituting suitable terms for the free variables introduced at the vertices labelled by $\forall$: left and $\exists$: right and by renaming the free variables. □

The unification problem U is constructed from a preproof P_0 as follows:

(1) We treat bounded variables, eigenvariables and free variables of $\Gamma \to \Delta$ as constants i.e. they cannot be substituted for;

(2) (t, s) is in U iff $t = t_i$, $s = s_i$, $i \leqq \ell$, for some initial sequent of P_0 of the form (**) above;

(3) for every free variable a introduced at some $\forall$: left or $\exists$: right vertex we require that any term $\sigma(a)$ substituted for a must not contain a bound variable, an eigenvariable of the proof or a free variable of $\Gamma \to \Delta$.

Because of (1), the restrictions of (3) are of the type (*) (see Sect. 1). Let A be the set of free variables introduced at $\forall$: left and $\exists$: right vertices. Let T be the set of all terms. Then using induction on the depth of P_0 one can prove:

Claim 2.2. For every $\sigma: A \to T$, σ is a solution to the unification problem U with the restrictions iff σ produces a regular proof from P_0. □

Now we can apply our bound to the depth of a most general unifier.

Theorem 2.3. *Suppose $\Gamma \to \Delta$ has a cut-free proof P with skeleton S. Let T be the set of maximal semiterms of $\Gamma \to \Delta$, let ℓ be the number of leaves of S and let q be the number of applications of the rules $\forall$: left and $\exists$: right. Then there exists a proof P' of $\Gamma \to \Delta$ with the same skeleton S such that the depth of each semiterm of P' is bounded above by*

(i) $$\ell \cdot \sum_{t \in T} |t| ;$$

(ii) $$(q+1) \cdot \max_{t \in T} \mathrm{dp}(t) .$$

Proof. The procedure above reduces the existence of a proof of $\Gamma \to \Delta$ with skeleton S to a unification problem with certain restrictions. Since there is a proof P of $\Gamma \to \Delta$ with skeleton S, the unification problem has a solution. The restrictions for the unifier are of the types considered in Lemma 1.1. Hence also a most general unifier

[1] The quantifiers of B may bound some variables inside of the semiterms

is a solution. As the semiterms of maximal depth in an LK proof are always in the initial sequents we can use our bounds for unification (Lemma 1.2).

(i) In the reduction procedure $\sum_{t\in T}|t|$ is a bound to the sum of the sizes of maximal semiterms assigned to any vertex of S, in particular to leaves. Since there are ℓ leaves, (i) in the theorem is an upper bound to the sum of sizes of the terms in the unification problem, hence, by Lemma 1.2 (i), also to the maximal depth of the unified terms.

(ii) The number of variables in the unification problem is q.

Again $\max_{t\in T}\mathrm{dp}(t)$ is an upper bound to the depth of any semiterm which appears in the reduction procedure. Thus (ii) follows from Lemma 1.2 (ii). □

Lemma 2.4. *Suppose a proof P has k proof lines. Then*

(1) *each sequent in P has at most $k+1$ formulas;*

(2) *P has at most $\binom{k+2}{2}-1$ formulas.*

Proof. The first part follows easily by induction. Let $f(k)$ be the maximal number of formulas in a proof with k proof lines. Then

$$f(1)=2$$

and by (1)

$$f(k+1)\leqq f(k)+k+2$$

whence (2) follows. □

Theorem 2.3 enables us to bound the size of a shortest cut-free proof of a sequent $\Gamma\to\Delta$ if we have a bound to the number of proof lines of some cut-free proof of $\Gamma\to\Delta$. The bounds are probably very crude.

Theorem 2.5. *Let m be the size of a sequent $\Gamma\to\Delta$ which has a cut-free proof P with k proof lines. Let c be the maximal arity of a function symbol in the sequent. Then there exists a proof P' of the sequent which has the same skeleton as P and its size can be bounded, for k, m sufficiently large, by*

$$\text{(i)}\qquad |P'|\leqq k^3m^2 \quad \text{if} \quad c\leqq 1,$$

$$\text{(ii)}\qquad |P'|\leqq c^{km} \quad \text{if} \quad c\geqq 2.$$

Proof. Since in LK each rule has at most two premises, the number of leaves of the skeleton of P is

$$\ell\leqq\frac{k+1}{2}.$$

By Theorem 2.3 (i) there is a proof P' of $\Gamma\to\Delta$ with the same skeleton which contains only semiterms whose depth is $\leqq m\cdot\ell$. Thus the maximal size r of a semiterm in P' is bounded by

$$r\leqq m\cdot\ell+1\leqq m\cdot\frac{k+1}{2}+1$$

if $c\leqq 1$ and by

$$r\leqq c^{m\ell}\leqq c^{m\cdot\frac{k+1}{2}}$$

otherwise. Using the subformula property of the cut-free proof P' we get that $m \cdot r$ is a bound to the maximal size of a formula in P'. Using the estimate to the number of formulas in P' (Lemma 2.4) and simple calculations we get (i) and (ii) of the theorem. □

We do not know how good the bounds are in the theorem above, since we lack lower bound techniques. So far we cannot rule out that e.g. P' can be constructed so that $|P'| = O(k \cdot m)$.

3. The Size of Proofs with Cuts

In Sect. 5 we shall prove that the problem whether a given sequent has a proof with a given skeleton is in general undecidable. Thus there is no recursive function $f(k, m)$ which bounds the size of the smallest proof of a sequent $\Gamma \rightarrow \Delta$, $|\Gamma \rightarrow \Delta| \leqq m$, with the skeleton S, $|S| \leqq k$, i.e. there is no reasonable analogue of Theorem 2.5 for general proofs. However, a primitive recursive bound can be shown, if one does not require that the skeleton is preserved. This is done by cut-elimination.

Define the *logical depth of a formula A* be the depth of A if A is considered as a term where

(1) atomic formulas are considered to be constants,

(2) $\wedge$, $\vee$, $\supset$ are considered to be binary function symbols, and $\neg$, $\exists x$, $\forall x$, for all bound variables, are considered to be unary function symbols.

Lemma 3.1 (cf. [Pa, F1, F2, K1]). *If a sequent $\Gamma \rightarrow \Delta$, $|\Gamma \rightarrow \Delta| = m$ has a proof P with k proof lines then $\Gamma \rightarrow \Delta$ has a proof P' with the same skeleton and such that P' contains only formulas of logical depth $m + O(k)$.*

Proof. Let P be given. We shall gradually replace formulas of P by propositional variables and at the same time construct a unification problem U. The variables of U will be the introduced propositional variables, the function symbols will be as in (2) above. For each initial sequent we introduce a new variable corresponding to both antecedent and succeedes of the sequent. For the weakening we add a new variable. For other structural rules we do not add new variables, but we add an equation for the contraction and for the cut. For logical rules we add a new variable for the principal formula of the rule in question and add an equation

$$f(a, b) = c \quad \text{or} \quad f(a) = c$$

where c is the variable corresponding to the principal formula, a, b are variables corresponding to auxiliary formulas and f is $\wedge$ or $\vee$ etc. Finally we add an equation

$$a = A$$

for each formula A of the sequent $\Gamma \rightarrow \Delta$ and the variable a corresponding to it and we treat the formulas of $\Gamma \rightarrow \Delta$ as constants in U. The proof P gives a solution to U. Thus we can apply Lemma 1.2 (i) and we obtain a proof P' where the logical depth of each formula is bounded by $m + O(k)$. This is not a proof in LK, since LK does not use propositional variables, but, of course, we can replace each propositional variable by an atomic formula which does not contain variables occurring in P. □

Since the cut-elimination is proved using induction over the logical depth of formulas used in cuts we obtain the following corollary, cf. [K1, O2].

Corollary 3.2. *If the sequent $\Gamma \to \Delta$, $|\Gamma \to \Delta| = m$ has a proof with k proof lines then $\Gamma \to \Delta$ has a cut-free proof with $2^0_{m+O(k)}$ proof lines.* □

Recall that 2^y_x is defined by

$$2^y_0 = y, \quad 2^y_{x+1} = 2^{2^y_x}.$$

Now our bound follows from Corollary 3.2 and Theorem 2.5 by a simple calculation.

Theorem 3.3. *Let m be the size of a sequent which has a proof with k proof lines. Then the sequent has also a proof with size $= 2^0_{O(k+m)}$.* □

It is an open problem whether the bound in Theorem 3.3 can be improved to a fixed time iterated exponential function (i.e. 2^{m+k}_c for some constant c). If such an improvement is possible, then it cannot be proved by cut-elimination as above, since the increase in the cut elimination cannot be bounded by such a function, cf. [St]. If the sequent does not contain function symbols at all, then an exponential bound follows directly from Lemma 3.1.

Proposition 3.4. *Let m be the size of a sequent $\Gamma \to \Delta$ which does not contain function symbols and which has a proof with k proof lines. Then the sequent has also a proof with size $2^{m+O(k)}$.*

Proof. Let P' be the proof of $\Gamma \to \Delta$ given by Lemma 3.1. Then each formula of P' has size $2^{m+O(k)}$, (since it does not contain function symbols either). By Lemma 2.4 (ii) there are $O(k^2)$ formulas in any proof with k proof lines. Thus the size of P' is

$$O(k^2) \cdot 2^{m+O(k)} = 2^{m+O(k)}. \quad \square$$

4. The Undecidability of the Second Order Unification Problem

Let L be a set of function symbols, $a_1, \ldots, a_m$ variables. Let $\underline{T} = (T, \mathrm{Sub}_1, \ldots, \mathrm{Sub}_m)$ be the algebra of terms where T is the set of terms in $L, a_1, \ldots, a_m$ and for $i = 1, \ldots, m$

$$\mathrm{Sub}_i(\delta, \sigma) := \delta(a_i/\sigma)$$

are substitutions as binary operations on T. *A second order unification problem* is a finite set of equations in the language $T \cup \{\mathrm{Sub}_1, \ldots, \mathrm{Sub}_m\}$ plus free variables for elements of T. The free variables will be called the *term variables*. By introducing new term variables we can transform any such system into an equivalent one where all equations have form

$$\delta(a_i/\sigma) = \varrho,$$

where δ, σ, ϱ are terms or term variables. The name "second order unification" is used since this problem can be considered as a generalization of the first order unification.

The existence of undecidable second order unifications has been proved by Goldfarb [G], (see also [F1, F2]). However, he uses in his construction parameters which are terms built from binary function symbols. We shall show that one can use, essentially, the ordinary numerals as parameters. This might be interesting because of the connection with Kreisel's length of proofs conjecture. Also our proof is simple.

Suppose a unary function symbol is chosen, say S. Then we call a *numeral* any term of the form $S^n(t)$, t a free variable or $t=0$, $n\in\omega$.

Theorem 4.1. *Let L contain a unary function symbol S, a constant 0 and a binary function symbol. Let τ_0 be a term variable. Then for every recursively enumerable set $X\subseteqq\omega$ there exists a second order unification problem Ω such that $\Omega\cup\{\tau_0=S^n(0)\}$ has a solution iff $n\in X$.*

Proof. As in [G] we shall use Matijasevič's theorem. It follows from this theorem that every r.e. set X can be defined by a formula

$$\exists y_1 \dots y_k\, D_X(x, y_l, \dots, y_k),$$

where D_X is a conjunction of formulas of the form

$$y_i=u,\ u<\omega$$

$$y_i=y_j+y_l,$$

$$y_i=y_j\cdot y_l$$

$$y_i=x,$$

$i,j,l\leqq k$. We shall simulate the variables $x, y_1 \dots y_k$ by numerals (defined above). This can be done easily using the following three claims where o denotes a binary symbol in L. We leave the details to the reader.

(1) The equation $s(\tau)=\tau(a/s(a))$, τ term variable, has solutions $\tau=S^n(a)$, $n\in\omega$.

(2) The equation $\tau(a/\sigma)=\varrho$ plus the equations from (1) for term variables τ,σ,ϱ have solutions:

$$S^p(a), S^q(a), S^m(a) \quad \text{for} \quad p+q=m.$$

(3) The equations

$$S(\sigma_1)=\sigma_1(a/S(a))$$

$$S(\sigma_2)=\sigma_2(a/S(a))$$

$$S(\sigma_3)=\sigma_3(b/S(b))$$

$$\tau(a/\sigma_1, b/S(b), c/a\circ(b\circ c))=\sigma_2\circ(\sigma_3\circ\tau)$$

with variables a,b,c and term variables $\sigma_1,\sigma_2,\sigma_3,\tau$ have solutions for $\sigma_1,\sigma_2,\sigma_3$ of the form

$$S^p(a), S^m(a), S^q(b) \quad \text{for} \quad p\cdot q=m.$$

The proof is nontrivial only for claim (3).

a) Assume $p \cdot q = m$. Then $S^p(a)$, $S^m(a)$, $S^q(b)$ and the following term are a solution for the equations above

$$S^{p(q-1)}(a) \circ (S^{q-1}(b) \circ (S^{p(q-2)}(a) \circ (S^{q-2}(b)$$
$$\circ (\ldots (S^p(a) \circ (S(b) \circ (a \circ (b \circ c) \ldots))))))).$$

b) Suppose $S^p(a)$, $S^m(a)$, $S^q(b)$, t are a solution.

We shall proceed by induction on the depth of t, denoted $\mathrm{dp}(t)$.

(i) $\mathrm{dp}(t) = 0$. Then t is c, hence σ_2 is a and σ_3 is b. Thus $p \cdot q = m = 0$.

(ii) $\mathrm{dp}(t) > 0$. Then t is $t_1 \circ t_2$ where

$$t_1(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = S^m(a)$$

i.e. $t_1 = S^{m-p}(a)$ and

$$t_2(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = S^q(b) \circ t.$$

Hence $\mathrm{dp}(t_2) > 0$, so $t_2 = t_3 \circ t_4$

$$t_3(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = S^q(b),$$

thus $t_3 = S^{q-1}(b)$. Further we have

$$t_4(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = t$$
$$= t_1 \circ (t_3 \circ t_4) = S^{m-p}(a) \circ (S^{q-1}(b) \circ t_4).$$

By the induction hypothesis, since $\mathrm{dp}(t_4) < \mathrm{dp}(t)$,

$$p \cdot (q-1) = m - p$$

i.e. $p \cdot q = m$. We have done. □

5. An Undecidable Proof Skeleton

In this section we shall show that there is no recursive procedure by which one can determine if a given sequent is provable in LK by a proof with a given skeleton. (For the definition of skeleton see Sect. 2.)

Theorem 5.1 (cf. Orevkov [O1, O3]). *Let L be a language containing a unary function symbol S, a constant 0 and a binary function symbol. Then for every recursively enumerable set $X \subseteq \omega$ there exist a sequent $A \to A$, $P(a)$ and a skeleton S such that $n \in X$ iff $A \to A$, $P(S^n(0))$ has an LK-proof with skeleton S.*

In order to make the description of the skeleton shorter we shall use *derived inference rules*. Such a rule is a binary relation R on pairs of sequents which satisfies the following property: For every $k, \ell \in \omega$, there exists a skeleton S in LK and a leaf ℓ_0 in S such that if $\Gamma \to \Delta$ and $\Pi \to \Lambda$ are in the relation R, k resp. ℓ is the number of formulas in Γ resp. in Δ, and we assign $\Gamma \to \Delta$ to ℓ_0, then

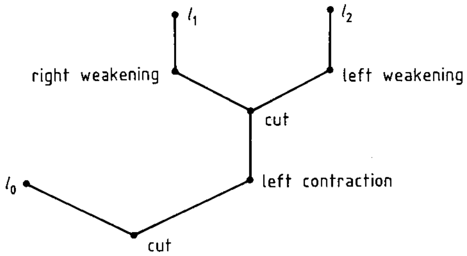
(1) we can find a correct assignment to the other vertices of S such that $\Pi \to \Lambda$ is on the root,

(2) any correct assignment has $\Pi \to \Lambda$ on the root.

This property enables us to transform any skeleton with derived inference rules into a skeleton in *LK*. (The dependence of *S* on the number of formulas in Γ and Δ is caused by the necessity of using exchange rules several times in order to obtain such a sequent.) We shall describe the rules using metavariables for formulas $A, B, \ldots$ and for sequents $\Gamma, \Delta, \ldots$ in the usual way. The following are derived inference rules for *LK*.

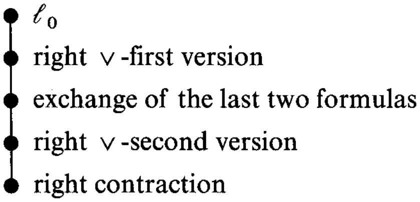
(1) doubling $\dfrac{\Gamma \to \Delta, B}{\Gamma \to \Delta, B, B}$.

Here is the skeleton for this rule:



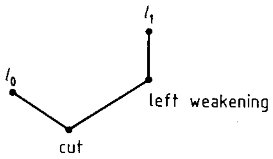
One can easily check that if we label ℓ_0 by $\Gamma \to \Delta, B, \ell_1$ by $C \to C$ and ℓ_2 by $D \to D$, then we can complete the labelling correctly iff $C = D = B$ in which case we obtain $\Gamma \to \Delta, B, B$ on the root.

(2) disjunction $\dfrac{\Gamma \to \Delta, B, C}{\Gamma \to \Delta, B \vee C}$ corresponding skeleton:


ℓ_0
right $\vee$-first version
exchange of the last two formulas
right $\vee$-second version
right contraction

(3) elimination $\dfrac{A \to A, \Gamma, B}{A \to A, \Gamma}$.

Using the following skeleton:



$A \to A, \Gamma, B$ is transformed into $A, C \to A, \Gamma, C$. Then using suitable exchanges and contracting A with C on both sides we obtain $A \to A, \Gamma$.

Proof of Theorem 5.1. Let $X \subsetneqq \omega$ be an r.e. set. Let Ω be the set of term equations (second order unification problem) such that $\Omega_n = \Omega \cup \{\tau_0 = S^n(0)\}$ has a solution iff $n \in X$ (Theorem 4.1). Let $s_1, \ldots, s_\ell$ be terms occurring in Ω and let $\tau_0, \ldots, \tau_k$ be term variables of Ω. Suppose $a_1, \ldots, a_m$ are the free variables used in Ω. Observe that if Ω_n has a solution in a language containing more free variables, then it has a solution in the language of Ω_n too, since the language of Ω_n contains a constant.

Let $P(a)$ be a formula with at least one occurrence of a and with no other semiterms than a.

Let B be the following formula:

$$P(a_1) \vee \ldots \vee P(a_m) \vee P(s_1) \vee \ldots \vee P(s_\ell)$$

[where always all occurrences of a in $P(a)$ are substituted for].

Let A be the sentence:

$$\exists x_1 \ldots \exists x_m B(a_1/x_1, \ldots, a_m/x_m).$$

Instead of defining skeleton S explicitely we shall describe a general shape of a proof of the sequent $A \rightarrow A, P(S^n(0))$ for $n \in X$. We shall show that the skeleton of such proofs can be extended to a proof of the sequent above iff Ω_n has a solution.

Let $n \in X$ and let $S^n(0) = t_0, t_1, \ldots, t_k$ be a solution of Ω_n. The proof will start with $B \rightarrow B$. Then we shall derive:

$$B \rightarrow B, P(S^n(0)), P(a_1), \ldots, P(a_m), P(s_1), \ldots, P(s_\ell), P(t_1), \ldots, P(t_k)$$

using several weakenings. The middle part of the skeleton will be arranged so that the form of this sequent is forced.

(1) First we shall show how the form of B is forced. At the end of the middle part of the skeleton we shall apply successively m rules left $\exists$ to the formula B. Otherwise we do not do anything with the occurrence of B in the antecedent. Any formula from which we can obtain A in this way must be just an alphabetical variant of B. As there are no free variables in the end-sequent we can assume w.l.o.g. that B is of the form above.

(2) The form of $P(S^n(0))$ is forced, since it will be preserved until the end-sequent.

(3) The form of $P(a_1), \ldots, P(a_m), P(s_1), \ldots, P(s_\ell)$ is easily forced as follows. Using the derived rule "doubling" we make replicas of these formulas. Then using the rule "disjunction" we construct a formula which should be equal to B. That it really is equal to B will be ensured by contracting it with B.

(4) It remains to show that the form of $P(t_1), \ldots, P(t_k)$ can be forced. First we show that we can force a formula to be of the form $P(t)$ (without any additional property of t). We make a replica of $P(a_1)$ and a replica of $P(t)$ (by the derived rule "doubling"), then we apply successively right $\exists$ to $P(a_1)$ and to $P(t)$ and contract the resulting two formulas. Since the form of $P(a_1)$ is forced (by A in the end-sequent), the contraction is possible iff $P(t)$ has such a form.

Finally we show that for $r, u, v \in \{s_1, \ldots, s_\ell, t_0, \ldots, t_k\}$ we can force

$$r(a_i/u) = v \qquad (*)$$

whenever this is prescribed in Ω_n. This will ensure that $t_0, \ldots, t_k$ is some solution.

Using "doubling" and "disjunction" [the derived rules (1) and (2)] derive in the succedent of the sequent formulas:

$$P(r) \vee P(a_i), P(v) \vee P(u). \qquad (**)$$

Then apply right $\exists$ to both formulas and contract them into one. If (*) holds this is possible since we can derive the same formula

$$\exists y(P(r(a_i/y)) \vee P(y)) \qquad (***)$$

from the formulas of (**). Now assume that for some r, v, u such a derivation is possible in which all occurrences of a_i are substituted by y in $P(r) \vee P(a_i)$ when applying right $\exists$ to it. Thus $P(r) \vee P(a_i)$ is transformed into (***). Hence also $P(v) \vee P(u)$ must be transformed to this form using right $\exists$. Thus the term which is replaced by a bound variable in $P(v) \vee P(u)$ must be u. Therefore v with some subterms u replaced by y must be equal to $r(a_i/y)$. But this is equivalent to (*). Thus we only need to show that the form of (***) can be forced. Let C be a formula obtained from $P(r) \vee P(a_i)$ after applying right $\exists$. Using "disjunction" we construct:

$$C \vee P(a_1) \vee \dots \vee P(a_{i-1}) \vee P(a_{i+1}) \vee \dots \vee P(a_m),$$

[from some replicas of $P(a_j)$'s obtained by "doubling"]. Then we apply $(m-1)$-times right $\exists$ to this formula. Let D be the resulting formula. This formula will be present in the sequent when we apply m-times the rule left $\exists$ to B. But this is possible only if D does not contain $a_1, \dots, a_m$. Then also C must not contain a_i, which means that it has the form (***).

The description of the skeleton is almost finished. We should only add that before applying left $\exists$ to the occurrence of B in the antecedent we have to apply m-times right $\exists$ to its occurrence in the succedent and eliminate $P(a_1), \dots, P(t_k)$ from the sequent using the derived rule (3) "elimination". Finally we eliminate also the other formulas which do not belong to the end-sequent (i.e. formulas such as D above). □

6. Generalizing Short Proofs with Large Terms

Georg Kreisel conjectured that for suitable systems a proof of a sentence containing large terms which has few proof lines can be transformed into a proof of a general statement. We shall be little more specific about this conjecture.

For systems related to those of [Pa] G. Kreisel conjectured (cf. the second edition of [T], footnote 3 on p. 402):

"For $A(x)$ and $c<\omega$ there are $M, N<\omega$ s.t. if d is a proof of $A(\underline{n})$ having $\leqq c$ proof lines and $n \geqq N$ then there are $m \leqq M$ and a derivation of a similar logical form to d that proves:

$$x \equiv n (\operatorname{mod} m) \supset A(x) ."$$

We shall call this new conjecture *Sharpened Kreisel's conjecture.*

As G. Kreisel observed the original conjecture follows easily from the new one. This is seen as follows.

Clearly it holds for any $n<\omega$ and any $m \leqq M$:

$$x \equiv n(\operatorname{mod} M!) \supset x \equiv n(\operatorname{mod} m) . \qquad (1)$$

Also trivially:

$$\bigvee_{i<M!} x \equiv (N+i)(\operatorname{mod} M!) . \qquad (2)$$

Assume that we have proofs of $A(\underline{0}), A(\underline{1}), A(\underline{2}), \ldots$ with $\leqq c$ proof lines. By Sharpened Kreisel's conjecture the proofs of $A(\underline{N+i})$, $i=0,1,2,\ldots,M!-1$, can be turned into proofs of:

$$x \equiv (N+i)(\mathrm{mod}\, m_i) \supset A(x), \tag{3}$$

for all $i \leqq (M!-1)$ and appropriate $m_i \leqq M$.

Combining (1), (2), (3) the wanted formula $\forall x A(x)$ follows.

The reduction to the unification that we have used in Sect. 2 can be applied to prove a theorem in this spirit. Since this application is straightforward we present it here, though our main concern in this paper was to investigate the relation of the number of proof lines to the size of proofs. The idea that unification can produce such result was communicated to us by M. Baaz. The methods of M. Baaz promise to be a deep insight into problems related to Sharpened Kreisel's conjecture.

Theorem 6.1. *Suppose $\Gamma \rightarrow \Delta, A(t)$ has a cut-free proof P with skeleton S. Let T be the set of maximal semiterms in $\Gamma \rightarrow \Delta, A(a)$, let ℓ be the number of leaves of S and let q be the number of applications of $\forall$: left and $\exists$: right. Then there exists a term s and a proof P' of $\Gamma \rightarrow \Delta$, $A(s)$ such that*

(1) *P' has the same skeleton as P;*

(2) *t can be obtained by a substitution from s,*

(3) *the depth of s satisfies the inequalities*

$$\mathrm{dp}(s) \leqq \ell \cdot \sum_{r \in T} |r| ;$$

$$\mathrm{dp}(s) \leqq (q+1) \cdot \max_{r \in T} \mathrm{dp}(r) .$$

Remarks. 1. If t does not satisfy the inequalities in (3) then s must contain a free variable, hence in this way one can obtain a proof of a general statement from a proof of a special case.

2. In the proof we shall show even more: any t' such that $\Gamma \rightarrow \Delta, A(t')$ has a proof with skeleton S can be obtained by a substitution from s.

3. The theorem is true also for proofs with cuts if we leave out condition (1), and increase (substantially) the bound in (3): This follows from the cut-elimination.

Proof. Extend P to a proof of $\Gamma \rightarrow \Delta$, $\exists x A(x)$ by adding one application of right $\exists$ rule. Then Theorem 2.3 gives us everything except for condition (2). This condition follows by observing that the terms of the constructed proof (in Theorem 2.3) are the terms of a most general unifier. □

Observe that Theorem 6.1 implies that Sharpened Kreisel's conjecture is true for a finite set of axioms. The next corollary follows also from a result of Miyatake [M] for A a little stronger.

Corollary 6.2. *Let A be a sentence such that*

$$A \rightarrow a=0 \vee a=S(0) \vee \ldots \vee a=S^{m-1}(0) \vee \exists x(a=S^m(x))$$

is provable in LK_e for every m. Suppose $B(a)$ is a formula and k a positive integer such that

$$A \rightarrow B(S^n(0))$$

is provable in LK_e using k proof lines for every n. Then $A \rightarrow \forall x\, B(x)$ is provable too.

Proof. By Theorem 3.2 we can assume w.l.o.g. that each $A \rightarrow B(S^n(0))$ has a *cut-free* proof with $\leqq k$ proof lines. Let $n > k \cdot |A \rightarrow B(a)|$. Then, by Theorem 6.1 there is a term s such that $\mathrm{dp}(s) < n$, $A \rightarrow B(s)$ is provable and $S^n(0)$ is a substitution instance of s. Thus s is $S^m(a)$ for some $m < n$ and a free variable a. Now a proof of $A \rightarrow \forall x\, B(x)$ can be constructed from the proofs of $A \rightarrow B(S^i(0))$, $i = 0, \ldots, m-1$ and the proof of $A \rightarrow B(S^m(a))$. □

As we have already pointed out, the situation is essentially different if we extend *LK* by axiom schemata. The following fact has been proved by Yukami [Y].

Fact 6.3. *There exists k such that, for all m, n, the sentence $S^n(0) + S^m(0) = S^{m+n}(0)$ has a proof in Peano arithmetic with $\leqq k$ proof lines.* □

It follows that, for the formula $A(a) := \exists y (a = y + y)$, there exists k such that each $A(S^{2n}(0))$ has a proof with $\leqq k$ proof lines in Peano arithmetic but $\forall x\, A(x)$ is obviously not provable. Hence in theories such as Peano arithmetic we cannot generalize short proofs with large terms in the manner of the preceding two theorems. However, observe that the proofs of the formula above does generalize in the sense of Sharpened Kreisel's conjecture.

(The reader interested in results obtained by various authors during the attempts to prove Kreisel's conjecture may consult a survey paper [K2].)

Acknowledgement. We thank to M. Baaz and to G. Kreisel for important suggestions.

References

[C–L] Chang, C.-L., Lee, R.C.-T.: Symbolic logic and mechanical theorem proving. New York and London: Academic Press 1973

[F1] Farmer, W.M.: Length of proofs and unification theory. Ph. D. thesis, Univ. of Wisconsin-Madison, 1984

[F2] Farmer, W.M.: A unification-theoretic method for investigating the *k*-provability problem, preprint, 1987

[G] Goldfarb, W.D.: The undecidability of the second-order unification problem. Theor. Comput. Sci. **13**, 225–230 (1981)

[K1] Krajıček, J.: On the number of steps in proofs, submitted to Ann. Pure Appl. Logic, 1985

[K2] Krajíček, J.: Generalizations of proofs, to appear in the Proc. 5th Easter Conf. on Model Th., Humboldt-Univ., Berlin (1987)

[M] Miyatake, T.: On the length of proofs in formal systems. Tsukuba J. Math. **4**, 115–125 (1980)

[O1] Orevkov, V.P.: Reconstitution of the proof from its scheme (Russian abstract), 8th Sov. Conf. Math. Log., Novosibirsk 1984, p. 133

[O2] Orevkov, V.P.: Upper bounds for lengthening of proofs after cut-elimination (Russian). In: Theor. compl. of Comp., ser. Notes of Sci. sem. of Leningrad dept. of Math. Inst. Acad. Sci. **137**, pp. 87–98, Leningrad (1984)

[O3] Orevkov, V.P.: Reconstruction of a proof by its analysis (Russian). Doklady Akad. Nauk **293** (2), 313–316 (1987)

[Pa] Parikh, R.: Some results on the length of proofs. TAMS **177**, 29–36 (1973)

[Si] Siekman, J.: Universal unification. In: Shostuk, R.E. (ed.), 7th Int. Conf. on Autom. Deduct., LN in Comp. Sci., No. 170, pp. 1–42. Berlin: Springer 1984

[St] Statman, R.: Bounds for proof-search and speed-up in the predicate calculus. Ann. Math. Logic **15**, 225–287 (1978)

[T] Takeuti, G.: Proof theory. North-Holland 1975

[Y] Yukami, T.: Some results on speed-up. Ann. Jap. Assoc. Philos. Sci., Vol. **6**, 195–205 (1984)

Received April 24, 1987/Revised July 22, 1987