The Undecidability of k-Provability

Samuel R. Buss*
Department of Mathematics
University of California, San Diego

April 3, 1989
Slightly revised December 4, 1990

Abstract

The k-provability problem is, given a first order formula ϕ and an integer k, to determine if ϕ has a proof consisting of k or fewer lines (i.e., formulas or sequents). This paper shows that the k-provability problem for the sequent calculus is undecidable. Indeed, for every r.e. set X there is a formula $\phi(x)$ and an integer k such that for all n, $\phi(S^n 0)$ has a proof of $\leq k$ sequents if and only if $n \in X$.

1 Introduction

The concept of the length of a proof is important because it provides a measure of the difficulty of proving a given theorem in a given formal system. There are two common ways to measure the length of a proof; namely, to count the number of formulas or inferences in the proof or to count the number of symbols appearing in the proof. It is important to note that knowing the number of formulas in a proof does not give a bound on the number of symbols since the formulas may be very long; in particular, the terms used in the proof could be large. For this paper, the length of a proof will be defined to be the number of distinct lines in the proof, where a line is either a formula

*Supported in part by NSF Grant DMS-8701828.

or, in the sequent calculus, a sequent. The *k-provability* problem for a first order theory is, given a formula A and an integer k, to determine if A has a proof with k or fewer lines.

The motivations for this paper arose out of work on Kreisel's conjecture [7] that if Peano arithmetic PA proves $A(S^n 0)$ with a proof of $\leq k$ formulas for all n then PA proves $(\forall x)A(x)$.[†] Parikh [11] showed that this is true for a variant PA^* of PA where addition and multiplication are three-place relations. He did this by first showing that if A is a formula and $k \in N$ then there is an a priori bound ℓ such that if A has a proof of $\leq k$ lines then it has a proof of $\leq k$ lines in which each formula contains $\leq \ell$ logical connectives — the bound ℓ is a function of k and the logical complexity of A. Hence when searching for a proof of length $\leq k$ we can control the logical complexity of the formulas appearing in the proof; however, the terms appearing in the proof might be arbitrarily complicated. For his result on PA^*, Parikh then exploited the fact that PA^* has only one (unary) function symbol to show that the k-provability problem for PA^* is definable in Presburger arithmetic and decidable.

A *proof analysis* is a partial description of a proof which describes the proof as a directed acyclic graph with a node for each formula (or sequent) in the proof. Each node is labelled with the rule of inference or axiom scheme which is used to derive the corresponding formula; incoming edges are ordered to specify which nodes represent which hypothesis of the inference. In short, a proof analysis specifies everything about the proof except the actual formulas in the proof. Every proof clearly has a proof analysis, but not all proof analyses correspond to proofs. Since first order systems typically have only a finite number of axiom schemes and rules of inference, there are, for fixed k, only finitely many possible proof analyses for proofs of length k. Hence the k-provability problem can be reduced to the problem of, given a formula A and a proof analyis, determining if A has a proof with that proof analysis.

Farmer [2, 1] showed that if the substitution axiom is modified then the k-provability problem for PA is decidable; he emphasized the fact that finding the terms to flesh out a proof analysis is a version of second-order unification. Second order unification was shown to be undecidable by Goldfarb [4].

[†]It is not clear to this author whether Professor Kreisel ever conjectured this or merely posed it as a problem. At any rate, Kreisel's conjecture was the original motivation for all the work outlined in this introduction.

Krajíček and Pudlák [6] showed that for the sequent calculus LK it is undecidable whether a given formula has a proof with a given proof analysis. Orevkov had earlier proved a similar result [10]. Other work related to Kreisel's conjecture has been done by Richardson [12], Miyatake [8, 9] and Yukami [14, 15]; see Krajíček [5] for a more complete survey. M. Baaz has recently announced a proof of Kreisel's conjecture.

The main result of this paper is:

Main Theorem 1 *Let LK be Gentzen's sequent calculus with a unary function symbol S, a binary function symbol and infinitely many binary relation symbols. For every recursively enumerable set X there is a formula $A(x)$ and an integer k such that for all n, $n \in X$ if and only if $\longrightarrow A(S^n 0)$ has an LK-proof with $\leq k$ distinct sequents.*

Hence the k-provability problem is undecidable for LK. The main theorem also holds for LK_e, i.e., for LK augmented with equality axioms. It is permissable for there to be additional function and predicate symbols besides the ones required in the hypothesis of the main theorem. The hypothesis that there be infinitely many binary relation symbols can be weakened to require only some bounded number of binary relation symbols; the precise number required depends on the size of a diophantine equation which defines an r.e. complete set.

There are of course many ways to formalize first order logic other than the sequent calculus. Unfortunately, our proof does not seem to apply immediately to all usual first order logics; however, our technique could probably be adapted to a lot of other specific first order logics. It would be desirable to improve our methods in this paper to be readily applicable to a wide range of formalizations of first order logic.

M. Baaz has announced an approach towards proving Kreisel's conjecture; but the details have not been fully worked out yet. Baaz's method avoids the undecidability of k-provability for the Gentzen sequent calculus firstly by translating proofs into a Hilbert-style ϵ-calculus and secondly by circumventing the need to solve the k-decidablity problem for the ϵ-calculus.

In section 2 below we introduce a variant of second-order unification and show that it is undecidable. In section 3 we review the sequent calculus and develop a tool called the "logical flow graph" for analyzing sequent proofs. In section 4 we prove the Main Theorem.

I wish to thank J. Krajíček and M. L. Bonet for suggesting improvements to a preliminary version of this paper and G. Kreisel for useful comments on an earlier version of this introduction.

2 Undecidability of Second Order Unification with Partial Substitution

Goldfarb [4] proved that second-order unification is undecidable; see Krajíček-Pudlák [6] for a simplified proof. We show here what a variant of second-order unification which allows partial substitution is also undecidable.

First some notation: $a, b, c, \ldots$, possibly with subscripts, are first-order variables (not metavariables); S is a unary function symbol and $\circ$ is a binary function symbol; both S and $\circ$ act on first-order objects. Other function symbols may be present and will not affect the results. The usual conventions on parentheses and term formation apply; we will usually omit parentheses and it is understood that $\circ$ associates from right to left. Symbols $r, s, t, \ldots$ will be used to denote first-order terms. Greek letters α, β, γ will be second-order variables which will range over first-order terms. Finally, the symbols ρ, σ, τ will be used to denote second-order terms built from S, $\circ$ and first- and second-order variables. Note that $a, b, c, S, \circ, \alpha, \beta, \gamma$ are symbols of a formal language whereas $r, s, t, \rho, \sigma, \gamma$ are metasymbols. For $k \geq 0$, we write $S^k\rho$ to denote the term consisting of S applied k times to ρ; e.g., S^3a is $SSSa$.

If r and s are first-order terms we write $r(s/a)$ to denote the result of replacing every occurence of a in r by the term s. Similarly, $r(s_1/a_1, s_2/a_2)$ denotes the simultaneous substitution of s_1 and s_2 for a_1 and a_2. Note that this is not in general the same as $r(s_1/a_1)(s_2/a_2)$ if a_2 occurs in s_1. A *second-order unification problem* is a finite set of equations

$$\beta_{i_j}(\rho_j/a_{i_j}) = \sigma_j$$

for $j = 1, \ldots, m$. Recall that a_{i_j} and β_{i_j} are specific first- and second-order variables and ρ_j and and σ_j are metavariables for second-order terms. A solution to the second-order unification problem is an assignment of first-order terms to second-order variables such that, when all the second-order variables are replaced by their assigned terms, the equalities become true. For example,

the unification problem consisting of the two equations $\beta(a \circ b/a) = \gamma \circ b$ and $\gamma(Sa/a) = S\gamma$ has as unique solution $\gamma = a$ and $\beta = a$.

We shall write $r(s/\!\!/a)$ to denote the result of a partial substitution of s for a in r. Actually, $r(s/\!\!/a)$ by itself is not uniquely defined and represents one of a finitely many possible terms; we shall use this notation only in an equation of the form

$$r(s/\!\!/a) = t.$$

Such an equation is true if and only if t can be obtained by replacing some (perhaps all or none) of the a's in r by s. A *second-order unification problem with partial substitution* is a finite set of equations of the form

$$\beta_{i_j}(\rho_j/\!\!/a_{i_j}) = \sigma_j$$

for $j = 1, \ldots, m$ and a solution to this system of equations is an assignment of first-order terms to second-order variables that makes all of the equations true. For example, $\beta(a \circ b/\!\!/a) = \gamma \circ b$ and $\gamma(Sa/\!\!/a) = S\gamma$ has an infinite number of solutions: (1) $\beta = \gamma = a$ and (2) $\gamma = S^k a$ and $\beta = (S^k a) \circ b$ for $k = 0, 1, 2, \ldots$. To see this, note that the only solutions to the second equation are $\gamma = S^k a$ for $k \geq 0$.

Theorem 2 *The second-order unification problem with partial substitution is undecidable.*

In [4] and [6] second-order unification (without partial substitution) is shown undecidable by use of Matijacevič's theorem; we shall use a similar technique to prove Theorem 2. In order to express the solvability of a diophantine equation as a second-order unification problem with partial substitution, we need to have a representation for integers and a way to force the correctness of addition and multiplication. A term of the form $S^k a$ will represent the nonnegative integer k. The following equation can be used to guarantee that β represents an integer:

(1) $\beta(Sa/\!\!/a) = S\beta$

The only solutions to (1) are $\beta = S^k a$ for $k \geq 0$. To prove this note that either $\beta = a$ or $\beta = S\beta_1$ where β_1 is a solution to $\beta_1(Sa/\!\!/a) = S\beta_1$. Arguing inductively shows $\beta = S^k a$ for some $k \geq 0$.

To express addition we need a set of equations whose only solutions are $\beta_1 = S^{k_1} a$, $\beta_2 = S^{k_2} a$, $\beta_3 = S^{k_1+k_2} a$. This is accomplished by:

$$
\begin{array}{lll}
(2) \quad i) & \beta_j(Sa/\!\!/a) = S\beta_j, & j = 1,2,3 \\
ii) & \beta_1(\beta_2/\!\!/a) = \beta_3 & \\
iii) & \beta_1(S\beta_2/\!\!/a) = S\beta_3 &
\end{array}
$$

By $(2.i)$, $\beta_j = S^{k_j}a$ for $j = 1,2,3$. By $(2.ii)$, depending on whether the substitution is performed, either $k_3 = k_1 + k_2$ or $k_3 = k_1$. By $(2.iii)$, either $k_3 = k_1 + k_2$ or $k_3 + 1 = k_1$. Hence, $k_3 = k_1 + k_2$.

Multiplication is more complicated. Consider the following set of equations:

$$
\begin{array}{lll}
(3) \quad i) & \beta_j(Sa/\!\!/a) = S\beta_j, & j = 1,2,3 \\
ii) & \beta_4(Sb/\!\!/b) = S\beta_4 & \\
iii) & \beta'_j(Sa'/\!\!/a') = S\beta'_j, & j = 1,3 \\
iv) & \beta'_4(Sb'/\!\!/b') = S\beta'_4 & \\
v) & \beta_j(a'/\!\!/a) = \beta'_j, & j = 1,3 \\
vi) & \beta_4(b'/\!\!/b) = \beta'_4 & \\
vii) & \beta_2(b/\!\!/a) = \beta_4 & \\
viii) & \alpha(\beta_1/\!\!/a, Sb/\!\!/b, \beta'_1/\!\!/a', Sb'/\!\!/b', a \circ b \circ a' \circ b' \circ c/\!\!/c) = & \\
 & \qquad = \beta_3 \circ \beta_4 \circ \beta'_3 \circ \beta'_4 \circ \alpha & \\
ix) & \alpha(\beta'_1/\!\!/a, Sb'/\!\!/b, a/\!\!/a', b/\!\!/b', a' \circ b' \circ c/\!\!/c) = \beta'_3 \circ \beta'_4 \circ \alpha &
\end{array}
$$

(Recall that $\circ$ associates from right to left.) Any solution to $(3.i)$–$(3.vii)$ must have $\beta_j = S^{k_j}a$ and $\beta'_j = S^{k_j}a'$ for $j = 1,2,3$ and have $\beta_4 = S^{k_2}b$ and $\beta'_4 = S^{k_2}b'$. We need to show that $(3.viii)$ and $(3.ix)$ are also satisfiable if and only if $k_1 \cdot k_2 = k_3$. In fact we claim that the only solution has α equal to

$$
\begin{aligned}
& S^{(k_2-1)k_1}a \circ S^{k_2-1}b \circ S^{(k_2-1)k_1}a' \circ S^{k_2-1}b' \circ \cdots \circ \\
& \qquad S^{2k_1}a \circ S^2 b \circ S^{2k_1}a' \circ S^2 b' \circ S^{k_1}a \circ Sb \circ S^{k_1}a' \circ Sb' \circ a \circ b \circ a' \circ b' \circ c
\end{aligned}
$$

where $k_1 \cdot k_2 = k_3$.

It is obvious that when $k_1 \cdot k_2 = k_3$ this value for α is a solution with all possible substitutions being made. It remains to see that this is the only possible solution. Suppose that values have been assigned to α and the β's which satisfy the equations. First of all, α might be set equal to the term c; in this case $k_2 = k_3 = 0$. Otherwise, α must be of the form

$$
S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a' \circ S^{n'_1}b' \circ \alpha_2.
$$

This follows from equation (3.*viii*) since we can write α uniquely in the form $\rho_1 \circ \rho_2 \circ \rho_3 \circ \cdots \rho_t$ and because of the form of the partial substitutions. From $\beta_1 = S^{k_1}a$ and $\beta_3 = S^{k_3}a$ it follows that ρ_1 must be either $S^{k_3}a$ or $S^{k_3-k_1}a$. Similarly ρ_2 must be either $S^{k_2}a$ or $S^{k_2-1}a$, and similarly for ρ_3 and ρ_4. Thus we have m_1 and m'_1 are either k_3 or $k_3 - k_1$ but not necessarily equal, and n_1 and n'_1 are k_2 or $k_2 - 1$ and again not necessarily equal. Furthermore, α_2 satisfies the equation

$$\alpha_2(\beta_1 /\!\!/ a, Sb /\!\!/ b, \beta'_1 /\!\!/ a', Sb' /\!\!/ b', a \circ b \circ a' \circ b' \circ c /\!\!/ c) = \\ = S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a' \circ S^{n'_1}b' \circ \alpha_2$$

which is identical in form to (3.*viii*). Reasoning inductively shows that α must be of the form

$$S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a' \circ S^{n'_1}b' \circ \cdots \circ S^{m_t}a \circ S^{n_t}b \circ S^{m'_t}a' \circ S^{n'_t}b' \circ c$$

where m_1 and m'_1 are k_3 or $k_3 - k_1$, n_1 and n'_1 are k_2 or $k_2 - 1$, m_{i+1} is m_i or $m_i - k_1$, m'_{i+1} is m'_i or $m'_i - k_1$, n_{i+1} is n_i or $n_i - 1$, n'_{i+1} is n'_i or $n'_i - 1$, and $m_t = n_t = m'_t = n'_t = 0$. Note that in each case the first choice of values holds when the corresponding instance of the substitution is *not* carried out; when the substitution is made, the second value applies.

Now consider the fact that equation (3.*ix*) is also satisfied. The righthand side of the equation has the form

$$S^{k_3}a' \circ S^{k_2}b' \circ S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a' \circ S^{n'_1}b' \circ \alpha_2.$$

The substitution must cause the first a, b, a', and b' of α to be replaced by $S^{k_1}a'$, Sb', a and b respectively and thus $k_3 = m_1 + k_1$, $k_2 = n_1 + 1$, $m_1 = m'_1$, and $n_1 = n'_1$. Furthermore α_2 satisfies the equation

$$\alpha_2(\beta'_1 /\!\!/ a, Sb' /\!\!/ b, a /\!\!/ a', b /\!\!/ b', a' \circ b' \circ c /\!\!/ c) = S^{m'_1}a' \circ S^{n'_1}b' \circ \alpha_2$$

which, by the same reasoning, implies that $m'_1 = m_2 + k_1$, $n'_1 = n_2 + 1$, $m_2 = m'_2$, $n_2 = n'_2$. Continuing inductively we have that $m_1 = m'_1 = k_3 - k_1$, $n_1 = n'_1 = k_2 - 1$, $m_{i+1} = m'_{i+1} = m_i - k_1$ and $n_{i+1} = n'_{i+1} = n_i - 1$, so $m_i = k_1 \cdot n_i$ for all i and $k_3 = k_1 \cdot k_2$.

We have established that equation 3 correctly prescribes multiplication; however, the last two equations allow simultaneous partial substitutions in five

variables and our definition of unification problems did not allow equations involving simultaneous substitutions. Fortunately, equation (3.*viii*) can easily be replaced by five single partial substitutions using new intermediate variables and equation (3.*ix*) can be equivalently replaced by two equations

$$\alpha(a''/\!\!/a', b''/\!\!/b') = \alpha'$$

$$\alpha'(\beta_1'/\!\!/a, Sb'/\!\!/b, a/\!\!/a'', b/\!\!/b'', a' \circ b' \circ c/\!\!/c) = \beta_3' \circ \beta_4' \circ \alpha$$

and these two simultaneous partial substitutions can be replaced by seven equations using more intermediate variables.

Given the above equations for defining the integers and addition and multiplication it is easy to effectively transform any diophantine equation into a second-order unification problem with partial substitution so that the unification problem has a solution if and only if the diophanitine equation has a zero. So Theorem 2 now follows from Matijacevič's theorem. The proof above establishes a stronger version of Theorem 2; namely, for any r.e. set X there is a set Ω of partial substitution equations such that, for all n, $n \in X$ if and only if $\Omega \cup \{\beta_1 = S^n 0\}$ has a solution.

For our proof of the undecidability of k-provability we shall use a restricted version of the unification problem with partial substitution:

Definition A partial substitution satisfies the *special restriction* if it is of the form $\beta(s/\!\!/a) = \sigma$ where s is neither a second-order variable nor the first-order variable a.

The above partial substitution equations did not all satisfy the special restriction, but it is easy to modify them so that they do. First, equation (2.*ii*) can be replaced by $\beta_1(SS\beta_2/\!\!/a) = SS\beta_3$ and the three equations still define addition. In equations (3.*viii*) and (3.*ix*), if β_1 and β_1' are replaced by $S\beta_1$ and $S\beta_1'$ then the equations obey the special restriction and define the property $(k_1 + 1)k_2 = k_3$. Now since multiplication can be defined by $xy = z \Leftrightarrow (x + 1)y = z + y$, Matijacevič's theorem implies:

Theorem 3 *The second-order unification problem with partial substitution under the special restriction is r.e.-complete. Indeed, for any r.e. set X there is a set Ω of partial substitution equations satisfying the special restriction such that, for all n, $n \in X$ if and only if $\Omega \cup \{\beta_1 = S^n 0\}$ has a solution.*

3 The Sequent Calculus

The sequent calculus is a formulation of the first-order logic due to Gentzen; this section contains a brief review (see [13] for a detailed exposition) and proves some lemmas needed for the proof of the Main Theorem.

The sequent calculus uses the logical symbols $\wedge$, $\vee$, $\neg$, $\supset$, $\exists$ and $\forall$; it has *free* variables denoted $a, b, c, \ldots$ and *bound* variables denoted $x, y, z, \ldots$. *Terms* are formed from constant symbols, free variables and function symbols; *semiterms* are like terms but may also contain bound variables. *Formulas* are defined as usual with the proviso that only bound variables may be quantified and only free variables may appear free. *Semiformulas* are defined similarly except both free and bound variables may occur free in a semiformula; note that in general a subformula of a formula is actually a semiformula. A *sequent* is a line of the form

$$A_1, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell$$

where the A_i's and B_j's are formulas; its intended meaning is $\bigwedge_i A_i \supset \bigvee_i B_i$. We permit k or ℓ to be zero. A (possibly empty) series of formulas separated by commas is a *cedent*; in the sequent above, $A_1, \ldots, A_k$ is the *antecedent* and $B_1, \ldots B_\ell$ is the *succedent*.

A sequent calculus proof is a series of sequents; each sequent must either be an axiom or be derived by one of the rules of inference given below. To avoid ambiguity, a proof also specifies explicitly how each sequent to derived by indicating which axiom or which rule and hyptheses are used. The size of a proof is the number of sequents in the proof.

It is actually more common to treat sequent proofs as trees of sequents; however, we define them here to be sequences of sequences or, equivalently, directed acyclic graphs. The results below also show that the Main Theorem also applies to the sequent calculus using proof trees. A sequent proof is said to be *tree-like* if every occurence of a sequent in the proof other than the endsequent is used exactly once as a hypothesis of an inference. Obviously any proof can be transformed into a tree-like proof by duplicating subproofs to derive intermediate results multiple times.

The logical axioms are sequents of the form $A \longrightarrow A$. The equality axioms are sequents of the form $\longrightarrow t_1 = t_1$ or $t_1 = t_2 \longrightarrow t_2 = t_1$ or

$$s_1 = t_1, \ldots, s_k = t_k, P(s_1, \ldots s_k) \longrightarrow P(t_1, \ldots t_k)$$

or

$$s_1 = t_1, \ldots, s_k = t_k \longrightarrow f(s_1, \ldots s_k) = f(t_1, \ldots t_k)$$

where s_i and t_i are terms, P is a k-ary predicate symbol and f is a k-ary function symbol. Since P may be equality ($=$), these axioms imply the transitivity of equality.

Letting capital Greek letters $\Gamma, \Delta, \Pi, \Lambda, \ldots$ stand for cedents, the valid rules of inference are:

$\neg$:*left* $\dfrac{\Gamma \longrightarrow \Delta, A}{\neg A, \Gamma \longrightarrow \Delta}$ $\neg$:*right* $\dfrac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg A}$

$\wedge$:*right* $\dfrac{\Gamma \longrightarrow \Delta, A \qquad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \wedge B}$

$\wedge$:*left* $\dfrac{A, \Gamma \longrightarrow \Delta}{A \wedge B, \Gamma \longrightarrow \Delta}$ $\dfrac{B, \Gamma \longrightarrow \Delta}{A \wedge B, \Gamma \longrightarrow \Delta}$

$\vee$:*left* $\dfrac{A, \Gamma \longrightarrow \Delta \qquad B, \Gamma \longrightarrow \Delta}{A \vee B, \Gamma \longrightarrow \Delta}$

$\vee$:*right* $\dfrac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \vee B}$ $\dfrac{\Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \vee B}$

$\supset$:*left* $\dfrac{\Gamma \longrightarrow \Delta, A \qquad B, \Gamma \longrightarrow \Delta}{A \supset B, \Gamma \longrightarrow \Delta}$

$\supset$:*right* $\dfrac{A, \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \supset B}$

$\exists$:*left* $\dfrac{A(b), \Gamma \longrightarrow \Delta}{(\exists x)A(x), \Gamma \longrightarrow \Delta}$ $\exists$:*right* $\dfrac{\Gamma \longrightarrow \Delta, A(t)}{\Gamma \longrightarrow \Delta, (\exists x)A(x)}$

$\forall$:*left* $\dfrac{A(t), \Gamma \longrightarrow \Delta}{(\forall x)A(x), \Gamma \longrightarrow \Delta}$ $\forall$:*right* $\dfrac{\Gamma \longrightarrow \Delta, A(b)}{\Gamma \longrightarrow \Delta, (\forall x)A(x)}$

In the $\exists$:*left* and $\forall$:*right* inferences the free variable b is called the *eigenvariable* and must not appear in the lower sequent. The variable x must be freely substitutable into A for all four quantifier inferences.

Cut $\dfrac{\Gamma \longrightarrow \Delta, A \qquad A, \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}$

Weakening: $\dfrac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta}$ $\qquad$ $\dfrac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A}$

Exchange: $\dfrac{\Gamma, A, B, \Pi \longrightarrow \Delta}{\Gamma, B, A, \Pi \longrightarrow \Delta}$ $\qquad$ $\dfrac{\Gamma \longrightarrow \Delta, A, B, \Lambda}{\Gamma \longrightarrow \Delta, B, A, \Lambda}$

Contraction: $\dfrac{A, A, \Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta}$ $\qquad$ $\dfrac{\Gamma \longrightarrow \Delta, A, A}{\Gamma \longrightarrow \Delta, A}$

The final four types of rules, *Cut* through *Contraction*, are called *structural* inferences; the rest are called *logical* inferences.

The *principal formula* of an inference is the formula in the lower sequent of the inference upon which the inference acted; for example, the $\forall$:*left* inference above has $(\forall x)A(x)$ as principal formula. Note that cut inferences have no principal formula and exchange inferences have two principal formulas. The *auxilliary formula(s)* of an inference are the formulas in the upper sequent which are used by the inference — the rest of the formulas (in Γ, Δ, Π, Λ) are the *side formulas*.

The above completes the definition of the sequent calculus LK_e. The system obtained by removing the equality symbol $=$ and its associated initial sequents is called LK.

We wish to develop a theory of how the influence of a formula spreads through a proof. This will be done by defining a directed graph called the *logical flow graph*[‡]. The logical flow graph has as nodes the subformulas occurring in the proof. For convenience, suppose we have a fixed proof P in hand; we define an *s-formula* to be an occurrence of a subformula of a formula occurring in P. (The "s-" stands for "semi-" or "sub-".) It should be stressed that an s-formula is an *occurrence* of a semiformula in a proof as compared to the semiformula itself which may occur many times in the proof. An s-formula A is a *variant* of B if A can be obtained from B by changing some of the semiterms in B. The logical flow graph (defined below) will have as nodes the s-formulas in P; two s-formulas will be connected by an

[‡]Concepts similar to our definition of logical flow graph have already been introduced by J.-Y. Girard [3] who discusses tracing the flow of formulas through linear logic proofs.

edge only if they are variants of each other. Furthermore, any two s-formulas connected by an edge will be in (distinct) sequents of some inference or will both be in an axiom on opposite sides of the sequent arrow ($\longrightarrow$).

We define the logical flow graph by specifying the edges: First, in an axiom $A \longrightarrow A$ there is an edge directed from the lefthand A to the righthand A. In an equality axiom

$$s_1 = t_1, \ldots, s_k = t_k, P(s_1, \ldots s_k) \longrightarrow P(t_1, \ldots, t_k)$$

there is an edge directed from the $P(\vec{s})$ to the $P(\vec{t})$. In all other equality axioms (and when P is equality in the above axiom), there is an edge from each formula in the antecedent to the formula in the succedent. Second, in any logical or structural inference listed above, there is an edge directed from the i-th formula in the cedent denoted Γ or Π in the lower sequent to the corresponding formula in the upper sequent. And, in each inference, there is an edge directed from the i-th formula in the cedent denoted Δ or Λ in the upper sequent to the corresponding formula in the lower sequent. Third, in any inference if A (sometimes B) is an auxilliary formula which appears in the *succedent* of an upper sequent of the inference then there is a edge directed from that A (or B) to the corresponding s-formula in the lower sequent. And if A (sometimes B) is an auxilliary formula which appears in the *antecedent* of an upper sequent of an inference then there is a edge directed *towards* that A (or B) *from* the corresponding s-formula in the lower sequent.

Before finishing the definition of the logical flow graph, lets illustrate two examples of the third part of the definition. In the $\wedge$*:right* inference there is an edge from the upper A to the lower A and an edge from the upper B to the lower B. In an $\exists$*:left* there is an edge from the $A(x)$ to the $A(b)$. Note there is no edge directed away from the s-formula $(\exists x)A(x)$.

Fourth, in a cut inference there is an edge directed from the cut formula A in the succedent of the lefthand upper sequent to the occurrence of A in the antecedent of the righthand upper sequent.

Fifth and finally, suppose there is a directed edge from an s-formula A_1 to A_2 and suppose B_1 is a subformula of A_1. Since A_1 and A_2 are variants there is a subformula B_2 of A_2 which corresponds to the subformula B_1 of A_1; B_1 and B_2 are, of course, variants. If B_1 occurs positively in A_1 then there is an edge from B_1 to B_2. If B_1 occurs negatively in A_1 then there is an edge directed from B_2 to B_1. Recall that B_1 occurs positively (negatively) in A if

the B_1 occurs an even (odd) number of times in the scope of a negation or in the lefthand operand of an implication. Of course B_1 occurs positively in A_1 if and only if B_2 occurs positively in A_2.

The above concludes the definition of the logical flow graph. As an example consider the following proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{A \longrightarrow A}{\neg A, A \longrightarrow}}{\neg A, A \longrightarrow B}}{A \longrightarrow (\neg A) \supset B} \qquad \dfrac{\dfrac{\dfrac{B \longrightarrow B}{\neg A, B \longrightarrow B}}{B \longrightarrow (\neg A) \supset B}}{A \vee B \longrightarrow (\neg A) \supset B}$$

The logical flow graph restricted to the formulas A and B is shown below (edges for $\neg A$ and $\neg A \supset B$ are not shown):

$$\begin{array}{cccc} A & A & & \\ \neg A, A & & & B \quad B \\ \neg A, A & B & \neg A, B & B \\ A & (\neg A) \supset B & B & (\neg A) \supset B \end{array}$$

$$A \vee B \longrightarrow (\neg A) \supset B$$

Looking at just the subgraph for A, there is a path from the A in the final antecedent up to the logical axiom for A and back down to the A in the succedent of the endsequent. And there is a path of length two from the subformula A of the $\neg A$ introduced with a *Weak:left* inference. Although this is a very simple example, it should be clear that the logical flow graph traces the influence of A through the proof.

The concept of the logical flow graph will be useful in the next section for proving lower bounds on the number of inferences in a proof. First a few more definitions and some lemmas must be established.

Definition An s-formula occurs positively if and only if it is in a sequent $\Gamma \longrightarrow \Delta$ and either occurs positively in a formula in Δ or negatively in a formula in Γ. Otherwise the s-formula occurs negatively.

Definition Let P be a proof and let E be an edge in the logical flow graph of P directed from A to B. Note that either (1) there is a unique common inference J containing both A and B such that J gave rise to E or (2) A and B are in an axiom. (There may be more than one inference containing both A and B but there is only one that caused E to be in the logical flow graph.) If A is in an upper sequent of J and B is in the lower sequent of J then we say E is a *downward* edge. If B is in an upper sequent and A in a lower sequent then E is an *upward* edge. If A and B are both in upper sequents (so J is a cut) or if A and B are in an axiom then E is a *lateral* edge.

Proposition 4 *Let P be a proof. Every downward edge connects two s-formulas which occur positively. Every upward edge connects s-formulas which occur negatively. Every lateral edge is incident on an s-formula which occurs positively and on an s-formula which occurs negatively.*

Proposition 5 *Let P be a proof and A an s-formula in P.*

(a) *Suppose A occurs positively in P. Then each edge directed towards A in the logical flow graph is either lateral or downward; all incoming edges have the same direction. If the incident edges are downward, there may be 0, 1 or 2 of them. Furthermore, if P is tree-like, the outdegree of A in the logical flow graph will be one (or zero if A is in the endsequent or in a sequent not used in the proof).*

(b) *Suppose A occurs negatively in P. Then either there is one lateral edge directed away from A or there are up to two upward edges directed away from A. Furthermore, if P is tree-like, the indegree of A will be one (or zero if A is in the endsequent or in a sequent not used in the proof).*

Propositions 4 and 5 are easily proved by examining the definition of the logical flow graph. For example, in Proposition 5 when A occurs positively, A will have lateral incoming edges only if A appears in an axiom. Otherwise the indegree is zero if and only if A is a subformula of a formula introduced by a weakening inference. The indegree is two if A is a subformula of a formula which is merged with an identical formula by a contraction, $\vee$*:left* or $\wedge$*:right* inference. There is one incoming downward edge in the other cases. Similar considerations apply to Proposition 5(b).

For the rest of this section we shall let $\top$ be an abbreviation for some (arbitrary) valid formula and $\bot$ be an abbreviation for its negation. So $\top$ and $\bot$ are formulas such that $\longrightarrow \top$ and $\bot \longrightarrow$ are LK-provable. We are not however adding these to our language for first-order logic; in particular, it is important for Propositions 6 and 10 that atomic formulas A and B are not $\top$ or $\bot$.

Definition Given a proof P, a *forward* (respectively, *backward*) path is a non-trivial path in the logical flow graph of P which traverses edges in the forward (backward) direction. By *path* we always mean non-trivial path. The s-formula B is *forward-reachable* from the s-formula A if and only if B is A or there is a forward path from A to B. B is *backward-reachable* from A if A is forward-reachable from B.

Proposition 6 *Let P be a proof of $\Gamma \longrightarrow \Delta$ and let A be an atomic s-formula appearing negatively (respectively, positively) in $\Gamma \longrightarrow \Delta$ such that A does not have equals ($=$) as its relation symbol. Then either there is a forward (respectively, backward) path from A to another s-formula B in $\Gamma \longrightarrow \Delta$ or the sequent $\Gamma^* \longrightarrow \Delta^*$ obtained by replacing A with $\top$ (respectively, $\bot$) is valid.*

The gist of Proposition 6 is that if A occurs negatively in $\Gamma \longrightarrow \Delta$ and is essential to the validity of the sequent then there is a forward path from A back to another s-formula B in $\Gamma \longrightarrow \Delta$; note that B must occur positively in $\Gamma \longrightarrow \Delta$. Note that this proposition implies the elementary fact that if B is a valid formula and if a predicate symbol Q appears only positively in B then every atomic subformula $Q(\cdots)$ of B may be replaced by $\bot$ and the resulting formula will still be valid. This fact has a simple model-theoretic proof; Proposition 6 gives a proof-theoretic proof.

Proof of Proposition 6. We shall only treat the case of A occuring negatively; the other case is handled similarly. Suppose there is no forward path from A back to the endsequent.

Claim: There is a *tree-like* proof P_1 of $\Gamma \longrightarrow \Delta$ such that in the logical flow graph of P_1 there is no forward path from A to another s-formula in $\Gamma \longrightarrow \Delta$.

Proof of Claim: P_1 is formed by converting P to a tree-like proof in the following manner: Find the first sequent in P which is used multiple times as

a hypothesis and duplicate the subproof of this sequent as necessary to remove the multiple usage of that sequent. Iterate this process until a tree-like proof is obtained. It is easy to see that this transformation can not create a new path from A back to the endsequent (although if such a path existed it might be destroyed). This proves the claim.

Since A is atomic, it is of the form $Q(s_1, \ldots, s_k)$ for some predicate symbol Q. Form P_2 from P_1 by replacing every s-formula forward-reachable from A by $\top$. To prove Proposition 6 it suffices to show that the endsequent of P_2 is valid. To accomplish this we show that P_2 can be modified to be a correct proof. There are several ways in which P_2 might fail to be a proof: First, an equality axiom forward-reachable from A might have been changed to (for example):

$$r_1 = t_1, \ldots, r_k = t_k, \top \longrightarrow \top.$$

This is no longer an axiom, but it is valid; indeed, $\longrightarrow \top$ is valid. Second, where P_1 had a contraction, P_2 might contain (for example):

$$\frac{\Gamma \longrightarrow \Delta, C', C''}{\Gamma \longrightarrow \Delta, C^*}$$

where C', C'' and C^* are obtained from a formula C replacing some subformulas of the form $Q(\cdots)$ by $\top$. If a subformula $Q(\cdots)$ is negatively occuring in C and it is replaced by $\top$ in any one of the formulas C', C'' or C^* then it will also be replaced by $\top$ in all three of them; this is because P_1 is tree-like and the only edges in the logical flow graph of P_1 directed towards the occurences of negatively occuring subformulas of C' and C'' come from the corresponding subformulas of C^*. Furthermore if $Q(\cdots)$ is a positively occuring subformula of C and is replaced by $\top$ in *either* C' or C'' then it will also be replaced in C^*. Thus C^* can be obtained from either one of C' and C'' by changing some positively occuring subformulas to $\top$. It follows that $C' \supset C^*$ and $C'' \supset C^*$ are valid. Hence the above "inference" in P_2 is sound. Third, $\vee$*:right* and $\wedge$*:left* inferences contain implicit contractions of the side formulas; these are handled in the same way as contractions. Because P_2 is tree-like, these three cases are the only way in which P_2 can fail to be a valid proof and its final sequent must be valid. (Note that if P_1 contains an inference

$$\frac{\Gamma \longrightarrow \Delta}{\Pi \longrightarrow \Lambda}$$

then a negatively occuring s-formula in $\Gamma \longrightarrow \Delta$ is forward-reachable from A only via a path which goes through $\Pi \longrightarrow \Lambda$. This will not necessarily be true of a non-tree-like proof[§].)
Q.E.D. Proposition 6

Proposition 7 *Let P be a proof and $A \vee B$ be an s-formula occuring negatively in the endsequent $\Gamma \longrightarrow \Delta$ of P. Then at least one of the following holds:*

(a) *There is a forward path from $A \vee B$ to another s-formula in $\Gamma \longrightarrow \Delta$,*

(b) *There is an $\vee$:left inference with principal formula $A^* \vee B^*$ forward-reachable from $A \vee B$, or*

(c) *$\Gamma \longrightarrow \Delta$ is still valid after $A \vee B$ is replaced by $\top$.*

There is a dual version of Proposition 7 regarding $A \wedge B$ occuring positively in $\Gamma \longrightarrow \Delta$; it is stated with "backward", "$\wedge$*:right*", and "$\bot$" replacing "forward", "$\vee$*:left*" and "$\top$".

Proof of Proposition 7. Suppose there is no forward path from $A \vee B$ back to the endsequent and that there is no $\vee$*:left* inference satisfying (b). We show that the result of changing $A \vee B$ to $\top$ in $\Gamma \longrightarrow \Delta$ is valid—the proof is similar to the proof of Proposition 6. First form a tree-like proof P_1 of $\Gamma \longrightarrow \Delta$ by duplicating subproofs of P_1 as necessary. There will still be no forward path from $A \vee B$ back to the endsequent and no inference satisfying (b). Now form P_2 from P_1 by replacing every s-formula forward-reachable from $A \vee B$ with $\top$. Just as in the proof of Proposition 6 every "inference" in P_2 is valid and hence the endsequent of P_2 is valid.
Q.E.D. Proposition 7

Propositions 6 and 7 are special cases of the following more general result.

Proposition 8 *Let P be a proof and A an s-formula occuring negatively (respectively, positively) in the endsequent $\Gamma \longrightarrow \Delta$ of P. Then (at least) one of the following holds:*

(a) *There is a forward (respectively, backward) path from A to another s-formula in $\Gamma \longrightarrow \Delta$,*

[§]Our construction works for non-tree-like proofs as well, but the proof is less clear.

(b) *There is an s-formula forward- (respectively, backward-) reachable from A which is the principal formula of a logical inference, or*

(c) $\Gamma \longrightarrow \Delta$ *is still valid if the s-formula A is replaced by $\top$ (respectively, $\bot$).*

Basically, Proposition 8 states that if an s-formula A of $\Gamma \longrightarrow \Delta$ is not used in an essential way in the proof of $\Gamma \longrightarrow \Delta$ then $\Gamma \longrightarrow \Delta$ maybe weakened by changing A to $\top$ or $\bot$ as appropriate and still remain valid. The proof of Proposition 8 is similar to the proofs Propositions 6 and 7 and is omitted.

The next proposition gives a related result for negatively occuring s-formulas which are conjunctions.

Proposition 9 *Let P be a proof and $A \wedge B$ be an s-formula occuring negatively in the endsequent $\Gamma \longrightarrow \Delta$ of P. Then at least one of the following holds:*

(a) *There is a forward path from $A \wedge B$ to another s-formula in $\Gamma \longrightarrow \Delta$,*

(b) *There are at least two $\wedge$:left inferences with principal formulas forward-reachable from $A \wedge B$,*

(c) $\Gamma \longrightarrow \Delta$ *is still valid if $A \wedge B$ is replaced by A, or*

(d) $\Gamma \longrightarrow \Delta$ *is still valid if $A \wedge B$ is replaced by B.*

Again there is a dual version of Proposition 9 regarding an s-formula $A \vee B$ occuring negatively in the endsequent of P.

Proof of Proposition 9. Suppose that neither (a) nor (b) hold and that the only (if any) $\wedge$*:left* inference with principal formula forward-reachable from $A \wedge B$ is of the form

$$\frac{A^*, \Pi \longrightarrow \Lambda}{A^* \wedge B^*, \Pi \longrightarrow \Lambda}$$

(The case where B^* appears in the upper sequent instead of A^* is handled similarly.) Obtain a tree-like proof P_1 of $\Gamma \longrightarrow \Delta$ by duplicating subproofs of P as necessary. As before, there will be no forward path from $A \wedge B$ back to the endsequent of P_1. Also, every $\wedge$*:left* inference with principal formula forward-reachable from $A \wedge B$ will be identical to the one in P. Now form P_2

from P_1 by replacing each s-formula $A' \wedge B'$ forward-reachable from $A \wedge B$ by A'. P_2 can fail to be a proof in several ways: First, the $\wedge$*:right* inference will become

$$\frac{A^*, \Pi \longrightarrow \Lambda}{A^*, \Pi \longrightarrow \Lambda}$$

which is clearly a valid "inference". Second, a contraction of a formula C in P_1 may become an "inference" of the form (for example):

$$\frac{\Pi \longrightarrow \Lambda, C', C''}{\Pi \longrightarrow \Lambda, C^*}$$

Here C', C'' and C^* are formed by replacing some subformulas of the form $A_i \wedge B_i$ by A_i. Now if $A_i \wedge B_i$ is a negatively occuring subformula of C which is replaced by A_i in any one of C', C'' or C^* then it will be replaced by A_i in all three formulas; this is because P_1 is tree-like and the only edges in the logical flow graph directed towards a negatively occuring subformula in the upper sequent come from the lower sequent of the contraction inference. If $A_i \wedge B_i$ is a positively occuring subformula of C and it is replaced by A_i in either C' or C'', then it is also replaced by A_i in C^*. Thus C^* can be obtained from C' by replacing some positively occuring subformulas of the form $A_i \wedge B_i$ by A_i; hence $C' \supset C^*$ is valid. Similarly, $C'' \supset C^*$ is valid. Hence the above "inference" in P_2 is valid. The implicit contractions of side formulas in $\vee$*:left* and $\wedge$*:right* inferences are handled the same way. Hence the final sequent of P_2 is valid.
Q.E.D. Proposition 9

Suppose $A \vee B$ occurs negatively in the endsequent $\Gamma \longrightarrow \Delta$ of a proof P with A and B atomic formulas not involving equality. According to Proposition 6, under certain circumstances there are forward paths π_A and π_B from A and B back to the endsequent. We shall say that the two paths *parallel each other* for as long as they travel together along a path from $A \vee B$. Of course there may be no path from $A \vee B$ back to the endsequent and π_A and π_B may be forced to stop paralleling each other and diverge at an $\vee$*:left* inference. The next proposition states sufficient conditions for there to be paths π_A and π_B that parallel each other until an $\vee$*:left* inference separates them.

Proposition 10 *Suppose P is a proof with endsequent $\Gamma \longrightarrow \Delta$ and $A \vee B$ is a negatively occuring s-formula in $\Gamma \longrightarrow \Delta$ with A and B atomic formulas not involving the equality sign. Then at least one of the following holds:*

(a) *There is a forward path form $A \vee B$ back to $\Gamma \longrightarrow \Delta$,*

(b) *There are forward paths π_A and π_B from A and B, respectively, back to $\Gamma \longrightarrow \Delta$ such that π_A and π_B parallel each other until they diverge at an $\vee$:left inference, or*

(c) *$\Gamma \longrightarrow \Delta$ is still valid after $A \vee B$ is replaced by $\top$.*

Proof As usual, it will suffice to prove the theorem for the cut-free proof P_1 obtained by duplicating subproofs of P as necessary. This is because any path in P_1 can be mapped back down to a path in P. It will suffice to show that there is an $\vee$*:left* inference

$$\frac{A^*, \Pi \longrightarrow \Lambda \qquad B^*, \Pi \longrightarrow \Lambda}{A^* \vee B^*, \Pi \longrightarrow \Lambda}$$

in P_1 with a forward path from $A \vee B$ to $A^* \vee B^*$ and with forward paths from A^* and from B^* back to $\Gamma \longrightarrow \Delta$. So suppose not. For each $\vee$*:left* inference of the form above with principal inference forward-reachable from $A \vee B$, if no path exists from A^* (respectively, B^*) to $\Gamma \longrightarrow \Delta$, replace A^* (respectively B^*) and every s-formula forward-reachable from it by $\top$. And replace every s-formula forward-reachable from the $A \vee B$ in Γ by $\top$. The same argument used for proving Propositions 6 and 7 shows that this transforms P_1 into a valid "proof"; note that the inference displayed above will become vacuous with one of its upper sequents equal to the lower sequent. Unless (a) holds, the resulting endsequent is $\Gamma \longrightarrow \Delta$ with the s-formula $A \vee B$ replaced by $\top$.
Q.E.D. Proposition 10

4 The Undecidability Proof for k-Provability

We shall first prove Main Theorem 1 for the system LK with no equality axioms. To do this, we reduce the second-order unification problem with

partial substitution problem to the k-provability problem for LK. Given a second-order unification problem satisfying the special restriction consisting of equations

$$\beta_{i_j}(\rho_j /\!\!/ a_{i_j}) = \sigma_j$$

for $j = 1, \ldots, m$, we shall produce a formula Φ and an integer N such that $\longrightarrow \Phi$ has a proof of $\leq N$ lines if and only if the unification problem has a solution. The formula Φ will always be valid and have a very straightforward proof; however, a solution to the unification problem will give a slightly shorter proof (in terms of number of sequents in the proof).

Recall that the β_i's are second-order variables, a_i's are first-order variables and ρ_j and σ_j are terms involving β_i's, a_i's and function and constant symbols. We shall also use the β_i's as *bound* variables in the sequent calculus. Let U_j be the semiformula

$$P_j(\sigma_j, \rho_j) \vee P_j(\beta_{i_j}, a_{i_j}) \vee P_j(z_j^1, b_j^1) \vee P_j(z_j^2, b_j^2) \vee P_j(z_j^3, b_j^3) \vee P_j(z_j^4, b_j^4)$$

where P_j is a binary relation symbol and $z_j^1, \ldots, z_j^4$ are new bound variables and $b_j^1, \ldots, b_j^4$ are new free variables. (We adopt the convention that conjunction and disjunction always associate from right to left.) Then Φ is the formula

$$\left(\forall z_1^1 \forall z_1^2 \cdots \forall z_m^3 \forall z_m^4 \forall \beta_1 \cdots \forall \beta_k \bigwedge_{j=1}^{m} U_j\right) \supset \left(\bigwedge_{j=1}^{m} \exists y \exists x P_j(x, y)\right)$$

where $\beta_1, \ldots, \beta_k$ are the second-order variables appearing in the unification problem.

By Theorem 3 we need only consider unification problems of the form $\Omega \cup \{\beta_1 = S^n 0\}$; note that in this case, Φ can be written as $A(S^n 0)$ where $A(x)$ depends only on Ω.

Φ is obviously a valid formula; the question is what the minimum size proof of Φ is. Lets begin by outlining a (non-optimal) proof of Φ. For arbitrary terms $t_1, \ldots, t_k, r_1^1, \ldots, r_m^4$ let $U(\vec{t}, \vec{r})$ be the result of substituting the $t_i's$ for the β_i's and the r_i^p's for the z_i^p's in U_j. Then $\longrightarrow \Phi$ will be derived by $k + 4m$ $\forall$*:left* inferences and one $\supset$*:right* inference from

$$\bigwedge_{j=1}^{m} U_j(\vec{t}, \vec{r}) \longrightarrow \bigwedge_{j=1}^{m} \exists y \exists x P_j(x, y).$$

This can be derived from the m sequents

$$U_j(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_j(x,y)$$

by $m-1$ $\wedge$*:right* inferences and $2(m-1)$ $\wedge$*:left* inferences; this derivation begins with

$$\frac{U_m(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_m(x,y)}{U_{m-1}(\vec{t},\vec{r}) \wedge U_m(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_m(x,y)}$$

$$\frac{\dfrac{U_{m-1}(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_{m-1}(x,y)}{U_{m-1}(\vec{t},\vec{r}) \wedge U_m(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_{m-1}(x,y)}}{U_{m-1}(\vec{t},\vec{r}) \wedge U_m(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_{m-1}(x,y) \wedge \exists y \exists x P_m(x,y)}$$

and continues this pattern $m-1$ times. Now $U_j(\vec{t},\vec{r})$ is of the form

$$P_j(\sigma_j^*,\rho_j^*) \vee P_j(t_{i_j},a_{i_j}) \vee P_j(r_j^1,b_j^1) \vee P_j(r_j^2,b_j^2) \vee P_j(r_j^3,b_j^3) \vee P_j(r_j^4,b_j^4)$$

where ρ_j^* and σ_j^* are the terms obtained from ρ_j and σ_j after the β_i's are changed to t_i's. The sequent $U_j(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_j(x,y)$ can be derived by using five $\vee$*:left* inferences to combine sequents of the form $P(v,w) \longrightarrow \exists y \exists x P_j(x,y)$. These latter sequents, of course, have simple proofs, each containing one logical axiom and two $\exists$*:left* inferences. This proof of $U_j(\vec{t},\vec{r}) \longrightarrow \exists y \exists x P_j(x,y)$ has exactly 23 sequents (all distinct since, because of the special restriction, ρ_j^* will not be equal to a_{i_j} or any b_j^i).

Counting the number of inferences and axioms in the above proof of Φ we see that there are $(k+4m+1)+(3m-3)+23m$ sequents. So the proof of Φ has $k+30m-2$ sequents. However, this proof of Φ is not the most efficient proof. Suppose the terms $\vec{t}$ are chosen so that setting $\beta_i = t_i$ provides a solution to

$$\beta_{i_j}(\rho_j /\!\!/ a_{i_j}) = \sigma_j$$

for some particular value of j. Since this equation is satisfied there must be some set S of occurences of a_{i_j} in t_{i_j} such that changing each a_{i_j} in S to ρ_j^* yields the term σ_j^*. Let $v(w)$ denote the result of substituting w into t_{i_j} for each $a_{i_j} \in S$. Thus $v(\rho_j^*) = \sigma_j^*$. If we further suppose that the terms r_j^i are

equal to $v(b^i_j)$ for $i = 1, 2, 3, 4$ there is a shorter derivation of the sequent $U_j \longrightarrow \exists y \exists x P_j(x, y)$: First derive the six sequents

$$P_j(\sigma^*_j, \rho^*_j) \longrightarrow \exists y P_j(v(y), y)$$

$$P_j(t_{i_j}, a_{i_j}) \longrightarrow \exists y P_j(v(y), y)$$

$$P_j(r^i_j, b^i_j) \longrightarrow \exists y P_j(v(y), y).$$

This takes a total of six inferences and six logical axioms. Then use five $\vee$*:left* inferences to derive $U_j \longrightarrow \exists y P_j(v(y), y)$. Finally use the following four inferences and one logical axiom:

$$\dfrac{U_j \longrightarrow \exists y P_j(v(y), y) \qquad \dfrac{\dfrac{\dfrac{P_j(v(a), a) \longrightarrow P_j(v(a), a)}{P_j(v(a), a) \longrightarrow \exists x P_j(x, a)}}{P_j(v(a), a) \longrightarrow \exists y \exists x P_j(x, y)}}{\exists y P_j(v(y), y) \longrightarrow \exists y \exists x P_j(x, y)}}{U_j \longrightarrow \exists y \exists x P_j(x, y)}$$

where a is a free variable not occuring in t_{i_j}. This derivation of $U_j \longrightarrow \exists y \exists x P_j(x, y)$ contains 22 sequents, one less than the earlier derivation which had 23 sequents.

If the second-order unification has a solution, then by appropriate choices for the t_j's and r^i_j's, the formula Φ can be proved with a proof containing $(k + 4m + 1) + (3m - 3) + 22m = k + 29m - 2$ sequents. So we let N be $k + 29m - 2$; we need to show that if the unification problem has no solution then any proof of Φ requires at least $N + 1$ lines. (However, if there is a solution to all but one of the unification equations, Φ will have a proof of exactly $N + 1$ lines.)

Suppose P is a proof of Φ. We say that a term t *is assigned to* β_i *in* P if there is an inference in P of the form

$$\dfrac{A(t), \Gamma \longrightarrow \Delta}{(\forall \beta_i) A(\beta_i), \Gamma \longrightarrow \Delta}$$

such that there is a forward path from the s-formula $\forall \beta_i \cdots \forall \beta_k \bigwedge U_j$ in the endsequent to the $(\forall \beta_i) A(\beta_i)$ in the inference displayed above. We call such an inference a *term-assigning inference* and its lower sequent is called a *term-assigning sequent*. Of course, more than one t may be assigned to β_i in P.

By Propositions 7 through 9, P must contain at least one $\supset$*:right* inference, $k+4m$ $\forall$*:left* inferences, $m-1$ $\wedge$*:right* inferences, $2m-2$ $\wedge$*:left* inferences and $5m$ $\vee$*:left* inferences. Since any sequent is derived by a unique inference this accounts for $k+12m-2$ sequents in P. (Note that we also know there are at least $2m$ $\exists$*:left* inferences in P; however, these will be counted separately below.)

To further count sequents in P we will form $m+1$ disjoint classes $S_1, \ldots, S_m$ and XS of sequents such that no member of these classes is one of the $k+12m-2$ sequents already accounted for. Nor will these classes contain any term-assigning sequent. The idea is that S_j is the set of sequents used to handle the derivation of

$$U_j \longrightarrow \exists y \exists x P_j(x,y)$$

although, in general, the proof P might not actually contain this sequent. The set XS will be a set of "excess sequents".

Claim: *The classes $S_1, \cdots, S_m$ and XS can be defined so that the cardinality of each S_j is at least 17 and so that if each S_j has cardinality exactly 17 and if XS is empty then there are terms $t_1, \ldots, t_k$ assigned to $\beta_1, \ldots, \beta_k$ so that*

$$t_{i_j}(\rho_j^* /\!\!/ a_{i_j}) = \sigma_j^*$$

where ρ_j^* and σ_j^* are obtained from ρ_j and σ_j by replacing each β_i by t_i for all i.

Before proving the claim, lets show that it suffices to prove the Main Theorem 1. If the S_j's have cardinality 17 and are disjoint, the proof P has $(k+12m-2)+17m$ sequents which have already been accounted for or are in the S_j's. In order to have exactly $N = k+29m-2$ sequents this must be all of the sequents of P; this implies that there are no excess sequents and XS is empty and there is exactly one term assigned to β_i for each $i = 1, \ldots, k$. That is because no S_j contains a term-assigning sequent and we only counted one term-assigning inference for each value of i. Now, by the claim, the terms assigned to the β_i's provide a solution to the second-order unification problem. If, on the other hand, XS is nonempty or any S_j contains more than 17 sequents or any β_i is assigned more than one term, then P has more than N lines. Thus we have established that $\longrightarrow \Phi$ has a proof of $\leq N$ if and only if the unification problem has a solution.

It remains to prove the Claim. Fix for the moment a value for j. In Φ there are six atomic subformulas of the form $P_j(\cdots)$ on the lefthand side of the implication $\supset$ and only one on the righthand side. Let $v_1 = \sigma_j$, $w_1 = \rho_j$, $v_2 = \beta_{i_j}$, $w_2 = a_{i_j}$, $v_{2+i} = z^i_j$, $w_{2+i} = b^i_j$; so the six atomic subformulas on the right are $P_j(v_i, w_i)$ for $1 \leq i \leq 6$. (We are suppressing a second subscript, j, on the v's and w's to avoid excessive notation.) By Proposition 7, there exists at least one forward path from each $P_j(v_i, w_i)$ on the left to the $P_j(x, y)$ on the right. We are going to choose six forward paths π_i, for $i = 1, \ldots 6$, from the s-formula $P_j(v_i, w_i)$ to $P_j(x, y)$. These paths must satisfy the following three restrictions:

(R1) The initial parts of the paths $\pi_1, \ldots, \pi_6$ parallel each other for as long as possible — they diverge at $\vee$*:left* inferences.

(R2) If $P_j(\tau_i, \tau'_i) \vee \cdots \vee P_j(\tau_6, \tau'_6)$ is an s-formula that paths $\pi_i, \ldots, \pi_6$ $(i < 6)$ pass through while still paralleling each other then $\tau'_i, \ldots, \tau'_6$ are *distinct* semiterms.

(R3) It is not possible to replace any one of the six paths by a shorter path and still have conditions (R1) and (R2) hold.

It is not immediately obvious that there are paths that satisfy the three conditions; it will suffice to show that there are paths that fulfill conditions (R1) and (R2) since by shortening these paths one at a time until no further shortening is possible we obtain paths satisfying all three conditions.

Proposition 11 *Fix j and let P be a proof of Φ. In P's logical flow graph, there are six paths π_i from $P_j(v_i, w_i)$ to $P_j(x, y)$ that satisfy conditions (R1) and (R2).*

Proof As usual it will suffice to assume P is tree-like; otherwise, P may be transformed into a tree-like proof and paths in the logical flow graph of the tree-like proof can be mapped back to paths in P's logical flow graph. Suppose that there is no set of six paths that satisfy (R1) and (R2). We shall show below that there is an LK_e-proof P^* of the formula Φ^* obtained from Φ by replacing U_j either with $\top$ or with

$$\bigwedge_{1 \leq n < s \leq 6} w_n \neq w_s.$$

Recall that $w_2, \ldots, w_6$ are distinct free variables and $w_1 = \rho_j^*$ is distinct from them by the special restriction. Therefore, Φ^* is not valid and we have a contradiction. Thus our assumption that the six paths do not exist will be shown to be wrong. (Note that P^* is an LK_e-proof even though P may not involve identity.)

Consider the six subformulas

$$A_i \;=\; \bigvee_{n=i}^{6} P_j(v_n, w_n)$$

of U_j occurring in the endsequent of P. If B is an s-formula in P forward-reachable from A_i then B is of the form $\bigvee_{n=i}^{6} P_j(\tau_n, \tau'_n)$; we say that B is *R2-bad* if τ'_n and τ'_s are identical semiterms for some $n \neq s$. We say that a path in the logical flow graph is *R2-bad* if some s-formula on the path is R2-bad. And an s-formula B forward-reachable from some A_i is *R2-good* if and only if there is a path from A_i to B which is not R2-bad. (So R2-good is not the opposite of R2-bad.) An s-formula B is *R2-borderline* if it is R2-bad and there is an edge in the logical flow graph from an R2-good formula to B. An s-formula $P_j(—)$ is *viable* if there is a forward path from it to the $P_j(x, y)$ in the endsequent of P.

We modify P to form P^* by the following transformations:

(1) If B is a maximal s-formula forward-reachable from one of the A_i's such that one of B's disjuncts is not viable, replace B by $\top$.

(2) Any remaining non-viable s-formulas $P_j(—)$ are replaced by $\top$.

(3) Suppose that B is a maximal s-formula in P of the form

$$\bigvee_{n=i}^{6} P_j(\tau_n, \tau'_n)$$

with $i \leq 5$ and that B is not altered by (1) or (2). If B is not R2-good it is replaced by

$$B_{\text{bad}} \;=\; \left(\bigvee_{n=i}^{6} P_j(\tau_n, \tau'_n)\right) \wedge \left(\bigwedge_{i \leq n < s \leq 6} \tau'_n \neq \tau'_s\right),$$

and if B is R2-good it is replaced by $B_{\text{good}} = \bigwedge_{n<s} \tau'_n \neq \tau'_s$.

The first two transformations apply to meeting condition (R1); compare with the proof of Proposition 10. The third transformation is used to handle condition (R2). We now claim that P^* is a "proof" in that every inference in P^* is sound. There are several ways in which P^* can fail to be a valid LK_e-proof. Firstly, consider an inference in P of the form

$$\frac{P_j(\tau_i, \tau_i'), \Pi \longrightarrow \Lambda \qquad \bigvee_{i<n} P_j(\tau_n, \tau_n'), \Pi \longrightarrow \Lambda}{\bigvee_{i\leq n} P_j(\tau_n, \tau_n'), \Pi \longrightarrow \Lambda}$$

If $\bigvee_{i\leq n} P_j(\tau_n, \tau_n')$ was replaced by $\top$ in P^* then so is at least one of the indicated formulas in the upper sequents; thus this is a vacuous inference in P^* with one of the upper sequents equal to the lower sequent. The subproof of the other upper sequent can be ignored or discarded since P is tree-like. If $\bigvee_{i\leq n} P_j(\tau_n, \tau_n')$ is not R2-good then in P^* the inference is replaced by

$$\frac{P_j(\tau_i, \tau_i'), \Pi \longrightarrow \Lambda \qquad \left(\bigvee_{i<n} P_j(\tau_n, \tau_n')\right) \wedge \left(\bigwedge_{i<n<s} \tau_n' \neq \tau_s'\right), \Pi \longrightarrow \Lambda}{\left(\bigvee_{i\leq n} P_j(\tau_n, \tau_n')\right) \wedge \left(\bigwedge_{i\leq n<s} \tau_n' \neq \tau_s'\right), \Pi \longrightarrow \Lambda}$$

which is a sound "inference". And if $\bigvee_{i\leq n} P_j(\tau_n, \tau_n')$ is R2-good we must treat the cases $i < 5$ and $i = 5$ separately. For $i < 5$, we have that the inference becomes

$$\frac{P_j(\tau_i, \tau_i'), \Pi \longrightarrow \Lambda \qquad \bigwedge_{i<n<s} \tau_n' \neq \tau_s', \Pi \longrightarrow \Lambda}{\bigwedge_{i\leq n<s} \tau_n' \neq \tau_s', \Pi \longrightarrow \Lambda}$$

in P^*; this inference is sound (with the left upper sequent unnecessary for the soundness). If $i = 5$, then by our hypothesis that there are no paths satisfying (R1) and (R2) we must have that some s-formulas on the path from $P_j(v_6, w_6)$ to $P_j(\tau_6, \tau_6')$ were not viable. And because P is tree-like we were able to discard a subproof of P containing the inference under consideration; hence this inference is not needed in the proof P^*. Secondly, P^* will not be a correct proof at a sequent containing an R2-borderline formula; such a sequent must be the upper sequent of a quantifier inference that causes an R2-good formula in the lower sequent to become R2-bad in the upper

sequent. But the formula B_{bad} is actually equivalent to B_{good} when B is R2-bad, because two of the semiterms τ'_n, τ'_s are equal ($n \neq s$). Hence the "inference" in P^* is sound. Thirdly we have to consider contractions in P^* that may be contracting unequal formulas (this is similar to the proofs of Propositions 6-10). Contractions can occur explicitly in contraction inferences and implicitly in $\vee$*:left* and $\wedge$*:right* inferences. Suppose, for example, that P contains a contraction inference

$$\frac{\Pi \longrightarrow \Lambda, B_1, B_2}{\Pi \longrightarrow \Lambda, B_3}$$

where $B_1 = B_2 = B_3$ are three occurrences of the same formula. In P^* this becomes

$$\frac{\Pi^* \longrightarrow \Lambda^*, B_1^*, B_2^*}{\Pi^* \longrightarrow \Lambda^*, B_3^*}$$

Let C_1, C_2, C_3 be corresponding (equal) subformulas of B_1, B_2, B_3. Suppose each C_i is replaced by C_i^* in P^* with at least one $C_i \neq C_i^*$. If C_n occurs positively in B_n then there are edges in the logical flow graph from C_1 and from C_2 to C_3 and these are the only edges out of C_1 and C_2 (since P is tree-like) and the only edges into C_3. Thus C_3 is transformed to $\top$ by transformations (1) and (2) iff either (both) C_1 and C_2 is (are). Also if one of C_1 or C_2 is R2-good then C_3 is R2-good. If however, C_i is not R2-good we still have $LK_e \models (C_i)_{\text{bad}} \supset (C_3)_{\text{good}}$. In all cases we have that $LK_e \models C_i^* \supset C_3^*$ for $i = 1, 2$. On the other hand, if C_n occurs negatively in B_n then the directions of the edges in the logical flow graph are reversed. Thus if C_3 is tranformed to $\top$ by (1) or (2) then both C_1 and C_2 are. Also, C_3 is R2-good if and only if either (both) of C_1 and C_2 is (are). In any case, we have that $LK_e \models C_3^* \supset C_i^*$ for $i = 1, 2$. By repeating this analysis for all appropriate subformulas C_1, C_2, C_3 of B_1, B_2, B_3, we have that $LK_e \models B_1 \supset B_3$ and $LK_e \models B_2 \supset B_3$. Hence this contraction "inference" preserves validity and is sound.
Q.E.D. Proposition 11

Returning to the proof of our main theorem, we now need to establish the Claim. The general idea for proving the Claim is to attempt to associate three sequents in P with each path π_i. If we are able to do this then we have 18 sequents in S_j. However, we will not always be successful in finding three

sequents per path π_i — in these cases we must either associate more than three sequents with the other paths or find sequents which, although they can not be associated with just one of the paths, can be put in S_j. For example, we will often want to associate two sequents with each of the six paths and associate an additional five sequents with the paths as a group: this will yield 17 sequents in S_j.

Fix two values $1 \leq i < n \leq 6$ and consider π_i and π_n. Since π_i and π_n both end at the $P_j(x, y)$ in Φ, there must be an s-formula ψ which is the first one in the path π_i which is also in the path π_n. Since π_n is a shortest path (condition (R3)), ψ is in addition the first s-formula on π_n which is also on π_i. Furthermore, without loss of generality, π_i and π_n coincide from ψ onward. The s-formula ψ must be of the form $P_j(\tau_1, \tau_2)$ for some semiterms τ_1 and τ_2. There are several possibilities to consider:

Case (1): If ψ occurs as a subformula of the formula $(\exists y)(\exists x)P_j(x, y)$ then each path must contain two $\exists$*:right* inferences to introduce the two existential quantifiers. Furthermore, both paths must pass though at least one axiom of the form $P_j(\cdots) \longrightarrow P_j(\cdots)$ before the $\exists$*:right* inferences. This associates three inferences with each of π_i and π_n.

Case (2): Other cases where ψ is in the scope of two or more quantifiers are handled similarly.

Case (3): If ψ occurs as a subformula of a formula of the form $(\exists y)P_j(\tau, y)$ then by the reasoning above, each of π_i and π_n has two sequents associated with it; namely, a logical axiom and an $\exists$*:right* inference. We may assume that π_i and π_n are going downward as they reach ψ (otherwise there are *Cut* inferences on π_i and π_n where the paths turn upwards after going downward through the $\exists$*:right* inferences). Now we claim that there must be at five sequents on the paths after ψ before the endsequent Φ is reached. Namely, one *Cut* inference to turn the paths upward again, one $\exists$*:left* inference to strip off the $(\exists y)$, one axiom to turn the path downward and two $\exists$*:right* inference to put $(\exists y)(\exists x)$ on. However, these five inferences can not be associated with π_i and π_n separately but must be shared among all six paths.

We have argued that, in this case (3), each of π_i and π_n has two associated sequents and that there are five additional sequents which may be put into S_j. This counting of sequents is in fact optimal; furthermore, to achieve this small number of sequents either some sort of unification must occur or there are excess sequents we can put in XS. Indeed at the beginning of the path π_i is an s-formula $P_j(v_i, w_i)$ where v_i is a semiterm. Following (upwards) along π_i,

various $\forall$*:left* inferences assign terms $t_1, \ldots, t_m$ to $\beta_1, \ldots, \beta_m$ and assign terms to z_i^j's. We can assume that the process of $\forall$*:left* inferences assigning terms is uninterupted by any downward path segments and therefore uninterupted by any inferences which introduce a quantifier; otherwise, the logical axiom and the *Cut* inferences used to change the direction of the path and the lower sequent of any quantifier introduction inference can be put in XS. Eventually, the $\forall$*:left* term-assigning inferences transform v_i into a term v_i^* with no bound variables. A similar process gives v_n^*. Now there must be a common term $q(x)$ such that $q(w_i) = v_i^*$ and $q(w_n) = v_n^*$ if our lower bound on the number of sequents associated with π_i and π_n is be achieved. This is because only then can $\exists$*:right* inferences transform $P_j(v_i^*, w_i)$ and $P_j(v_n^*, w_n)$ into $(\exists y)P_j(\tau, y)$ — here τ will be $q(y)$. But because we are dealing with LK-proofs and there are no equality axioms, the only way to change a term is by quantifier inferences. The lower sequent of such quantifier inference can be put into XS. Thus we have shown that if S_j has cardinality 17 then either there are sequents we can put in XS or the term assignments along the initial part of π_i and π_n provide a solution to the unification equation $v_i(w_n/w_i) = v_n$.

Case (4): Other cases where ψ is $P_j(\tau, y)$ for y a bound variable are handled similarly.

Case (5): Finally we must consider the case where ψ is a (sub)formula of the form $P_j(\tau, t)$ where t is a term with no bound variables and τ is a semiterm which may in general contain variables bound in the formula in which ψ occurs. Since $w_i \neq w_n$ either w_i or w_n must have been changed along the path from $P_j(v_i, w_i)$ or $P_j(v_n, w_n)$; we shall show that at least four sequents can be associated with the change from w_i or w_n to t. Because π_i and π_n parallel each other for as long as possible (by condition (R1)), they will diverge at an $\vee$*:left* inference while travelling upwards. By condition (R2) at the $\vee$*:left* inference where the paths π_i and π_n diverge, the s-formulas are $P_j(v_i', w_i')$ and $P_j(v_n', w_n')$ with $w_i' \neq w_n'$. Hence one of w_i' or w_n' must be changed to t: this requires a logical axiom to change the path direction downward, an $\exists$*:right* or $\forall$*:left* inference to quantify the w_i or w_n, a *Cut* inference to turn back upwards, and another quantifier inference to remove the quantifier. (Here we use the fact that LK has no equality axioms.) These inferences and axiom give four sequents which can be associated with one of the paths and put into S_j.

The above concludes the analysis of the intersection of two paths π_i and π_n. This analysis actually needs to be performed five times to merge all six paths for atomic s-formulas involving P_j. This should be done by considering first intersections first (in order of travel along the paths). The result is that either (a) there are at least three sequents associated with each path or if case (5) applies each time there are four sequents associated with five of the paths, and hence there are ≥ 18 total sequents to put in S_j, or (b) each path has at least two associated sequents and there are five additional "shared" sequents. Also, if exactly 17 sequents are in S_j, case (b) holds and P contains a "solution" to $\beta_{i_j}(\rho_j /\!\!/ a_{i_j}) = \sigma_j$.

It may appear that the Claim is now proved; however, there is a small gap in our argument so far: we still need to show that the S_j's are disjoint. Unfortunately, the above argument does not work since the $\exists$*:right* inferences in case (1) above and the first $\exists$*:right* inference and the $\exists$*:left* of case (3) might be put into more than one S_j. For instance, it may be that in case (3) the s-formula ψ above occurs in a formula

$$(\exists z)(P_j(\tau, z) \vee P_{j'}(\tau', z))$$

with $j' \neq j$. And if the $P_{j'}(x, y)$ is a point where two paths for $P_{j'}(\cdots)$ merge then we will have put the $\exists$*:right* and $\exists$*:left* inferences which introduce and eliminate the $(\exists z)$ into both S_j and $S_{j'}$.

To fix this problem, we need to count the inferences which are necessary to introduce and eliminate the disjunction and put these into $S_{j'}$. Consider what happens along a path that leads to $P_{j'}(\tau', z)$. The path begins at the endsequent and must pass through an axiom of the form $P_{j'}(\cdots) \longrightarrow P_{j'}(\cdots)$ before reaching an $\vee$*:right* inference to introduce the disjunction. There is an additional $\vee$*:left* inference on each path leading to $P_j(\tau, z)$. This gives a total of three sequents which we can associate with the path leading to $P_{j'}(\tau', z)$ and which are put into $S_{j'}$. Note we haven't even counted inferences necessary to eliminate the disjunction.

A similar and slightly more complicated argument works for the implication connective ($\supset$) replacing $\vee$; we leave this to the reader.

The case where a conjunction links $P_j(\cdots)$ and $P_{j'}(\cdots)$ is similar but more complicated. First along a forward path leading to $P_{j'}(\tau', z)$ there is an axiom and an $\wedge$*:right* inference; this provides only two sequents to associate with the path and put into $S_{j'}$. To eliminate the conjunction

requires two $\wedge$*:left* inferences; there is also an axiom $P_{j'}(\cdots) \longrightarrow P_{j'}(\cdots)$ and two $\exists$*:right* inferences which introduce the quantifiers in the endsequent (i.e., in Φ). Furthermore, before the reaching the endsequent, the subformula $P_j(\tau, z) \wedge P_{j'}(\tau', z)$ must be split into two copies, one on the P_j-path and one on the $P_{j'}$-path (as in Proposition 9). Splitting into two can occur either (1) by a *contract:left* inference on an upward path, or (2) while on a downward path. The latter requires no extra inferences since it can be that the sequent is merely used twice as a hypothesis. However, in case (2), there are two *Cut* inferences required to turn upward towards the $\wedge$*:right* inferences (because both copies of the conjunction need to be handled with a $\wedge$*:left*).

Thus there are at least six inferences associated with eliminating the conjunction along the forward paths. These six sequents may be shared among the six paths for $P_{j'}$ and put into $S_{j'}$. Thus $S_{j'}$ will contain a total of 18 inferences.

So far we have discussed the very simple case of a formula with one binary connective linking two atomic subformulas $P_j(\cdots)$ and $P_{j'}(\cdots)$; however, in principle, arbitrary Boolean combinations of multiple predicates might occur. (Actually this will always be grossly inefficient, but we need merely find the requisite 18 sequents for each S_j.) Luckily, our technique extends to handling complicated formulas. In any Boolean formula with n atomic subformulas there are $n-1$ binary connectives. We set up a one-to-one correspondence between the binary connectives and $n-1$ of the atomic subformulas by assigning a given binary connective to the first atomic subformula of its second operand. Now in a proof P of the sequent $\longrightarrow \Phi$ if there is a formula with $n-1$ binary connective and n atomic subformulas, for each atomic subformula $P_{j'}(\cdots)$ associated with one of the binary connectives we find three sequents to associate with each path to the s-formula $P_{j'}(\cdots)$ by the analysis used above. For the one atomic subformula $P_j(\cdots)$ not associated with a binary connective we use the original analysis which found either 17 or 18 sequents to put in S_j.

That completes the proof of the Claim and of Main Theorem 1. It remains to prove the Main Theorem for LK_e, the logical calculus for first-order logic with equality.

Main Theorem 12 *Let LK_e be Gentzen's sequent calculus with the nonlogical equality symbol, a unary function symbol S, a binary function symbol and infinitely many unary relation symbols. For every recursively enumerable*

set X there is a formula $A(x)$ and an integer k such that for all n, $n \in X$ if and only if $\longrightarrow A(S^n0)$ has an LK_e-proof with $\leq k$ distinct sequents.

Proof The proof is almost exactly like the proof of Main Theorem 1 except we need to modify Φ somewhat so as to make sure that the equality axioms can't help prove Φ. What is done is replace every subformula of Φ of the form $P_j(—)$ by

$$(\cdots((P_j(—) \wedge \top) \wedge \top) \wedge \cdots \wedge \top).$$

where there are N disjunctions in this formula. (N is the same number as for the previous proof.) Since the equality axioms only apply to atomic formulas at least N $\vee$*:left* inferences would be needed to apply even one equality axiom to a formula containing a P_j.
Q.E.D. Main Theorem 12

The proof above for LK_e is somewhat unsatisfactory since it depends on the fact that equality axioms only apply to atomic formulas. It seems likely that the k-provability problem remains undecidable even for more general equality axioms. In connection with this let us state an open problem. Suppose a formula ϕ does not involve the equality symbol and has an LK_e-proof of k lines; does ϕ necessarily have a proof of $\leq k$ lines in which no equality symbol occurs?

5 Conclusion

Our proof of the undecidability of the k-provability problem for the sequent calculus depended of course on the details of the definition of the sequent calculus; however, it doesn't seem to exploit any unusual features of the sequent calculus. For LK_e, our proof did exploit the fact that equality axioms only apply to atomic formulas; however, this is a common feature of many systems of first-order logic. Thus it seems reasonable that our method of proof might work for other systems of first-order logic. The main proviso is that the system of first-order logic should have some general version of cut or modus ponens and substitution axioms; Farmer [1] has proved decidability results for first-order proof systems with restricted substitution axioms and Krajíček and Pudlák [6] show that the k-provability problem is decidable

for the cut-free sequent calculus. (Recall that substitution axioms are of the form $(\forall x)A \supset A(t/x)$; the $\forall$*:left* rule in the sequent calculus corresponds to the substitution axioms.) Another feature of the sequent calculus that our proof exploited is the fact that quantifier rules can only add or remove one quantifier at a time.

Our original motivation for looking at the k-provability problem was to approach Kreisel's problem. For this, we had hoped to show, for instance, that there is a formula $\phi(x)$ such that each $\phi(S^n 0)$ either has a proof of $\leq n$ lines or has no proof with $\leq 2^n$ lines and such that it is undecidable which case holds. Such a result would likely be very useful in extending the undecidability of k-provability to other systems of first-order logic. It should be noted that there is no hope of proving such a result with 2^n replaced by a function which grows faster than the superexponential function; this is because if there is a proof of n lines then there is a cut-free proof with number of lines bounded by a stack of $O(n)$ 2's and, as mentioned above, the k-provability problem for cut-free proofs is decidable.

References

[1] William M. Farmer. A unification-theoretic method for investigating the k-provability problem. Typewritten manuscript, January 1987.

[2] William M. Farmer. A unification algorithm for second order monadic terms. *Annals of Pure and Applied Logic*, 39:131–174, 1988.

[3] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[4] Warren D. Goldfarb. The undecidability of the second-order unification problem. *Theoretical Computer Science*, 13:225–230, 1981.

[5] Jan Krajíček. Generalizations of proofs. In *Proc. Fifth Easter Conference on Model Theory, Seminarberichte #93*, pages 82–99. Humboldt Universität, Berlin, 1987.

[6] Jan Krajíček and Pavel Pudlák. The number of proof lines and the size of proofs in first-order logic. *Archive for Mathematical Logic*, 27:69–84, 1988.

[7] Georg Kreisel. Proof theory: Some personal recollections. Appendix to [13].

[8] Tohru Miyatake. On the length of proofs in a formal system of recursive arithmetic. In *Logic Symposia, Hakone, Lecture Notes in Mathematics #891*, pages 81–108. Springer-Verlag, 1980.

[9] Tohru Miyatake. On the length of proofs in formal systems. *Tsukuba Journal of Mathematics*, 4:115–125, 1980.

[10] V. P. Orevkov. Reconstruction of a proof from its scheme. *Soviet Mathematics Doklady*, 35:326–329, 1987. Original Russian version in Dokl. Akad. Nauk. **293** (1987) 313-316.

[11] Rohit J. Parikh. Some results on the lengths of proofs. *Transactions of the American Mathematical Society*, 177:29–36, 1973.

[12] Daniel Richardson. Sets of theorems with short proofs. *Journal of Symbolic Logic*, 39:235–242, 1974.

[13] Gaisi Takeuti. *Proof Theory.* North-Holland, second edition, 1987.

[14] Tsuyoshi Yukami. A theorem on the formalized arithmetic with function symbols $'$ and $+$. *Tsukuba Journal of Mathematics*, 1:195–211, 1977.

[15] Tsuyoshi Yukami. A note on a formalized arithmetic with function symbols $'$ and $+$. *Tsukuba Journal of Mathematics*, 2:69–73, 1978.