Annals of Mathematical Logic 15 (1978) 225–287

BOUNDS FOR PROOF-SEARCH AND SPEED-UP IN THE PREDICATE CALCULUS

Richard STATMAN
The University of Michigan, Ann Arbor, MI, U.S.A.

Received 9 March 1976

Preface

This work is based on research done by the author as a graduate student at Stanford University and as the Berry–Ramsey Fellow of King's College, Cambridge (1973–1975). The organization of the work is based on lectures given at Oxford in Michaelmas term 1975.

The work is not self-contained and references are provided at the end (unpublished references are not necessary for understanding the main body of text). In particular, the reader is assumed to be familiar with current proof-theory (although it is not necessary that he be sympathetic with its aims).

The author would like to thank Professor Kreisel, who is responsible for most of whatever virtues this work may have (the author must take full responsibility for its defects). The author would also like to thank Professor Mints of the Steklov Institute and Professor Troelstra of the University of Amsterdam for their advice and encouragement.

Finally, the author would like to thank King's College, Cambridge, for providing the time (= money) for the author to carry out his research. Special thanks go to Professor Williams.

0. Introduction

This paper consists of a study of the elementary properties of the relation

$$\vdash^{n}_{S} A$$

$=_{\mathrm{df}}$ there is a derivation of the formula A in the formal system S of length $\leqslant n$, where the length of a derivation is its number of inferences (lines). In particular, we are interested in two kinds of questions:

(1) Proof-search. Given a notion of validity Val for the language of A, is there a function m such that

$$\mathrm{Val}(A) \Rightarrow \vdash^{m(\mathrm{lh}(A))}_{S} A$$

where the length of A is its number of symbols, and if so how fast must such an m grow?

(2) Speed-up. Given a system $S^* \supseteq S$, is there a function m such that

$$\vdash^{n}_{S^*} A \Rightarrow \vdash^{m(n)}_{S} A$$

and if so how fast must such an m grow?

Our principal results will be stated for the language of predicate logic (including type theory without the axioms of choice or infinity) and systems of natural deduction (along with sequential variants of these systems). Systems of natural deduction, first introduced by Gentzen in 1935, lend themselves to our study for several reasons:

(1) Each natural deduction has the same structure as some informal description of the proof it represents (for some case by case verification of this the reader should consult [8, Chapter 4, II.1–II.5]. Thus, pending completeness considerations, structural results about natural deductions have a natural interpretation in terms of intelligibility of proofs.

(2) Generally speaking, natural deductions are shorter than their counterparts in other "schematic" calculi (however, it turns out that most of the bounds established below for systems of natural deduction would have the same order of magnitude if other systems were used).

(3) Natural (deduction) rules represent thoroughly analyzed inferences. This means that length is a significant measure of structural complexity.

(4) Systems of natural deduction admit a relatively simple analysis of the notion of identify of structure between derivations (see 4.2.4).

Section 1 gives upper bounds for proof-search in the equation calculus (sequential rules + cut) based on a proof-search procedure due to Tait. In addition, this chapter contains an analysis of equational derivations (natural rules) after the style of Gentzen's cut-elimination argument. This analysis is applied to obtain upper bounds for speed-up by the sequential rules + cut over the rules without cut and certain auxiliary results which will be used in later sections. For connections to computational complexity the reader should refer to Kozen [15], and Statman [33, 37, 35].

Section 2 gives upper and lower bounds for proof-search in the propositional calculus (sequential rules − cut). In addition, it contains lower bounds for speed-up by the sequential rules + cut over the rules without (upper bounds are given in Section 4). For connections to computational complexity the reader should refer to Cook [3], Cook and Reckhow [4], and Statman [34, 35].

Section 3 considers proof-search in the predicate calculus. An upper bound for the monadic case (sequential rules − cut) is obtained by formalization of the usual decision procedure and application of the standard bounds for cut-elimination. In addition, the Turning degree of optimal proof-search bounds for the general case is computed to be $0'$.

Section 4 gives upper and lower bounds for speed-up by the predicate calculus (without equality) over the propositional calculus. The upper bound is obtained by combining the bounds of Section 2 with the following observation; there is a function m such that $\vdash^{n}_{N_1} A \Rightarrow$ there is a valid B of logical complexity $\leq m(n)$ such that A is a substitution instance of B.

Section 5 presents upper and lower bounds for speed-up by the predicate calculus with equality over the equation calculus (for equational theories a la Herbrand's theorem). The upper bound is obtained by analyzing Prawitz style normalization, and the lower bound is obtained for a fixed equational theory by making use of a result of Hindley and an idea of Tait. In addition, the chapter contains upper and lower bounds for speed-up by the sequential rules for the predicate calculus without equality + cut over the rules without.

In Section 6 we prove the existence of bounds for proof search in and speed-up by (over first-order logic, with and without equality) second-order logic (with and without equality). The existence of bounds for speed-up is obtained by analyzing a Prawitz style normalization procedure for second-order logic (here the reader should note that [30, B.3] is in error). The section also contains lower bounds for speed-up.

Section 7 considers proof-search in and speed-up by the theory of types without choice and infinity. It is shown that there are no bounds for proof-search even for (higher type) propositional formulae, and there are no bounds for speed-up even for quantifier-free formulae (over the propositional calculus). In addition, it is shown that there are no bounds for speed-up by the theory of types with equality over the equation calculus (for equational theories a la Herbrand's theorem). Thus the theory of types constitutes an upper bound for the kind of work done in Sections 1–6.

1. Proof-search in the equation calculus

1.1. *Preliminaries*

1.1.1. We consider equations E between individual terms $a, b, d, e, \ldots$, built up from constants $c, \ldots$, parameters $u, v, \ldots$, and function symbols $f, g, h, \ldots$. We write $\mathrm{Sub}^{a_1 \cdots a_n}_{u_1 \cdots u_n}$ for the operation of simultaneously substituting a_i for u_i.

1.1.2. A function m from terms to non-negative integers is called a pre-measure if $m(a) \leq m(b) \Rightarrow m(\mathrm{Sub}^{a}_{u}\, d) \leq m(\mathrm{Sub}^{b}_{u}\, d)$ and whenever u occurs in d we have $m(a) \leq m(\mathrm{Sub}^{a}_{u}\, d)$.

m is a measure if $m(\mathrm{Sub}^{a}_{u}\, d) = m(d) - m(u)k + m(a)k$ for u occuring k times in d.

1.1.3. If m is a pre-measure and θ a substitution, then m_θ is the pre-measure defined by $m_\theta(a) = m(\theta a)$.

1.1.4. If m is a measure we define the linear form l_m^a as follows;

$$l_m^u = u,$$
$$l_m^c = m(c),$$
$$l_m^{fa_1\cdots a_n} = m(fv_1\cdots v_n) - \sum_{1\le i\le n} m(v_i) + \sum_{1\le j\le n} l_m^{a_j},$$

so if a contains just the parameters $u_1\cdots u_n$, then $l_m^a = l_m^a(u_1,\ldots,u_n)$ and $m(\mathrm{Sub}_{u_1\cdots u_n}^{a_1\cdots a_n} a) = l_m^a(m(a_1),\ldots,m(a_n))$.

In addition we set $m(a=b) =_{\mathrm{df}} m(a)+m(b)$ and $m(F) =_{\mathrm{df}} \sum_{E\in F} m(E)$ for F a finite set of equations. Finally if $m>0$ we define m^* by

$$m^*(a=b) = \max\{m(a)/m(b), m(b)/m(a)\}$$

and set $m^*(F) =_{\mathrm{df}} \max\{m^*(E) : E\in F\}$.

1.1.5. If F is a finite set of equations, then $\mathrm{Sub}\,F$ is the set of all substitution instances of members of F.

1.1.6. F is called simple if each equation in it has one of the forms;

$$u=v, \qquad u_{n+1} = fu_1\cdots u_n, \quad \text{or} \quad u=c.$$

1.1.7. F is called symmetric if each equation in it contains only parameters which occur on both sides (i.e. each model M of F can be extended to a model M^+ of F by the addition of a single element ω so that ω is a fixed point of each function explicitly definable from parameters in M^+).

1.1.8. The calculus NE (natural rules for equality) consists of the axioms $a=a$ and the rule of substituting equals for equals

$$(=) \qquad \frac{\mathrm{Sub}_u^a E \qquad a \ominus b}{\mathrm{Sub}_u^b E}$$

where $a\ominus b$ is, ambiguously, $a=b$ and $b=a$.

NE-derivations D are binary trees of equation occurrences built up from assumptions and axioms by the rule $(=)$.

1.1.9. The calculus SE (sequential rules for equality) has as its deducible objects sequents of the form $F\vdash E$. It consists of the axioms $F\vdash a=a$ and the rules

$$(=) \qquad \frac{\mathrm{Sub}_u^a F\vdash \mathrm{Sub}_u^a E}{\{a\ominus b\}\cup \mathrm{Sub}_u^b F\vdash \mathrm{Sub}_u^b E},$$

$$(\mathrm{cut}) \qquad \frac{F_1\vdash E_2 \qquad \{E_2\}\cup F_2\vdash E_1}{F_1\cup F_2\vdash E_1}.$$

SE-derivations D are binary trees of sequent occurrences built up from axioms by the rules $(=)$ and (cut).

1.1.10. If S is a set of equations, then "$S \vdash^{n}_{\mathrm{NE}} E$" means that there is an NE-derivation of E from S of length $\leqslant n$ and "$S \vdash^{n}_{\mathrm{SE}} E$" means that there is an SE-derivation of $F \vdash E$ of length $\leqslant n$ for F some finite subset of S

1.2. *Normal forms*

1.2.1. An NE-derivation is said to be pre-singular if each of its $(=)$ inferences

$$\frac{\mathrm{Sub}^{a}_{u}\,E \qquad a \ominus b}{\mathrm{Sub}^{b}_{u}\,E} \tag{1}$$

has the form

$$\frac{(\mathrm{Sub}^{a}_{u}\,d) = e \qquad a \ominus b}{(\mathrm{Sub}^{b}_{u}\,d) = e} \quad \text{(left)}, \tag{2}$$

or the form

$$\frac{d = (\mathrm{Sub}^{a}_{u}\,e) \qquad a \ominus b}{d = (\mathrm{Sub}^{b}_{u}\,e)} \quad \text{(right)}. \tag{3}$$

The derivation is said to be singular if each of its $(=)$ inferences (1) has u occurring exactly once in E.

1.2.2. An NE-derivation of $a_1 = a_n$ from F is called a computation if it has the form

$$\frac{a_1 = a_1 \qquad E_1}{a_1 = a_2}$$

$$\cdot \quad \cdot \quad \cdot$$

$$\frac{a_1 = a_{n-1} \qquad E_{n-1}}{a_1 = a_n}$$

with each E_i in F.

1.2.3. Proposition. *If D is a pre-singular NE-derivation of E from F, then there is a computation of E from F of length* $\leqslant \mathrm{lh}(D) + 1$.

Proof. Given a pre-singular NE-derivation D, a switch is a replacement of a subderivation

$$\dfrac{\dfrac{\begin{matrix} D_1 \\ \mathrm{Sub}^{a,b}_{u,v}\,E \end{matrix} \qquad \begin{matrix} D_2 \\ a \ominus e \end{matrix}}{\mathrm{Sub}^{e,b}_{u,v}\,E} \qquad \begin{matrix} D_3 \\ b \ominus d \end{matrix}}{\mathrm{Sub}^{e,d}_{u,v}\,E} \quad \text{by} \quad \dfrac{\dfrac{\begin{matrix} D_1 \\ \mathrm{Sub}^{a,b}_{u,v}\,E \end{matrix} \qquad \begin{matrix} D_3 \\ b \ominus d \end{matrix}}{\mathrm{Sub}^{a,d}_{u,v}\,E} \qquad \begin{matrix} D_2 \\ a \ominus e \end{matrix}}{\mathrm{Sub}^{e,d}_{u,v}\,E}$$

and a shift is a replacement of a subderivation

$$\dfrac{\begin{array}{c}D_1\\ \mathrm{Sub}_u^a E\end{array} \qquad \dfrac{\begin{array}{c}D_2\\ a \ominus \mathrm{Sub}_v^b e\end{array} \qquad \begin{array}{c}D_3\\ b \ominus d\end{array}}{a \ominus \mathrm{Sub}_v^d e}}{\mathrm{Sub}_u^{\mathrm{Sub}_v^d e} E}$$

by

$$\dfrac{\dfrac{\begin{array}{c}D_1\\ \mathrm{Sub}_u^a E\end{array} \qquad \begin{array}{c}D_2\\ a \ominus \mathrm{Sub}_v^b e\end{array}}{\mathrm{Sub}_u^{\mathrm{Sub}_v^b e} E} \qquad \begin{array}{c}D_3\\ b \ominus d\end{array}}{\mathrm{Sub}_u^{\mathrm{Sub}_v^d e} E}$$

or

$$\dfrac{\begin{array}{c}D_1\\ \mathrm{Sub}_v^{\mathrm{Sub}_u^a b} E\end{array} \qquad \dfrac{\begin{array}{c}D_2\\ (\mathrm{Sub}_u^e b) \ominus d\end{array} \qquad \begin{array}{c}D_3\\ e \ominus a\end{array}}{(\mathrm{Sub}_u^a b) \ominus d}}{\mathrm{Sub}_v^d E}$$

by

$$\dfrac{\dfrac{\begin{array}{c}D_1\\ \mathrm{Sub}_v^{\mathrm{Sub}_u^a b} E\end{array} \qquad \begin{array}{c}D_3\\ a \ominus e\end{array}}{\mathrm{Sub}_v^{\mathrm{Sub}_u^e b} E} \qquad \begin{array}{c}D_2\\ (\mathrm{Sub}_u^e b) \ominus d\end{array}}{\mathrm{Sub}_v^d E}$$

A move is a switch or a shift, and we say that D_1 reduces to D_2 if D_2 results from D_1 by a sequence of moves.

Let D be a pre-singular NE-derivation; first we show that D reduces to a derivation of the form

$$\dfrac{a_n = b_m \qquad E_1}{a_{n-1} = b_m}$$

$$\vdots$$

$$(*) \qquad \dfrac{\dfrac{a_2 = b_m \qquad E_{n-1}}{a_1 = b_m} \qquad E_n}{a_1 = b_{m-1}}$$

$$\ddots$$

$$\dfrac{a_1 = b_2 \qquad E_{n+m-2}}{a_1 = b_1}$$

Measure the "leftness" of D by the k-tuple $(j_1, \ldots, j_k)$ where j_i is the length of the ith maximal path, from left to right, in D, and order these lexicographically. The maximum value for the leftness of a derivation of length l is $((l+1)/2, (l+1)/2, (l+1)/2-1, \ldots, 2)$, a shift is applicable to any pre-singular derivation which does not take on this value, and shifts increase leftness. Thus D reduces to a derivation of maximum leftness for its length. The desired derivation $(*)$ is obtained from this reduct by applying switches until no right inference preceeds a left inference.

Now suppose that D is a pre-singular derivation of E from F, and D reduces to $(*)$. W.l.o.g. assume that each E_i belongs to F. If a_n is b_m, then the desired computation is

$$\frac{a_1 = a_1 \qquad E_{n-1}}{a_1 = a_2}$$

$$\vdots$$

$$\cfrac{\cfrac{a_1 = a_{n-1} \qquad E_1}{a_1 = a_n} \qquad E_n}{a_1 = b_{m-1}}$$

$$\vdots$$

$$\frac{a_1 = b_2 \qquad E_{n+m-2}}{a_1 = b_1}$$

Otherwise the desired computation is

$$\frac{a_1 = a_1 \qquad E_{n-1}}{a_1 = a_2}$$

$$\vdots$$

$$\cfrac{\cfrac{\cfrac{a_1 = a_{n-1} \qquad E_1}{a_1 = a_n} \qquad a_n = b_m}{a_1 = b_m} \qquad E_n}{a_1 = b_{m-1}}$$

$$\vdots$$

$$\frac{a_1 = b_1 \qquad E_{n+m-2}}{a_1 = b_1}$$

1.3. *Symmetric equations*

1.3.1. For what follows we refer the reader to Kreisel and Tait [21]. $\forall F$ is the set of universal closures of members of F.

Proposition. *Suppose that F is symmetric, containing at most the constant 0 and the function symbols $s, h, h_1, \ldots, h_n$, and*

(i) *$\forall F$ is satisfiable over the set of natural numbers with 0 denoting zero and s the successor function,*

(ii) *h is NE-reckonable from F and* $\text{Sub}\, F \vdash_{\text{NE}} h0 = 0$; *let f and g be new unary function symbols and set* $F^+ =_{\text{df}} F \cup \{g0 = 0,\ gsu = gu,\ f0 = 0,\ fsu = fghu\}$ *then if* $\text{Sub}\, F^+ \vdash^{l}_{\text{NE}} f(s^{m+1}0) = 0$ *and* $\text{Sub}\, F \vdash_{\text{NE}} h(s^m 0) = s^l 0$ *we have* $l \leqslant m$.

Proof. Let val be the valuation function for closed terms determined by some interpretation over the set of natural numbers (with 0 denoting zero and s the successor function) satisfying $\forall F$, and let G be a closed finite subset of $\text{Sub}\, F^+$ such that $G \vdash_{\text{NE}} f(s^{m+1}0) = 0$; by Proposition 1.2.3 there is a computation of $f(s^{m+1}0) = 0$ from G of the form

$$\frac{f(s^{m+1}0) = a_1 \qquad E_1}{f(s^{m+1}0) = a_2}$$

$$\vdots$$

$$\frac{f(s^{m+1}0) = a_{l-1} \qquad E_{l-1}}{f(s^{m+1}0) = a_l}$$

where a_1 is $f(s^{m+1}0)$ and a_l is 0. Define $o(b)$ for b a closed term as follows; if b is fa and $\text{val}\,(a) = j$, then $o(b) = \text{val}\,(h(s^{j+1}0))$, if b is ga, then $o(b) = \text{val}(a)$, otherwise $o(b) = 0$. Let $o(i) =_{\text{df}} \max\,\{o(b) : b \text{ occurs in } a_i\}$ and suppose that $o(i+1) < o(i)$; consider the ith inference

$$\frac{f(s^{m+1}0) = \text{Sub}_u^{\text{Sub}_{v_1 \cdots v_n}^{b_1 \cdots b_n} a}\, d \qquad (\text{Sub}_{v_1 \cdots v_n}^{b_1 \cdots b_n} a) \ominus (\text{Sub}_{v_1 \cdots v_n}^{b_1 \cdots b_n} b)}{f(s^{m+1}0) = \text{Sub}_u^{\text{Sub}_{v_1 \cdots v_n}^{b_1 \cdots b_n} b}\, d}$$

where $a \ominus b$ belongs to F^+. If t occurs in a_i with $o(t) = o(i)$, then t begins with f or g so by the symmetry of F and (ii) $a \ominus b$ is either $gsu = gu$ or $fsu = fghu$ ($n = 1$ and v_1 is u).

Case 1: Suppose that E_i is $gsb_1 = gb_1$, then t is gsb_1 and $o(i+1) = o(i) - 1$.

Case 2: Suppose that E_i is $fsb_1 = fghb_1$, then $o(i+1) = o(i)$ which contradicts the choice of i.

Thus for each $1 \leqslant j \leqslant \text{val}\,(h(s^m 0))$ there is an equation $gsa = ga$ in G such that $\text{val}\,(sa) = j$; hence, $\text{card}\,(G) \geqslant \text{val}\,(h(s^m 0))$.

1.3.2. Proposition. *Suppose that F is symmetric and $F \cup \{E\}$ contains only unary function symbols; let no term in $F \cup \{E\}$ have length $>k$, then if* $\text{Sub}\, F \vdash_{\text{NE}} E$ *there is a finite subset G of* $\text{Sub}\, F$ containing no term of length $>k \cdot (2^n + 1)$ *with* $G \vdash_{\text{NE}} E$.

Proof. Suppose $\text{Sub}\, F \vdash^{n}_{\text{NE}} E$, then there is a pre-singular NE-derivation of E from $\text{Sub}\, F$ of length $\leqslant 2^n$. Thus by Proposition 1.2.3 there is a computation of E from $\text{Sub}\, F$ of length $\leqslant 2^n + 1$. Since $F \cup \{E\}$ contains only unary function symbols this computation is w.l.o.g. singular. It follows easily that no term occurring in this computation has length $>k \cdot (2^n + 1)$.

1.3.3. Lemma. *Suppose $m>0$ is a measure, then $F \vdash^{n}_{\mathrm{NE}} E \Rightarrow m^*(E) \leq m^*(F)^{2n+1}$.*

Proof. By induction on n.

Basis: trivial.

Induction step: suppose that $D=$

$$\frac{\begin{array}{cc} D_1 & D_2 \\ \mathrm{Sub}^a_u(d=e) & a \ominus b \end{array}}{\mathrm{Sub}^b_u(d=e)}$$

is an NE-derivation of E from F of length $\leq n$. Let u occur in d k times and in e l times, and w.l.o.g. suppose that $m(\mathrm{Sub}^b_u d) \geq m(\mathrm{Sub}^b_u e)$.

Case 1: $m(a) \leq m(b)$. If $k=0$ the case is trivial so assume $k \neq 0$. We have

$$m(\mathrm{Sub}^a_u d)/m(\mathrm{Sub}^a_u e) = [(m(d)-m(u)\cdot k)/m(\mathrm{Sub}^a_u e)] + [m(a)\cdot k/m(\mathrm{Sub}^a_u e)] \leq m^*(F)^{\mathrm{lh}(D_1)\cdot 2+1}$$

and

$$m(b)k/m(a)\cdot k \leq m^*(F)^{\mathrm{lh}(D_2)\cdot 2+1}.$$

Thus

$$m(b)k/m(\mathrm{Sub}^a_u e) \leq m^*(F)^{\mathrm{lh}(D)\cdot 2}$$

so

$$m(\mathrm{Sub}^b_u d)/m(\mathrm{Sub}^a_u e) \leq m^*(F)^{\mathrm{lh}(D)\cdot 2+1}$$

which gives the desired inequality since $m(\mathrm{Sub}^a_u e) \leq m(\mathrm{Sub}^b_u e)$.

Case 2: $m(b) < m(a)$. If $l=0$ the case is trivial so suppose $l \neq 0$. We have

$$m(a)\cdot l/m(b)\cdot l \leq m^*(F)^{\mathrm{lh}(D2)\cdot 2+1}$$

hence

$$m(\mathrm{Sub}^b_u e) \geq [(m(e)-m(u)\cdot l)/(m^*(F)^{\mathrm{lh}(D_2)\cdot 2+1})] + [m(a)\cdot l/(m^*(F)^{\mathrm{lh}(D_2)\cdot 2+1})]$$

so

$$m(\mathrm{Sub}^a_u d)/m(\mathrm{Sub}^b_u e) \leq m^*(F)^{\mathrm{lh}(D_2)\cdot 2+1}\, m(\mathrm{Sub}^a_u d)/m(\mathrm{Sub}^a_u e) \leq m^*(F)^{\mathrm{lh}(D)2}$$

which gives the desired inequality since $m(\mathrm{Sub}^b_u e) \leq m(\mathrm{Sub}^a_u e)$.

Proposition. *Suppose F is symmetric, then there is a k s.t.*

$$\mathrm{Sub}\, F \vdash^{n}_{\mathrm{NE}} E \Rightarrow \mathrm{lh}^*(E) \leq k^{2n+1}.$$

Proof. For each $a=b$ in F the function $\max\{l^a_{\mathrm{lh}}/l^b_{\mathrm{lh}}, l^b_{\mathrm{lh}}/l^a_{\mathrm{lh}}\}$ is bounded. The proposition follows from the lemma.

1.3.4. For what follows we refer the reader to Hindley [11–13]. We consider here only terms built up from the constants S, B, C, I, P, Q, 0 and 1, parameters, and the binary function symbol ( ). Terms written as a concatenation of constants and parameters are to be associated by ( ) to the left. Let $CL =_{\mathrm{df}} \{Su_1u_2u_3 = ((u_1u_3)(u_2u_3)),\ Bu_1u_2u_3 = (u_1(u_2u_3)),\ Cu_1u_2u_3 = ((u_1u_3)u_2),\ Iu = u\}$ and set $F =_{\mathrm{df}} \{Pu = (P(Qu))\}$. Let $T =_{\mathrm{df}} ((SB)((CB)I))$, set $T_1 =_{\mathrm{df}} T$ and put $T_{n+1} =_{\mathrm{df}} (T_nT)$. Let E_n be the equation $PQ = (P((T_nQ)Q)$. The equations in CL correspond in an obvious way to axiom schemes which define a reducibility relation enjoying the Church–Rosser property. The phrase "CL-normal form" has the obvious meaning.

Lemma. *Suppose that G is a closed finite subset of* Sub F *such that* $G \cup$ Sub $CL \vdash_{\mathrm{NE}} E_n$, *then there is a closed finite subset H of* Sub F *s.t.* $H \cup$ Sub $CL \vdash_{\mathrm{NE}} E_n$, card $(H) \leq$ card (G), *and each term occurring in H is in CL-normal form.*

Proof. Observe first that if u occurs in b

(i) $\mathrm{Sub}_u^{(Pa)}\, b$ has a CL-normal form $\Rightarrow$ (Pa) has a CL-normal form, and

(ii) $\mathrm{Sub}_u^{(Pa)}\, b$ has a CL-normal form $\Leftrightarrow$ $\mathrm{Sub}_u^{(P(Qa))}\, b$ has a CL-normal form.

If $G \cup \mathrm{Sub}\, CL \vdash_{\mathrm{NE}} E_n$, then by Proposition 1.2.3 there is a computation of E_n from $G \cup \mathrm{Sub}\, CL$ of the form

$$\frac{PQ = a_1 \qquad E^1}{PQ = a_2}$$

$$\vdots$$

$$\frac{PQ = a_l \qquad E^l}{PQ = a_{l+1}}$$

where a_{i+1} is different from a_i. Since a_1 and a_{l+1} have CL-normal forms it follows from (ii) and the Church–Rosser theorem that each a_i has a CL-normal form. Thus for each E^i of the form $Pa = (P(Qa))$ the term a has a CL-normal form by (i) (and (ii)).

Let the function 2_m^n be defined by the recursion equations $2_1^n = 2^n$, and $2_{m+1}^n = 2^{2_m^n}$.

Lemma. *Suppose G is a closed finite subset of* Sub F *such that each term occurring in G is in CL-normal form and* $G \cup$ Sub $CL \vdash_{\mathrm{NE}} E_n$, *then* card $(G) \leq 2_n^1/2$.

Proof. Suppose that $G = \{Pa_i = (P(Qa_i)) : 1 \leq i \leq m < 2_n^1/2\}$; let $Q^1 =_{\mathrm{df}} Q$ and $Q^{i+1} =_{\mathrm{df}} (QQ^i)$, then for some $1 < k \leq 2_n^1 + 1$ for each $1 \leq i \leq m$ neither a_i nor (Qa_i) is Q^k. We now define a certain extention CL^+ of CL. CL^+ is obtained from CL by adding the (infinitely many) equations corresponding to the following axioms;

if a is a closed term in Cl-normal form without P in function position, then

$(PA) \trianglerighteq 0$ if a is Q^j for $j<k$, and
$(Pa) \trianglerighteq 1$ otherwise.

By [13, Theorem 3], CL^+ has the Church–Rosser property; thus $\mathrm{Sub}\, CL^+ \vdash_{\overline{\mathrm{NE}}} 0=1$. Let E_n^+ be the equation $PQ=(PQ^{2^1_n+1})$, then $\mathrm{Sub}\, CL^+ \vdash_{\overline{\mathrm{NE}}} E_n^+$ so since $(PQ^{2^1_n+1})$ is the Cl-normal form of $(P((T_nQ)Q)$ we have $\mathrm{Sub}\, CL^+ \vdash_{\overline{\mathrm{NE}}} E_n$.
It suffices to show that $\mathrm{Sub}\, CL^+ \vdash_{\overline{\mathrm{NE}}} Pa_i = (P(Qa_i))$ for $1 \leqslant i \leqslant m$.

Case 1: Suppose that a_i does not contain P in function position. Either a_i is not of the form Q^j for any j so Pa_i, $(P(Qa_i)) \trianglerighteq 1$, or a_i is Q^j and $j, j+1<k$ so Pa_i, $(P(Qa_i)) \trianglerighteq 0$ or $k<j, j+1$ so Pa_i, $(P(Qa_i)) \trianglerighteq 1$.

Case 2: Suppose that a_i contains P in function position. a_i has a CL^+-normal form containing 0 or 1 and without P in function position so Pa_i, $(P(Qa_i)) \trianglerighteq 1$.

Finally we obtain the

Proposition. $\mathrm{Sub}\,(CL \cup F) \vdash^{m}_{\overline{\mathrm{NE}}} E_n \Rightarrow m \geqslant 2^1_n/2$.

1.4. Speed-up

1.4.1. A linear derivation of E from S is a sequence

$$\begin{array}{l} E_1 \\ \cdot \\ \cdot \\ \cdot \\ E_n \end{array}$$

such that each E_i is an axiom of the form $a=a$, a member of S, or follows from some E_j and E_k for $1 \leqslant j, k<i$ by the rule $(=)$, and E_n is E.

1.4.2. Lemma. *If there is a linear derivation of E from S of length $\leqslant n$, then there is a pre-singular* NE*-derivation of E from S of length $\leqslant 4^n - 1$.*

Proof. If there is a linear derivation of E from S of length $\leqslant n$, then there is a "pre-singular" one of length $\leqslant 2n$. Consider this linear derivation as an acyclic digraph on its equation occurrences, and select a maximal subgraph with some occurrence of E as a sink. The tree of paths to the sink in this subgraph (with the obvious adjacency relation) gives the desired NE-derivation.

1.4.3. Lemma. *If there is a pre-singular* NE*-derivation of E from F of length $\leqslant n$, then there is a cut-free* SE*-derivation of $F \vdash E$ of length $\leqslant n+1$.*

Proof. If there is a computation of E from F of length $\leqslant n$, then there is a cut-free SE-derivation of $F \vdash E$ of length $\leqslant n$. Now apply Proposition 1.2.3.

1.4.4. Lemma. *$F \vdash^{n}_{SE} E \Rightarrow$ there is a linear derivation of E from F of length $\leq n \cdot (n+1)/2$.*

Proof. Let D be an SE-derivation of $F \vdash E$. We construct an SE-derivation D^- of $F^- \vdash E$, for F^- a subset of F of cardinality $\leq \text{lh}(D)$, of length $\leq \text{lh}(D)$ by recursion as follows:

Basis: $D = F \vdash a = a$. Set $D^- =_{df} \emptyset \vdash a = a$.

Induction step: Suppose $D =$

$$\frac{\text{Sub}^a_u G \vdash \text{Sub}^a_u E'}{\{a \ominus b\} \cup \text{Sub}^b_u G \vdash \text{Sub}^b_u E'}.$$

By induction hypothesis we have a

$$\begin{array}{c} D_1^- \\ (\text{Sub}^a_u G)^- \vdash \text{Sub}^a_u E'; \end{array}$$

let $H =_{df} (\text{Sub}^a_u G)^- \cap (\text{Sub}^a_u G - \text{Sub}^b_u G)$, then each E'' in H has the form $\text{Sub}^a_u E'''$ for $\text{Sub}^b_u E'''$ in $\text{Sub}^b_u G$ (this representation may not be unique). Thus there is a J such that $H = \text{Sub}^a_u J$, $\text{Sub}^b_u J \subseteq \text{Sub}^b_u G$, and $\text{card}(J) = \text{card}(H)$. Let $K =_{df} (\text{Sub}^a_u G)^- - H$, we set $D^- =_{df}$

$$\frac{K \cup \text{Sub}^a_u J \vdash \text{Sub}^a_u E'}{\{a \ominus b\} \cup K \cup \text{Sub}^b_u J \vdash \text{Sub}^b_u E'}.$$

Now suppose that $D =$

$$\frac{F_1 \vdash E_2 \qquad \{E_2\} \cup F_2 \vdash E_1}{F_1 \cup F_2 \vdash E_1}.$$

By hyp. ind. we have a

$$\begin{array}{c} D_1^- \\ F_1^- \vdash E_2 \end{array} \quad \text{and a} \quad \begin{array}{c} D_2^- \\ (\{E_2\} \cup F_2)^- \vdash E_1 \end{array}.$$

If E_2 does not belong to $(\{E_2\} \cup F_2)^-$, then we set $D^- =_{df} D_2^-$; otherwise, we set $D^- =_{df}$

$$\frac{\begin{array}{c} D_1^- \\ F_1^- \vdash E_2 \end{array} \qquad \begin{array}{c} D_2^- \\ (\{E_2\} \cup F_2)^- \vdash E_1 \end{array}}{F_1^- \cup ((\{E_2\} \cup F_2)^- - \{E_2\}) \vdash E_1}.$$

Observe that if a subderivation of D^- of length m ends in $F_1 \vdash E_1$, then $\text{card}(F_1) \leq m$; the desired linear derivation can easily be constructed from D^- making use of this fact to obtain the bound $n \cdot (n+1)/2$.

1.4.5. Proposition. $F \vdash^{n}_{\mathrm{SE}} E \Rightarrow F \vdash^{2n\cdot(n+1)}_{\mathrm{SE\text{-}cut}} E$.

1.5. *Proof-search*

1.5.1. An SE-derivation D of $F \vdash E$ is said to be m-direct for a pre-measure m if for each term a occurring in D there is a term b occurring in $F \vdash E$ such that $m(a) \leqslant m(b)$. $\mathrm{pm}(F)$ is the number of parameters occurring in F.

1.5.2. Lemma. *If F is simple and $\&F \to u = v$ is valid, then there is an m-direct SE-derivation of $F \vdash u = v$ of length $\leqslant \mathrm{pm}(F) \cdot 3$.*

Proof. Let $F_1 =_{\mathrm{df}} F \cup \{u' = u' : u' \text{ occurs in } F\}$, set $u_1 =_{\mathrm{df}} u$, and put $v_1 =_{\mathrm{df}} v$. We define a sequence of sequents $F_i \vdash u_i = v_i$, for $1 \leqslant i \leqslant k$ and $k \leqslant \mathrm{pm}(F) \cdot 2$, such that

$$F_k \vdash u_k = v_k$$
$$\vdots$$
$$F_1 \vdash u_1 = v_1$$

is an m-direct SE-derivation of $F_1 \vdash u_1 = v_1$. The desired SE-derivation is obtained from this by applying cut to the equations in $F_1 - F$.

Suppose that $F_l \vdash u_l = v_l$ has been defined, and there are $a = d$, $b = d$ in F_l such that a is not b and $m(a) \leqslant m(b)$, then we set $F_{l+1} =_{\mathrm{df}} (F_l - \{a = d\}) \cup \{a = b\}$, $u_{l+1} =_{\mathrm{df}} u_l$, $v_{l+1} =_{\mathrm{df}} v_l$, and define $F_{l+2} = \mathrm{Sub}^{a}_{b}(F_{l+1} - \{a = b\})$, $u_{l+2} = \mathrm{Sub}^{a}_{b}\, u_l$, and $v_{l+2} = \mathrm{Sub}^{a}_{b}\, v_l$.

To prove the lemma it suffices to show that u_k is v_k. Now F_k has the following properties:

(i) if $fu'_1 \cdots u'_l$ occurs in F_k, then there is exactly one u'_{l+1} s.t. $u'_{l+1} = fu'_1 \cdots u'_l$ belongs to F_k, and similarly for a constant c;

(ii) if $u' = v'$ belongs to F_k, then u' is v'.

Thus an interpretation of F_k can be read off from F_k which satisfies $u_k = v_k$ if and only if u_k is v_k. But this model of F_k can be expanded to a model of F_1 and $\&F_1 \to (u_1 = v_1 \leftrightarrow u_k = v_k)$.

1.5.3. Proposition. *If $\&F \to a = b$ is valid, then there is a lh-direct SE-derivation of $F \vdash a = b$ of length $\leqslant \mathrm{lh}(F \cup \{a = b\}) \cdot 7$*

Proof. To each occurrence t of a term in $F \vdash a = b$ assign a new parameter u_t. Let $F_1 =_{\mathrm{df}} \{u_{ft_1 \cdots t_n} = fu_{t_1} \cdots u_{t_n}, u_t = v, u_{t'} = c : ft_1 \cdots t_n$ an occurrence, t an occurrence of v, and t' an occurrence of $c\}$, and set $F_2 =_{\mathrm{df}} \{u_t = u_{t'} : t = t' \text{ in } F\}$. Now apply Lemma 5.2 to $F_1 \cup F_2 \vdash u_a = u_b$ for the pre-measure lh_θ where $\theta =_{\mathrm{df}} \mathrm{Sub}^{\cdots t \cdots}_{\cdots u_t \cdots}$, and apply cut to equations in $\theta(F_1 \cup F_2) - F$.

2. Proof-search in the propositional calculus

2.1. *Preliminaries*

2.1.1. We consider formulae $A, B, C, \ldots$ built up from propositional parameters $U, V, W, \ldots$, the propositional constant $\perp$ (falsehood), and the connective constant $\to$, and sequents $F \vdash G$ for F and G finite sets of formulae with $G \neq \emptyset$.

We set $\neg A =_{df} A \to \perp$ and $\neg F =_{df} \{\neg A : A \in F\}$. If $F = \{A_i : 1 \leqslant i \leqslant m\}$ we set

$$\& F \to B =_{df} \underset{1 \leqslant i \leqslant m}{\&} A_i \to B =_{df} A_1 \to (\cdots (A_m \to B) \cdots).$$

2.1.2. The interpretation of $F \vdash G$ is $\& F \to (\& \neg G \to \perp)$.

2.1.3. We define the notion of positive and negative occurrence as follows: A occurs positive in A; if A occurs positive in B or negative in C, then it occurs negative in $B \to C$; if A occurs negative in B or positive in C, then it occurs positive in $B \to C$; A occurs positive in $F \vdash G$ if it occurs positive in a member of G or negative in a member of F; A occurs negative in $F \vdash G$ if it occurs positive in a member of F or negative in a member of G.

2.1.4. The calculus S_0 (cut-free sequential rules for the propositional calculus) consists of the axioms $F \cup \{\perp\} \vdash G$, $F \cup \{A\} \vdash G \cup \{A\}$ and the rules

$$(\vdash\ \to)\quad \frac{F \cup \{A\} \vdash G \cup \{B\}}{F \vdash G \cup \{A \to B\}},$$

$$(\to\ \vdash)\quad \frac{F \vdash G \cup \{A\} \qquad F \cup \{B\} \vdash G}{F \cup \{A \to B\} \vdash G}.$$

S_0-derivations D are binary trees of sequent occurrences built up from axioms by the rules $(\vdash\ \to)$ and $(\to\ \vdash)$.

2.1.5. "$F \vdash_{S_0}^{n} G$" means that there is an S_0-derivation of $F \vdash G$ of length $\leqslant n$.

2.2. *Upper bound*

2.2.1. Proposition. *If $F \vdash G$ is valid, then $F \vdash_{S_0}^{2lh(F)+lh(G)} G$.*

Proof. Inspection of the usual completeness proof for semantic tableaus.

2.3. *Lower bound*

2.3.1. Lemma. *If*

$$F \cup \left\{ \underset{1 \leqslant i \leqslant n}{\&} A_i \to B_1 \right\} \vdash_{S_0}^{m} G$$

and $A_n \to B_1$ *does not occur positive in*

$$F \cup \left\{ \underset{1 \le i \le n}{\&} A_i \to B_1 \right\} \vdash G,$$

then $F \mid\!\frac{m}{S_0}\, G \cup \{A_n\}$.

The proofs for this and the following four lemmas will follow.

2.3.2. Lemma. *If*

$$F \cup \left\{ \underset{1 \le i \le n}{\&} A_i \to B_1 \right\} \mid\!\frac{m}{S_0}\, G$$

and $A_n \to B_1$ *does not occur positive in*

$$F \cup \left\{ \underset{1 \le i \le n}{\&} A_i \to B_1 \right\} \vdash G,$$

then

$$F \cup \left\{ \underset{1 \le i \le n-1}{\&} A_i \to B_1 \right\} \mid\!\frac{m}{S_0}\, G.$$

2.3.3. Lemma. *If* $F \mid\!\frac{m}{S_0}\, G \cup \{A_1 \to B_1\}$ *and* $A_1 \to B_1$ *does not occur negative in* $F \vdash G \cup \{A_1 \to B_1\}$, *then either* $F \mid\!\frac{m}{S_0}\, G \cup \{B_1\}$ *or* $F \cup \{A_1\} \mid\!\frac{m-1}{S_0}\, G \cup \{B_1\}$.

2.3.4. Lemma. *If*

$$F \cup \left\{ \underset{1 \le i \le n-1}{\&} A_i \to ((U \to A_n) \to B_1) \right\} \mid\!\frac{m}{S_0}\, G$$

and U *does not occur positive in*

$$F \cup \left\{ \underset{1 \le i \le n-1}{\&} A_i \to ((U \to A_n) \to B_1) \right\} \vdash G,$$

then

$$F \cup \left\{ \underset{1 \le i \le n}{\&} A_i \to B_1 \right\} \mid\!\frac{m}{S_0}\, G.$$

2.3.5. Lemma. *If*

$$F \cup \left\{ \underset{1 \le i \le n-1}{\&} A_i \to ((U \to (U \to A_n)) \to B_1) \right\} \mid\!\frac{m}{S_0}\, G$$

and $U \to A_n$ *does not occur negative in*

$$F \cup \left\{ \underset{1 \le i \le n-1}{\&} A_i \to ((U \to (U \to A_n)) \to B_1) \right\} \vdash G,$$

then

$$F\cup\left\{\mathop{\&}_{1\leq i\leq n-1} A_i \to ((U\to A_n)\to B_1)\right\}\vdash^{n}_{S_0} G.$$

2.3.6. Cases for Lemmas 2.3.1–2.3.6

(i)
$$\frac{\overset{D_1}{H\vdash G\cup\{A\}} \qquad \overset{D_2}{H\cup\{B\}\vdash G}}{F\cup\{A\to B\}\vdash G}$$

where $H=F-\{A\to B\}$, $H=F$, or $H=F\cup\{A\to B\}$.

(ii)
$$\frac{\overset{D_1}{H\vdash G\cup\{C_1\}} \qquad \overset{D_2}{H\cup\{C_2\}\vdash G}}{F\cup\{A\to B\}\vdash G}$$

where $H=F\cup\{A\to B\}$ or $H=(F\cup\{A\to B\})-\{C_1\to C_2\}$, and $C_1\to C_2\neq A\to B$.

(iii)
$$\frac{\overset{D_1}{\{C_1\}\cup(F\cup\{A\to B\})\vdash J\cup\{C_2\}}}{F\cup\{A\to B\}\vdash G}$$

where $J=G$ or $J=G-\{C_1\to C_2\}$.

(iv)
$$\frac{\overset{D_1}{F\cup\{A\}\vdash J\cup\{B\}}}{F\vdash G\cup\{A\to B\}}$$

where $J=G-\{A\to B\}$, $J=G$, or $J=G\cup\{A\to B\}$.

(v)
$$\frac{\overset{D_1}{F\cup\{C_1\}\vdash J\cup\{C_2\}}}{F\vdash G\cup\{A\to B\}}$$

where $J=G\cup\{A\to B\}$ or $J=(G\cup\{A\to B\})-\{C_1\to C_2\}$, and $C_1\to C_2\neq A\to B$.

(vi)
$$\frac{\overset{D_1}{H\vdash G\cup\{A\to B\}\cup\{C_1\}} \qquad \overset{D_2}{H\cup\{C_2\}\vdash G\cup\{A\to B\}}}{F\vdash G\cup\{A\to B\}}$$

where $H=F$ or $H=F-\{C_1\to C_2\}$.

2.3.7. The proofs of Lemmas 2.3.1–2.3.5 are by induction on m; in each case we assume at the induction step that D is an S_0-derivation of the appropriate sequent with length $\leq m$.

Proof of Lemma 2.3.1.

Basis: trivial.
Induction step:

Case 1: $D=$(i), $A=A_1$, and $B=\&_{2\leq i\leq n} A_i \to B_1$. W.l.o.g. can assume $A\to B\notin F$ and $H=F\cup\{A\to B\}$. If $n=1$, by applying hyp. ind. to D_1 we get $F\vdash^{m}_{S_0} G\cup\{A_n\}$. If $n\neq 1$, by applying hyp. ind. to D_2 we get an S_0-derivation of

$$(*)\qquad F\cup\left\{\underset{2\leq i\leq n}{\&} A_i\to B_1\right\}\vdash G\cup\{A_n\}$$

of length $\leq m-1$. By applying hyp. ind. to the derivation of $(*)$ we get $F\vdash^{m}_{S_0} G\cup\{A_n\}$.

Case 2: $D=$(ii), $A=A_1$, and $B=\&_{2\leq i\leq n} A_i\to B_1$. W.l.o.g. can assume $H=F\cup\{A\to B\}$. Apply hyp. ind. to both D_1 and D_2 and end with $(\to\vdash)$.

Case 3: $D=$(iii), $A=A_1$, and $B=\&_{2\leq i\leq n} A_i\to B_1$. W.l.o.g. can assume $J=G$. Apply hyp. ind. to D_1 and end with $(\vdash\to)$.

2.3.8. Proof of Lemma 2.3.2.

Basis: trivial.
Induction step:

Case 1: $D=$(i), $A=A_1$, and $B=\&_{2\leq i\leq n} A_i\to B_1$. W.l.o.g. can assume $A\to B\notin F$ and $H=F\cup\{A\to B\}$. If $n=1$, by applying hyp. ind. to D_2 we get $F\cup\{B_1\}\vdash^{m}_{S_0} G$. If $n\neq 1$, by applying hyp. ind. to D_1 we get an S_0-derivation of

$$\text{(a)}\qquad F\cup\left\{\underset{1\leq i\leq n-1}{\&} A_i\to B_1\right\}\vdash G\cup\{A_1\}$$

of length $\leq \text{lh}(D_1)$. By applying hyp. ind. to D_2 we get an S_0-derivation of

$$\text{(b)}\qquad F\cup\left\{\underset{1\leq i\leq n-1}{\&} A_i\to B_1\right\}\cup\left\{\underset{2\leq i\leq n}{\&} A_i\to B_1\right\}\vdash G$$

of length $\leq \text{lh}(D_2)$. By applying hyp. ind. to the derivation of (b) we get an S_0-derivation of

$$\text{(c)}\qquad F\cup\left\{\underset{1\leq i\leq n-1}{\&} A_i\to B_1\right\}\cup\left\{\underset{2\leq i\leq n-1}{\&} A_i\to B_1\right\}\vdash G$$

of length $\leq \text{lh}(D_2)$. Combining the derivation of (a) and the derivation of (c) by $(\to\vdash)$ gives the desired S_0-derivation.

Cases 2 and 3 are similar to those of 2.3.7.

2.3.9. Proof of Lemma 2.3.3.

Basis: trivial.
Induction step:

Case 1: $D = \text{(iv)}$ $A = A_1$, and $B = B_1$. W.l.o.g. can assume $J = G \cup \{A \to B\}$ and $A \to B \notin G$. By applying hyp. ind. to D_1 we get $F \cup \{A_1\} \vdash^{m-1}_{S_0} G \cup \{B_1\}$.

Case 2: $D = \text{(v)}$, $A = A_1$, and $B = B_1$. W.l.o.g. can assume $J = G \cup \{A \to B\}$ and $A \to B \notin G$. Apply hyp. ind. to D_1 and end with $(\vdash \to)$.

Case 3: $D = \text{(vi)}$, $A = A_1$, and $B = B_1$. W.l.o.g. can assume $H = F$ and $A \to B \notin G$. Apply hyp. ind. to both D_1 and D_2 and end with $(\to \vdash)$.

2.3.10. Proof of Lemma 2.3.4.

Basis: trivial.
Induction step:

Case 1: $D = \text{(i)}$, $A = A_1$, and $B = \&_{2 \le i \le n-1} A_i \to ((U \to A_n) \to B_1)$, or $D = \text{(i)}$, $A = U \to A_1$, and $B = B_1$ $(n = 1)$. W.l.o.g. can assume $H = F \cup \{A \to B\}$ and $A \to B \notin F$. If $n \ne 1$ proceed as in Case 1 of 2.3.8. If $n = 1$, by Lemma 2.3.3 there is an S_0-derivation of

(a) $\quad F \cup \{(U \to A_1) \to B_1\} \cup \{U\} \vdash G \cup \{A_1\}$

of length $\le \text{lh}(D_1)$. Since U does not occur positive in (a) there is an S_0-derivation of

(b) $\quad F \cup \{(U \to A_1) \to B_1\} \vdash G \cup \{A_1\}$

of length $\le \text{lh}(D_1)$. By hyp. ind. there is an S_0-derivation of

(c) $\quad F \cup \{A_1 \to B_1\} \vdash G \cup \{A_1\}$

of length $\le \text{lh}(D_1)$. By applying hyp. ind. to D_2 we get an S_0-derivation of

(d) $\quad F \cup \{A_1 \to B_1\} \cup \{B_1\} \vdash G$

of length $\le \text{lh}(D_2)$. Combining the derivations of (c) and (d) by $(\to \vdash)$ gives the desired derivation.

Cases 2 and 3 are similar to those of 2.3.7.

2.3.11. Proof of Lemma 2.3.5.

Basis: trivial.
Induction step:

Case 1: $D = \text{(i)}$, $A = A_1$, and $B = \&_{2 \le i \le n-1} A_i \to ((U \to (U \to A_n) \to B_1)$, or $D = \text{(i)}$, $A = U \to (U \to A_1)$, and $B = B_1$ $(n = 1)$. W.l.o.g. can assume $H = F \cup \{A \to B\}$ and $A \to B \notin F$. If $n \ne 1$, proceed as in Case 1 of 2.3.8. If $n = 1$, by Lemma 2.3.3 there is an S_0-derivation of

(a) $\quad F \cup \{(U \to (U \to A_1)) \to B_1\} \vdash G \cup \{U \to A_1\}$

of length $\leq \mathrm{lh}(D_1)$ or an S_0-derivation of

(b) $\quad F \cup \{(U \to (U \to A_1)) \to B_1\} \cup \{U\} \vdash G \cup \{U \to A_1\}$

of length $< \mathrm{lh}(D_1)$. By hyp. ind. applied to D_2 there is an S_0-derivation of

(c) $\quad F \cup \{(U \to A_1) \to B_1\} \cup \{B_1\} \vdash G$

of length $\leq \mathrm{lh}(D_2)$. In case (a), by hyp. ind. there is an S_0-derivation of

(d) $\quad F \cup \{(U \to A_1) \to B_1\} \vdash G \cup \{U \to A_1\}$

of length $\leq \mathrm{lh}(D_1)$. Combining the derivation of (d) with the derivation of (c) by $(\to \vdash)$ gives the desired derivation. In case (b), by Lemma 2.3.3 there is an S_0-derivation of

(e) $\quad F \cup \{(U \to (U \to A_1)) \to B_1\} \cup \{U\} \vdash G \cup \{A_1\}$

of length $< \mathrm{lh}(D_1)$. Thus by hyp. ind. applied to the derivation of (e) there is an S_0-derivation of

(f) $\quad F \cup \{(U \to A_1) \to B_1\} \cup \{U\} \vdash G \cup \{A_1\}$

of length $< \mathrm{lh}(D_1)$. Hence there is an S_0-derivation of

(g) $\quad F \cup \{(U \to A_1) \to B_1\} \vdash G \cup \{U \to A_1\}$

of length $\leq \mathrm{lh}(D_1)$. Combining the derivation of (g) with the derivation of (c) by $\to \vdash$ gives the desired derivation.

Cases 2 and 3 are similar to those of 2.3.7.

2.3.12. Let $U_{i,j,l}$, for $0 \leq i \leq n$, $1 \leq j \leq m$, and $1 \leq l \leq k$, be $(n+1) \cdot m \cdot k$ distinct parameters, let $V_{i,j}$, for $0 \leq i \leq n$, and $1 \leq j \leq m$, be $(n+1) \cdot m$ distinct new parameters, let W_j, for $1 \leq j \leq k$, be k distinct new parameters and let W be a new parameter; we make the following definitions: $(n, m, k \neq 0)$

$$A_{i,j} =_{\mathrm{df}} \mathop{\&}_{1 \leq l \leq k} U_{i,j,l} \to V_{i,j} \quad \text{for} \quad 0 \leq i \leq n \quad \text{and} \quad 1 \leq j \leq m;$$

$$B_{i,j} =_{\mathrm{df}} \mathop{\&}_{1 \leq l \leq k} U_{i,j,l} \to \left(\mathop{\&}_{1 \leq u \leq m} A_{i-1,u} \to V_{i,j} \right) \quad \text{for} \quad 1 \leq i \leq n \quad \text{and} \quad 1 \leq j \leq m$$

$$B_{n+1} =_{\mathrm{df}} \mathop{\&}_{1 \leq l \leq k} W_l \to \left(\mathop{\&}_{1 \leq u \leq m} A_{n,u} \to W \right);$$

$$A^l_{i,j} =_{\mathrm{df}} \mathop{\&}_{l < u \leq k} U_{i,j,u} \to V_{i,j};$$

$$B^l_{i,j} =_{\mathrm{df}} \mathop{\&}_{l < u \leq k} U_{i,j,u} \to \left(\mathop{\&}_{1 \leq v \leq m} A_{i-1,v} \to V_{i,j} \right);$$

$$C^l_{i,j} =_{\mathrm{df}} \mathop{\&}_{1 \leq u \leq k} U_{i,j,u} \to \left(\mathop{\&}_{1 \leq v < l} A_{i-1,v} \to \left(\mathop{\&}_{l < v \leq m} A_{i-1,v} \to V_{i,j} \right) \right);$$

$$B^{1,*}_{i,j} =_{\mathrm{df}} \mathop{\&}_{2\leq u\leq k} U_{i,j,u} \to \Big(\mathop{\&}_{1\leq \upsilon\leq m} A^1_{i,j} \to V_{i,j}\Big);$$

$$B^l_{n+1} =_{\mathrm{df}} \mathop{\&}_{l<i\leq k} W_i \to \Big(\mathop{\&}_{1\leq j\leq m} A_{n,j} \to W\Big);$$

$$C^{l,*}_{n+1} =_{\mathrm{df}} \mathop{\&}_{l<i\leq m} A_{n,i} \to W;$$

$$C^l_{n+1} =_{\mathrm{df}} \mathop{\&}_{i<l} A_{n,i} \to \Big(\mathop{\&}_{l<i\leq m} A_{n,i} \to W\Big);$$

$$F_{n,m,k} =_{\mathrm{df}} \{B_{i,j} : 1\leq i\leq n, 1\leq j\leq m\} \cup \{B_{n+1}\} \cup \{W_j : 1\leq j\leq k\};$$

$$G_{n,m,k} =_{\mathrm{df}} \{W\} \cup \{U_{0,j,l} : 1\leq j\leq m, 1\leq l\leq k\};$$

$$A_n =_{\mathrm{df}} \mathop{\&}_{1\leq i,j\leq n} B_{i,j} \to \Big(B_{n+1} \to \Big(\mathop{\&}_{1\leq i,j\leq n} - U_{0,i,j} \to \Big(\mathop{\&}_{1\leq j\leq n} W_j \to W\Big)\Big)\Big).$$

2.3.13. Lemma. $F_{n,m,k} \mid\!\frac{r}{S_0}\, G_{n,m,k} \Rightarrow 2^{\min\{n,m,k\}} \leq r.$

Proof. By induction on $\min\{n, m, k\}$ with a subsidiary induction on r.

Basis: $\min\{n, m, k\} = 1$. Trivial.

Induction step: $\min\{n, m, k\} \neq 1$. Suppose that D is an S_0-derivation of $F_{n,m,k} \vdash G_{n,m,k}$ of length $\leq r$.

Case 1: $D =$

$$\dfrac{\dfrac{H\cup J_1 \vdash G_{n,m,k} \cup \{W_1\} \qquad H\cup J_1 \cup \{B^1_{n+1}\} \vdash G_{n,m,k}}{H\cup J_1\cup\{B_{n+1}\}\vdash G_{n,m,k}}}{\begin{array}{c}\vdots\\ \dfrac{\begin{array}{cc} D_1 & D_2 \\ H\cup J_p \vdash G_{n,m,k}\cup\{A_{n,1}\} & H\cup J_p\cup\{C^{1,*}_{n+1}\}\vdash G_{n,m,k}\end{array}}{H\cup J_{p-1}\vdash G_{n,m,k}}\end{array}}$$

where $H = F_{n,m,k} - \{B_{n+1}\}$ and $J_i \subseteq \{B^j_{n+1} : 0\leq j\leq k\}$. By Lemma 2.3.2 there is an S_0-derivation of

(a) $\quad H \cup \{B^k_{n+1}\} \vdash G_{n,m,k} \cup \{A_{n,1}\}$

of length $\leq \mathrm{lh}(D_1)$. Let $H_1 =_{\mathrm{df}} H - \{W_j : 1\leq j\leq k\}$, since W_j does not occur positive in (a) there is an S_0-derivation of

(b) $\quad H_1 \cup \{B^k_{n+1}\} \vdash G_{n,m,k} \cup \{A_{n,1}\}$

of length $\leq \mathrm{lh}(D_1)$. By Lemma 2.3.1 there is an S_0-derivation of

(c) $\quad H_1 \vdash G_{n,m,k} \cup \{A_{n,1}\}$

of length $\leq \mathrm{lh}(D_1)$. Let $G_1 =_{\mathrm{df}} G_{n,m,k} - \{W\}$, since W does not occur negative in (c) there is an S_0-derivation of

(d) $\quad H_1 \vdash G_1 \cup \{A_{n,1}\}$

of length $\leq \mathrm{lh}(D_1)$. Let H_2 result from H_1 and G_2 from G_1 by identifying each $V_{n,i}$ with $V_{n,1}$ and each $U_{n,j,i}$ with $U_{n,1,i}$ (by the appropriate substitution), then there is an S_0-derivation of

(e) $\quad H_2 \vdash G_2 \cup \{A_{n,1}\}$

of length $\leq \mathrm{lh}(D_1)$. By Lemma 2.3.3 there is an S_0-derivation of

(f) $\quad H_2 \cup \{U_{n,1,j}: 1 \leq j \leq k\} \vdash G_2 \cup \{V_{n,1}\}$

of length $\leq \mathrm{lh}(D_1)$. Applying hyp. ind. to the derivation of (f) we get $2^{\min\{n,m,k\}-1} \leq \mathrm{lh}(D_1)$.

By Lemma 2.3.2 there is an S_0-derivation of

(g) $\quad H \cup \{C^{1,*}_{n+1}\} \vdash G_{n,m,k}$

of length $\leq \mathrm{lh}(D_2)$. Let $H_1 =_{\mathrm{df}} \{C^1_{i,j}: 1 \leq i \leq n,\ 1 \leq j \leq m\} \cup \{W_j: 1 \leq j \leq k\}$; by Lemma 2.3.2 there is an S_0-derivation of

(h) $\quad H_1 \cup \{C^{1,*}_{n+1}\} \vdash G_{n,m,k}$

of length $\leq \mathrm{lh}(D_2)$. Let H_2 result from H_1 and G_2 from G by identifying $V_{i,1}$ with $V_{i,2}$ and $U_{i,1,j}$ with $U_{i,2,j}$ (by the appropriate substitution), then there is an S_0-d rivation of

(i) $\quad H_2 \cup \{C^{1,*}_{n+1}\} \vdash G_2$

of length $\leq \mathrm{lh}(D_2)$. Thus there is an S_0-derivation of

(j) $\quad H_2 \cup \left\{ \mathop{\&}_{1 \leq i \leq k} W_i \rightarrow C^{1,*}_{n+1} \right\} \vdash G_2$

of length $\leq \mathrm{lh}(D_2) + p - 1$. Hence by applying hyp. ind. to the derivation of (j) we get $2^{\min\{n,m,k\}-1} \leq \mathrm{lh}(D_2) + p - 1$, so $2^{\min\{n,m,k\}} \leq \mathrm{lh}(D)$.

Case 2: $D =$

$$\dfrac{\begin{matrix} D_1 \\ K \cup J_p \cup L \vdash G_{n,m,k} \cup \{U_{l,q,1}\} \end{matrix} \qquad \begin{matrix} D_2 \\ K \cup J_p \cup L \cup \{B^1_{l,q}\} \vdash G_{n,m,k} \end{matrix}}{K \cup J_p \cup L \cup \{B_{l,q}\} \vdash G_{n,m,k}}$$

$$\vdots$$

$$\dfrac{H \cup J_1 \vdash G_{n,m,k} \cup \{W\} \qquad H \cup J_1 \cup \{B^1_{n+1}\} \vdash G_{n,m,k}}{H \cup J_1 \cup \{B_{n+1}\} \vdash G_{n,m,k}}$$

where $H = F_{n,m,k} - \{B_{n+1}\}$, $J_i \subseteq \{B^j_{n+1}: 0 \leq j \leq k\}$, $K = H - \{B_{l,q}\}$, and $L \subseteq \{B_{l,q}\}$. Let

$H_1 =_{df} \{C^q_{i,j}: 1 \le i \le n,\ 1 \le j \le m\} \cup \{W_j: 1 \le j \le m\}$, and $J^* =_{df} \{\&_{i \le j \le k} W_j \to C^q_{n+1}: \&_{i \le j \le k} W_j \to C^{0,*}_{n+1} \in J_p,\ 1 \le i \le k+1\}$, by Lemma 2.3.2 there is an S_0-derivation of

(a) $H_1 \cup J^* \vdash G_{n,m,k} \cup \{U_{l,q,1}\}$

of length $\le \mathrm{lh}(D_1)$. Since $U_{l,q,1}$ does not occur negatively in (a) there is an S_0-derivation of

(b) $H_1 \cup J^* \vdash G_{n,m,k}$

of length $\le \mathrm{lh}(D_1)$. Let H_2 result from H_1 and G_2 from $G_{n,m,k}$ by identifying $V_{i,q}$ with $V_{i,t}$ and $U_{i,q,j}$ with $U_{i,t,j}$ for some fixed $t \ne q$ (by the appropriate substitution), then there is an S_0-derivation of

(c) $H_2 \cup J^* \vdash G_2$

of length $\le \mathrm{lh}(D_1)$. Thus there is an S_0-derivation of

(d) $H_2 \cup \left\{ \underset{1 \le i \le k}{\&} W_i \to C^q_{n+1} \right\} \vdash G_2$

of length $\le \mathrm{lh}(D_1)+p$. Hence by applying hyp. ind. to the derivation of (d) we get $2^{\min\{n,m,k\}-1} \le \mathrm{lh}(D_1)+p$.

By Lemma 2.3.1 there is an S_0-derivation of

(e) $K \cup L \cup \{B^1_{l,q}\} \vdash G_{n,m,k} \cup \{A_{n,1}\}$

of length $\le \mathrm{lh}(D_2)$. Let $K_1 =_{df} K - \{W_j: 1 \le j \le k\}$, since W_j does not occur positive in (e) there is an S_0-derivation of

(f) $K_1 \cup L \cup \{B^1_{l,q}\} \vdash G_{n,m,k} \cup \{A_{n,1}\}$

of length $\le \mathrm{lh}(D_2)$. Let $G_1 =_{df} G_{n,m,k} - \{W\}$, since W does not occur negative in (f) there is an S_0-derivation of

(g) $K_1 \cup L \cup \{B^1_{l,q}\} \vdash G_1 \cup \{A_{n,1}\}$

of length $\le \mathrm{lh}(D_2)$. Let K_2 result from $K_1 \cup L \cup \{B^1_{l,q}\}$ and G_2 from G_1 by identifying each $V_{n,j}$ with $V_{n,1}$ and each $U_{n,j,i}$ with $U_{n,1,i}$ (by the appropriate substitution), then there is an S_0-derivation of

(h) $K_2 \vdash G_2 \cup \{A_{n,1}\}$

of length $\le \mathrm{lh}(D_2)$. Let $K_3 =_{df} \{B^1_{i,j}: 1 \le i \le n-1,\ 1 \le j \le m\} \cup \{B^1_{n,1}\}$; by Lemma 2.3.2 there is an S_0-derivation of

(i) $K_3 \vdash G_2 \cup \{A_{n,1}\}$

of length $\le \mathrm{lh}(D_2)$. Let $K_4 =_{df} \{B^{1,*}_{i,j}: 1 \le i \le n-1,\ 1 \le j \le m\} \cup \{B^{1,*}_{n,1}\}$, then by Lemma 2.3.4 there is an S_0-derivation of

(j) $K_4 \cup \{B^1_{1,j}: 1 \le j \le m\} \vdash G_2 \cup \{A_{n,1}\}$

of length $\leqslant \mathrm{lh}(D_2)$. By Lemma 2.3.3 there is an S_0-derivation of

(k) $\quad K_4 \cup \{B^1_{1,j}: 1 \leqslant j \leqslant m\} \cup \{U_{n,1,1}\} \vdash G_2 \cup \{A^1_{n,1}\}$

of length $\leqslant \mathrm{lh}(D_2)$. Since $U_{n,1,1}$ does not occur positive in (k) there is an S_0-derivation of

(l) $\quad K_4 \cup \{B^1_{1,j}: 1 \leqslant j \leqslant m\} \vdash G_2 \cup \{A^1_{n,1}\}$

of length $\leqslant \mathrm{lh}(D_2)$. Let K_5 result from $\{B^1_{1,j}: 1 \leqslant j \leqslant m\}$ by substituting $U_{0,j,2}$ for $U_{0,j,1}$ for $1 \leqslant j \leqslant m$, then there is an S_0-derivation of

(m) $\quad K_4 \cup K_5 \vdash (G_2 - \{U_{0,j,1}: 1 \leqslant j \leqslant m\}) \cup \{A^1_{n,1}\}$

of length $\leqslant \mathrm{lh}(D_2)$. By Lemma 2.3.5 there is an S_0-derivation of

(n) $\quad \{B^{1,*}_{i,j}: 1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant m\} \cup \{B^{1,*}_{n,1}\} \vdash (G_2 - \{U_{0,j,1}: 1 \leqslant j \leqslant m\}) \cup \{A^1_{n,1}\}$

of length $\leqslant \mathrm{lh}(D_2)$. Let

$$K_6 =_{\mathrm{df}} \{B^{1,*}_{i,j}: 1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant m\} \cup \{B^{1,*}_{n,1}\} \cup \{U_{n,1,j}: 2 \leqslant j \leqslant k\},$$

then by Lemma 2.3.3 there is an S_0-derivation of

(o) $\quad K_6 \vdash \{V_{n,1}\} \cup (G_2 - \{U_{0,j,1}: 1 \leqslant j \leqslant m\})$

of length $\leqslant \mathrm{lh}(D_2)$. Thus by applying hyp. ind. to the derivation of (o) we get $2^{\min\{n,m,k\}-1} \leqslant \mathrm{lh}(D_2)$. Hence $2^{\min\{n,m,k\}} \leqslant \mathrm{lh}(D)$.*

Since all cases can be put in the form of Case 1 or Case 2, this completes the proof.

2.3.14. Proposition. *There is no polynomial $p(x)$ such that if A is valid, then $\emptyset \vdash^{p(\mathrm{lh}(A))}_{S_0} \{A\}$.*

Proof. By Lemma 2.3.1, 2.3.3 and 2.3.13 $\emptyset \vdash^{m}_{S_0} \{A_n\} \Rightarrow 2^n \leqslant m$.

2.4. *Speed-up*

2.4.1. The rule of cut is the following

(cut) $$\frac{F \vdash G \cup \{A\} \qquad \{A\} \cup F \vdash G}{F \vdash G}.$$

2.4.2. It is easily seen that for the A_n of Section 2.3 there is a polynomial $q(x)$ such that $\emptyset \vdash^{q(n)}_{S_0+\mathrm{cut}} \{A_n\}$. Thus there is no polynomial such that $\emptyset \vdash^{n}_{S_0+\mathrm{cut}} \{A\} \Rightarrow$

* Inspection of the proof shows that variation of the parameter k is unnecessary (i.e., $k=1$ is sufficient, replacing $2^{\min\{n,m,k\}}$ by $2^{\min\{n,m\}}$).

$\emptyset \vdash^{p(n)}_{S_0} \{A\}$. In Section 4 we shall show that for a suitable constant k, $\emptyset \vdash^{n}_{S_0+c\,n} \{A\} \Rightarrow \emptyset \vdash^{2^{kn}_{3}}_{S_0} \{A\}$.†

3. Proof-search in the predicate calculus

3.1. *Preliminaries*

3.1.1. We consider formulae $A, B, C, \ldots$ of predicate logic built up from arbitrary individual terms relation symbols $U, V, W, \ldots$ individual (bound) variables $x, y, z, \ldots, \rightarrow, \bot$, and $\forall$. We refer the reader to Prawitz [29] for additional syntactic conventions and distinctions. In what follows we shall make no mention of the changing and choice of bound variables (and proper parameters) leaving these to the reader.

3.1.2. A formula is called monadic if all its relation symbols are unary and all its pseudo-terms are parameters and variables.

3.1.3. The calculus S_1 (cut-free sequential rules for the predicate calculus) is obtained from S_0 by the addition of the rules

$$(\forall \vdash) \qquad \frac{F \cup \{A(a)\} \vdash G}{F \cup \{\forall x\, A(x)\} \vdash G},$$

$$(\vdash \forall) \qquad \frac{F \vdash G \cup \{A(u)\}}{F \vdash G \cup \{\forall x\, A(x)\}}$$

provided that u does not occur in the conclusion.

3.1.4. The calculus N_1 (natural rules for the predicate calculus) is the system C' of Prawitz [23] (under the definition of Section 1.4; the reader should consult this chapter for additional explanations). It consists of the rules

$$(\rightarrow I) \qquad \frac{\begin{matrix}(A)\\ B\end{matrix}}{A \rightarrow B}$$

$$(\rightarrow E) \qquad \frac{A \rightarrow B \qquad A}{B}$$

$$(\bot) \qquad \frac{\begin{matrix}(\neg A)\\ \bot\end{matrix}}{A}$$

$$(\forall I) \qquad \frac{A(u)}{\forall x\, A(x)}$$

† By a more refined "unification" algorithm 2^{kn}_{3} can be replaced by 2^{kn}.

provided that u does not occur in any assumption

$$(\forall E) \qquad \frac{\forall x\, A(x)}{A(a)}.$$

3.1.5. The calculus N_0 (natural rules for the propositional calculus) consists of N_1 less the rules $(\forall I)$ and $(\forall E)$.

3.1.6. The calculus NE_1 (natural rules for the predicate calculus with equality) consists of N_1 together with the axiom $\forall x(x = x)$ and the rule

$$(=) \qquad \frac{A(a) \qquad a \ominus b}{A(b)}.$$

3.1.7. The calculus NE_0 (natural rules for the propositional calculus with equality) consists of $N_0 + (=)$ together with the axioms $a = a$.

3.2. *Upper bound for the monadic case*

3.2.1. Lemma. *If $F \vdash G$ has an S_1 + cut-derivation of length $\leq n$ with cuts only on prime formulae, then $F \vdash^{2^n}_{S_1} G$.*

Proof. By induction on n. We shall prove a much more general result in Section 5.

3.2.2. Let $P_1 \cdots P_n$ be fixed unary relation symbols; a type σ is any subset of $\{P_1, \ldots, P_n\}$. The language $L(P_1 \cdots P_n)$ is built up from $P_1, \ldots, P_n$, typed individual parameters $u^{\sigma_1}, v^{\sigma_2}, \ldots$ (types are unique), individual variables $x, y, z, \ldots$, $\rightarrow$, $\perp$, and $\forall$. The calculus $S_1(P_1 \cdots P_n)$ has as axioms $F \cup \{\perp\} \vdash G$, $F \vdash G \cup \{P_i u^\sigma\}$ for $P_i \notin \sigma$ and $F \cup \{P_i u^\sigma\} \vdash G$ for $P_i \in \sigma$, and as rules $(\vdash \rightarrow)$, $(\rightarrow \vdash)$, $(\forall \vdash)$, and

$$(\vdash \forall(P_1 \cdots P_n)) \quad \frac{F \vdash G \cup \{A(u_1^{\sigma_1})\} \cdots F \vdash G \cup \{A(u_m^{\sigma_m})\}}{F \vdash G \cup \{\forall x\, A(x)\}}$$

where $\sigma_1 \cdots \sigma_m$ is an enumeration of all types ($m = 2^n$), and $u_i^{\sigma_i}$ does not occur in the conclusion.

3.2.3. If $F \vdash G$ is an $L(P_1 \cdots P_n)$-sequent its interpertation $F^* \vdash G^*$ (this is an abuse of notation since F^* may depend on G and G^* on F) is defined as follows; let $u_1^{\sigma_1} \cdots u_m^{\sigma_m}$ be the parameters occurring in $F \vdash G$ and set $\vartheta =_{\mathrm{df}} \mathrm{Sub} \cdots_{a_i}^{u_i} \cdots$, then $F^* =_{\mathrm{df}} \vartheta F \cup \{P_j u_i : P_j \notin \sigma_i\}$ and $G^* =_{\mathrm{df}} \vartheta G \cup \{P_j u_i : P_j \in \sigma_i\}$.

3.2.4. Lemma. *If $F^* \vdash G^*$ is valid, then $F \vdash_{\overline{S_1(P_1 \cdots P_n)}} G$.*

Proof. The usual completeness proof for semantic tableaux.

3.2.5. Formulae A and B of $L(P_1 \cdots P_n)$ are called similar, in symbols $A \doteq B$, if letting $u_1^{\sigma_1} \cdots u_m^{\sigma_m}$ be all the occurrences of parameters in A from left to right so $A = A(u_1^{\sigma_1}, \ldots, u_m^{\sigma_m})$ we have $B = A(v_1^{\sigma_1}, \ldots, v_m^{\sigma_m})$ for some $v_1^{\sigma_1} \cdots v_m^{\sigma_m}$ (note that this definition permits $u_i^{\sigma_i} = u_j^{\sigma_j}$ and $v_i^{\sigma_i} \neq v_j^{\sigma_j}$, and $u_i^{\sigma_i} \neq u_j^{\sigma_j}$ and $v_i^{\sigma_i} = v_j^{\sigma_j}$ provided $\sigma_i = \sigma_j$). $L(P_1 \cdots P_n)$-sequents $F \vdash G$ and $H \vdash J$ are called similar if $F/\doteq = H/\doteq$ and $H/\doteq = J/\doteq$.

3.2.6. Lemma. *Suppose $F \vdash G$ is an $L(P_1 \cdots P_n)$-sequent with $\mathrm{lh}(F) + \mathrm{lh}(G) = m$, then at most $2_2^{(n+1)m+1}$ similarity types of sequents occur in any $S_1(P_1 \cdots P_n)$-derivation of $F \vdash G$.*

Proof. This is the so called "subformula property" for cut-free derivations.

3.2.7. Lemma. *For any parameters $u_1^{\sigma}, u_2^{\sigma}$ and any $L(P_1 \cdots P_n)$-sequent $F \vdash G$,*

$$\mathrm{Sub}_{v}^{u_1^{\sigma}} F \vdash^{m}_{S_1(P_1 \cdots P_n)} \mathrm{Sub}_{v}^{u_1^{\sigma}} G \Leftrightarrow \mathrm{Sub}_{v}^{u_2^{\sigma}} F \vdash^{m}_{S_1(P_1 \cdots P_n)} \mathrm{Sub}_{v}^{u_2^{\sigma}} G.$$

Proof. By induction on m.

3.2.8. Lemma. *For an $L(P_1 \cdots P_n)$-sequent $F \vdash G$; if $\mathrm{lh}(F) + \mathrm{lh}(G) = m$ and $F \vdash_{S_1(P_1 \cdots P_n)} G$, then $F \vdash^{2^k}_{S_1^2(P_1 \cdots P_n)} G$ where $k = 2^{(n+1)m+1} + \log\log(n)$.*

Proof. This follows easily from Lemmas 3.2.6 and 3.2.7.

3.2.9. Lemma. *For an $L(P_1 \cdots P_n)$-sequent $F \vdash G$; $F \vdash^{m}_{S_1(P_1 \cdots P_n)} G \Rightarrow F^* \vdash^{2^k}_{S_1} G^*$ where $k = 2^n \cdot m$.*

Proof. Let D be an $S_1(P_1 \cdots P_n)$-derivation of $F \vdash G$. Obtain an S_1 + cut-derivation of $F^* \vdash G^*$, D^*, by replacing each sequent $H \vdash J$ by $H^* \vdash J^*$ and each $(\vdash \forall(P_1 \cdots P_n))$ by the obvious binary tree of cuts on prime formulae followed by $(\vdash \forall)$. Now apply Lemma 3.2.1 to D^*.

3.2.10. Proposition. *If $F \vdash G$ is a valid monadic sequent and $\mathrm{lh}(F) + \mathrm{lh}(G) = n$, then $F \vdash^{2^{p(n)}}_{S_1} G$ for a suitable quadratic polynomial $p(x)$.*

Proof. Given $F \vdash G$ let A be the universal closure of its interpertation (under the definition of 2.1.2) and apply Lemmas 3.2.8 and 3.2.9 to the sequent $\emptyset \vdash \{A\}$. The proposition now follows from the so called "inversion theorem" (for $\forall$).

3.3. *Bounds for the general case*

3.3.1. In Section 5 we shall prove that there is a recursive function m such that

(a) $\vdash^{n}_{N_1} A \Rightarrow \emptyset \vdash^{m(n)}_{S_1} A$, and
(b) if F is a finite set of equations, then $\forall F \vdash^{n}_{NE_1} E \Rightarrow \mathrm{Sub}\, F \vdash^{m(n)}_{NE} E$.

This result will be used below.

3.3.2. Lemma. *The relation* $\emptyset \vdash^{n}_{S_1} \{A\}$ *is decidable.*

Proof. As in Richardson [31].

3.3.3. Proposition. *There are functions* m_1, m_2 *such that*

(a) *if* A *is valid, then* $\vdash^{m_1(\mathrm{lh}(A))}_{N_1} A$, *and*
(b) *if* A *is valid (with equality), then* $\vdash^{m_2(\mathrm{lh}(A))}_{\mathrm{NE}_1} A$.

Proof. There are notions $\doteq_1$, $\doteq_2$ of similarity between formulae satisfying

(i) length is a property of $\doteq_i$-types,
(ii) there are only finitely many $\doteq_i$-types of length $\leq n$,
(iii) $A \doteq_1 B \Rightarrow (\vdash^{n}_{N_1} A \Leftrightarrow \vdash^{n}_{N_1} B)$, and
(iv) $A \doteq_2 B \Rightarrow (\vdash^{n}_{\mathrm{NE}_1} A \Leftrightarrow \vdash^{n}_{\mathrm{NE}_1} B)$.

3.3.4. Proposition. *For any* m_i *satisfying Proposition* 3.3.3 *we have* $\emptyset'$ *is recursive in* m_i; *moreover, for the optimal such* m_i *we have* m_i *is recursive in* $\emptyset'$.

Proof. For $i=1$ the proposition follows from 3.3.1(a) and Lemma 3.3.2. Let $i=2$. Now any word problem for a finitely generated, finitely presented semigroup is equivalent to the validity of a formula of the form $\&\forall F \rightarrow E$, for F a finite set of equations, where $F \cup \{E\}$ is symmetric and contains only unary function symbols. Thus the proposition follows from 1.3.2 and 3.3.1(b).

4. Speed-up by the predicate calculus

4.1. *Preliminaries*

4.1.1. We consider formulae of predicate logic as in 3.1.1. The notion of a relation term is defined as follows: U is a relation term for each relation symbol U; $\lambda x_1 \cdots x_n A(x_1, \ldots, x_n)$ is a relation term for each formula $A(u_1, \ldots, u_n)$.

4.1.2. The logical complexity of a formula A, $\lg(A)$, is the number of occurrences of logical operations and prime pseudo-formulae in A. $\lg(U) =_{\mathrm{df}} 1$, and $\lg(\lambda x_1 \cdots x_n A(x_1, \ldots, x_n)) =_{\mathrm{df}} \lg(A(u_1, \ldots, u_n))$.

4.1.3. In this section we shall make use of a very special notion of substitution. A substitution θ is a map from relation symbols to relation terms such that

(i) $\mathrm{dom}\,\theta =_{\mathrm{df}} \{U : \theta U \neq U\}$ is finite,
(ii) $\mathrm{arity}(\theta U) = \mathrm{arity}(U)$, and
(iii) if $\theta U = \lambda x_1 \cdots x_n A$, then x_i actually occurs in A.

θ induces a map from relation terms to relation terms and from N_1-derivations to N_1-derivations in the obvious way. Both of these maps will also be denoted "θ".

If $\mathrm{dom}\,\theta \subseteq \{U_1, \ldots, U_n\}$, then we write $\theta = \mathrm{Sub}_{U_1}^{\theta U_1} \cdots_{U_n}^{\theta U_n}$ in the usual way.

4.1.4. If θ and ϕ are substitutions, then $\theta\phi$ is their composition and $\theta + \phi$ is the substitution defined by

$$\begin{aligned}(\theta+\phi)U &= \phi U \quad \text{if} \quad U \in \mathrm{dom}\,\phi,\\ &= \theta U \quad \text{if} \quad U \notin \mathrm{dom}\,\phi.\end{aligned}$$

If F_i is a finite set of relation terms and $F = F_1 \cdots F_n$, then $\theta \upharpoonright F$ is the substitution defined by

$$\begin{aligned}(\theta \upharpoonright F)U &= \theta U \quad \text{if } U \text{ occurs in a member of some } F_i,\\ &= U \quad \text{otherwise.}\end{aligned}$$

We say that θ unifies F if for each $1 \leq i \leq n$, $\mathrm{card}\,(\theta'' F_i) = 1$.

4.1.5. If F_i is a finite set of relation terms and $F = F_1 \cdots F_n$, then $\lg(F)$ is the maximum logical complexity of a relation term belonging to some F_i and $\mathrm{rel}\,(F)$ is the total number of relation symbols occurring in members of the F_i.

4.1.6. If θ is a subsitution, then $\lg(\theta) =_{\mathrm{df}} \max\{\lg(\theta U): U \in \mathrm{dom}\,\theta\}$. Note that $\lg(\theta\phi) \leq \lg(\theta) \cdot \lg(\phi)$ and $\lg(\theta F) \leq \lg(\theta) \cdot \lg(F)$ where $\theta F =_{\mathrm{df}} \theta'' F_1 \cdots \theta'' F_n$.

4.2. *Upper bound*

4.2.1. Lemma. *Suppose that F_i is a finite set of formulae, $F = F_1 \cdots F_n$, and θ unifies F, then there are substitutions ϕ_1, ϕ_2 such that*

(1) *ϕ_1 unifies F,*
(2) *$\theta \upharpoonright F = (\phi_2\phi_1) \upharpoonright F$, and*
(3) *$\lg(\phi_1) \leq \lg(F)^m$ where $m = 2^{\mathrm{rel}(F)}$.*

Proof. Let $F^1 =_{\mathrm{df}} F$ and $\phi_2^0 =_{\mathrm{df}} \theta$; we construct F^i, ϕ_2^i, ϕ_1^i for $1 \leq i \leq k$ satisfying

(i) $F^{i+1} = \phi_1^i F^i$,
(ii) $\phi_2^{i-1} \upharpoonright F^i = (\phi_2^i \phi_1^i) \upharpoonright F^i$,
(iii) ϕ_1^k unifies F^k,
(iv) $\mathrm{rel}\,(F^i) = \mathrm{rel}\,(F) - i + 1$, and
(v) $\lg(\phi_1^i) \leq \lg(F^i)$.

Given such ϕ_2^i and ϕ_1^i the desired substitutions are obtained by setting $\phi_2 =_{\mathrm{df}} \phi_2^k$ and $\phi_1 =_{\mathrm{df}} \phi_1^k \cdots \phi_1^1$.

Suppose that F^i and ϕ_2^{i-1} have been defined, $F^i = F_1^i \cdots F_n^i$, and $\mathrm{card}\,(F_j^i) \neq 1$. Select A_1, A_2 from F_j^i such that $A_1 \neq A_2$. Assuming that A_1 and A_2 are written in Polish notation, let B_1 resp. B_2 be the pseudo-subformulae beginning with the first symbols at which they differ. Since ϕ_2^{i-1} unifies F_i^1 either B_1 or B_2 is prime and $\neq\perp$. W.l.o.g. suppose that $B_1 = Ua_1 \cdots a_m$ and $B_2 = B(U_1 b_1^1 \cdots b_{n_1}^1, \ldots, U_l b_1^l \cdots b_{n_l}^l)$ indicating the prime pseudo-formula occurrences in B_2 from left to right. Note that if U_q exists, then $U \neq U_q$ because of our special notion of substitution. Since $\phi_2^{i-1} B_1 = \phi_2^{i-1} B_2$ we have $\phi_2^{i-1} B_1 = B(C_1, \ldots, C_l)$ where $C_q = (\phi_2^{i-1} U_q) b_1^q \cdots b_{n_q}^q$. Let $C_q = C_q^*(t_1^q, \ldots, t_{k_q}^q)$ indicating the maximal occurrences (from left to right) of pseudo-terms not containing variables bound in C_q at their occurrence, then $\phi_2^{i-1} U$ has the form $\lambda x_1 \cdots x_m B(C_1^*(d_1^1, \ldots, d_{k_1}^1), \ldots, C_l^*(d_1^l, \ldots, d_{k_l}^l))$ and $\phi_2^{i-1} U_q$ has the form $\lambda y_1^q \cdots y_{n_q}^q C_q^*(e_1^q, \ldots, e_{k_q}^q)$ where

$$\operatorname*{Sub}_{x_1 \cdots x_m}^{a_1 \cdots a_m} d_p^q = t_p^q = \operatorname*{Sub}_{y_1^q \cdots y_{n_q}^q}^{b_1^q \cdots b_{n_q}^q} e_p^q.$$

Let $V_1 \cdots V_l$ be new relation symbols satisfying

(a) arity $(V_q) = k_q$, and
(b) $V_p = V_q \Leftrightarrow U_p = U_q$.

Let $T =_{\mathrm{df}} \lambda x_1 \cdots x_m B(V_1 d_1^1 \cdots d_{k_1}^1, \ldots, V_l d_1^l \cdots d_{k_l}^l)$, set $T_q =_{\mathrm{df}} \lambda y_1^q \cdots y_{n_q}^q V_q e_1^q \cdots e_{k_q}^q$, and put $T_q^* =_{\mathrm{df}} \lambda z_1 \cdots z_{k_q} C_q^*(z_1, \ldots, z_{k_q})$. Finally, define

$$\phi_1^i = \operatorname*{Sub}_{UU_1 \cdots U_l}^{TT_1 \cdots T_l}$$

and

$$\phi_2^i = (\phi_2^{i-1} \restriction (\operatorname{dom} \phi_2^{i-1} - [\{U\} \cup \{U_q \mid 1 \leq q \leq l\}])) + \operatorname*{Sub}_{V_1 \cdots V_l}^{T_1^* \cdots T_l^*}.$$

Conditions (ii)–(v) are easily checked.

4.2.2. Proposition. *For each N_1-derivation D there is an N_1-derivation D^* and a substitution θ such that*

(1) $D = \theta D^*$, *and*
(2) *if A occurs in D^*, then* $\lg(A) \leq 3^n$ *where* $n = 2^{3 \cdot \mathrm{H}(D)-1} + 1$.

Proof. Let w be an injective assignment of 0-ary relation symbols to the formula occurrences of D: to each inference in D we assign a sequence of finite sets of formulae as follows;

$$(A) \neq \emptyset$$

$$\frac{B}{A \to B} \mapsto \{w(C) \to w(B) \colon C \in (A)\} \cup \{w(A - B)\},$$

$$\frac{B}{A \to B} \mapsto \{U \to w(B), w(A \to B) \colon U \text{ a new 0-ary relation symbol}\},$$

$$\frac{\begin{matrix}(\neg A)\\ \perp\end{matrix}}{A} \mapsto \{w(\perp), \perp\} \quad \{w(C): C \in (\neg A)\} \cup \{w(A) \to \perp\},$$

$$\frac{A \to B \qquad A}{B} \mapsto \{w(A) \to w(B), w(A \to B)\},$$

$$\frac{A(u)}{\forall x\, A(x)} \mapsto \{w(A(u)), Uu\} \quad \{w(\forall x\, A(x)), \forall x\, Ux\}$$

for U a new 1-ary relation symbol u a proper parameter,

$$\frac{A}{\forall x\, A} \mapsto \{w(A), U\} \quad \{w(\forall x\, A), \forall x\, U\}$$

for U a new 0-ary relation symbol,

$$\frac{\forall x\, A(x)}{A(a)} \mapsto \{w(A(a)), Ua\} \quad \{w(\forall x\, A(x)), \forall x\, Ux\}$$

for U a 1-ary relation symbol x occurs in $A(x)$,

$$\frac{\forall x\, A}{A} \mapsto \{w(A), U\} \quad \{w(\forall x\, A), \forall x\, U\}$$

for U a new 0-ary relation symbol.

Let F be the sequence of all such sets, then there is a substitution θ such that θ unifies F and for each occurrence A in D we have $A = \theta w(A)$. By Lemma 4.2.1 there are ϕ_1, ϕ_2 satisfying the conditions stated there; let D^* result from D by replacing each formula occurrence A by $\phi_1 w(A)$ (D^* is an N_1-derivation by 4.1.3(iii)).

4.2.3. Proposition. *For quantifier-free* A, $\vdash^{n}_{N_1} A \Rightarrow \vdash^{2^{l(n)}}_{N_0} A$ *for l a suitable linear function.*‡

Proof. By Proposition 4.2.2 for quantifier-free A, $\vdash^{n}_{N_1} A \Rightarrow$ there is a valid quantifier-free B with $\lg(B) \leq 3^m$ where $m = 2^{3\cdot n+1}+1$ such that A is a substitution instance of B. It is obvious that $\emptyset \vdash^{n}_{S_0} \{B\} \Rightarrow \vdash^{l(n)}_{N_0} B$ for a suitable linear l; thus the proposition follows from 2.2.1.

4.3. *Lower bound*

4.3.1. Let 1 and 2 be constants, ( ) a binary function symbol, and U an unary relation symbol. To each sequence s of 1's, 2's, parameters and variables we assign a pseudo-term a_s as follows: $a_\emptyset =_{df} 1$; $a_{ts} =_{df} (ta_s)$.

If A is a quantifier-free formula, let t^*A be the result of replacing each maximal a_s in A by a_{ts}. If $s = t_1 \cdots t_n$, then we set $s^*A =_{df} t_1^*(\cdots(t_n^*A)\cdots)$. Let $A_1 =_{df} Ua_\emptyset \to Ua_\emptyset$ and set $A_{k+1} =_{df} (1^*A_k \to (2^*A_k \to Ua_\emptyset)) \to Ua_\emptyset$.

‡ By a more refined "unification" algorithm $2_3^{l(n)}$ can be replaced by $2_2^{l(n)}$.

4.3.2. Lemma. $\vdash^{11n}_{N_1} A_n$.

Proof. Let $s = u_1 \cdots u_m$ and define N_1-derivations $D_k(s)$ as follows:

$$D_1(s) =_{\mathrm{df}} \dfrac{[s^* Ua_\emptyset]^1}{s^* Ua_\emptyset \rightarrow s^* Ua_\emptyset}$$

and $D_{k+1}(s) =_{\mathrm{df}}$

$$\dfrac{\dfrac{\dfrac{s^*1^*A_k \rightarrow ([s^*2^*A_k]^1 \rightarrow s^*Ua_\emptyset) \qquad \dfrac{\forall x\, s^*x^*A_k}{s^*1^*A_k}}{s^*2^*A_k \rightarrow s^*Ua_\emptyset} \qquad \dfrac{\forall x\, s^*x^*A_k}{s^*2^*A_k}}{s^*Ua_\emptyset}}{s^*A_{k+1}}\,1$$

Now let $D^1(s) =_{\mathrm{df}} D_1(s)$ and set $D^{k+1}(s) =_{\mathrm{df}}$

$$\dfrac{\dfrac{\begin{matrix}[\forall x\, s^*x^*A_k]^1 \\ D_{k+1}(s) \\ s^*A_{k+1}\end{matrix}}{(\forall x\, s^*x^*A_k) \rightarrow s^*A_{k+1}}\,1 \qquad \dfrac{D^k(su)}{\forall x\, s^*x^*A_k}}{s^*A_{k+1}}$$

for u a new parameter. The desired N_1-derivation of A_n is $D^n(\emptyset)$.

4.3.3. Lemma. $\vdash^{m}_{N_0} A_n \Rightarrow 2^{n-2} - 1 \leq m$.

Proof. For each sequence s of 1's and 2's of length k, A_{k+1} contains a subformula of the form $Ua_s \rightarrow Ua_s$. For each such s this subformula must occur in any N_0-derivation of A_{k+1} since the result of replacing it by a new 0-ary relation symbol is not valid.

4.3.4. Proposition. *There is no polynomial $p(x)$ such that for quantifier-free A, $\vdash^{n}_{N_1} A \Rightarrow \vdash^{p(n)}_{N_0} A$.*

4.4. *Normalization procedures*

4.4.1. Proposition 4.2.3 cannot be obtained by the analysis of Prawitz [30] normalization procedure as this procedure is super-exponential w.r.t. length. This can be easily seen from the corresponding fact for the typed λ-calculus through Howard's derivations as terms construction (Howard [14]). The fact for the typed λ-calculus follows easily from the observation that

$$(\cdots \underbrace{(mm) \cdots)m}_{n \text{ occurrences}}$$

where

$$\mathbf{n} =_{\mathrm{df}} \lambda yxy\underbrace{(\cdots(yx)\cdots)}_{n \text{ occurrences}}$$

is a term of the typed system (see [2, p. 10]).

4.4.2. In contrast to 4.4.1, we shall show in Section 5 that the analysis of Prawitz [30] normalization procedure does give the right order of magnitude for speed-up by the predicate calculus with equality.

5. Speed-up by the predicate calculus with equality

5.1. *Upper bound*

5.1.1. For what follows we refer the reader to Prawitz [30].

5.1.2. An NE_1-derivation is called normal if it does not contain any of the following combinations of inferences;

(a) an $\to I$ whose conclusion is the major premiss of an $\to E$,
(b) a $\forall I$ whose conclusion is the premiss of a $\forall E$,
(c) a $\perp$ whose conclusion is the major premiss of an elimination,
(d) an $=$ whose conclusion is the major premiss of an elimination, and
(e) an $=$ whose major (left) premiss is the conclusion of an introduction.

5.1.3. Lemma. *If F is a finite set of equations and there is a normal NE_1-derivation of E from $\forall F$ of length $\leq n$, then* $\mathrm{Sub}\, F \vdash^{n}_{\mathrm{NE}} E$.

Proof. Prove by induction on n the following; if G is a finite set of equations and there is a normal NE_1-derivation of E' or $\perp$ from $\forall F \cup \neg G$, then for some $E \in G \cup \{E'\}$ we have $\mathrm{Sub}\, F \vdash^{n}_{\mathrm{NE}} E$.

5.1.4. Lemma. *If there is a normal N_1-derivation of A of length $\leq n$, then* $\emptyset \vdash^{l(n)}_{S_1} \{A\}$ *for a suitable linear l.*

Proof. Straightforward

5.1.5. Consider the reductions II.3.3.1.3 and II.3.3.1.4 of Prawitz [30]; these are defined on NE_1-derivations as well as the ones considered there. We denote the corresponding reducibility relation by "$>$".

5.1.6. Lemma. *If there is a normal NE_1-derivation D^* such that $D \geq D^*$, then* $\mathrm{lh}\,(D^*) \leq 2^{\mathrm{lh}\,(D)}_{\mathrm{lh}\,(D)\cdot 2+1}$.

Proof. By Prawitz [30, II.3.5.3] it suffices to find a sequence $D = D_0 \geq D_1 \geq \cdots \geq$

D_n such that D_n is normal, $n \leqslant \mathrm{lh}(D)$, and $\mathrm{lh}(D_{i+1}) \leqslant 2^{\mathrm{lh}(D_i)}$. If A occurs in D_i let $\mathrm{rnk}_i(A) =_{\mathrm{df}} 1 + \max\{\mathrm{rnk}_i(B): B$ occurs in D_i and $\lg(B) < \lg(A)\}$ and set $\mathrm{rnk}(i) =_{\mathrm{df}} \max\{\mathrm{rnk}_i(A): A$ is a maximal formula of $D_i\}$. Obtain D_{i+1} from D_i by eliminating (from top to bottom) all maximal formulae of maximum rnk_i, then $\mathrm{lh}(D_{i+1}) \leqslant 2^{\mathrm{lh}(D_i)}$ and $\mathrm{rnk}(i+1) < \mathrm{rnk}(i) \leqslant \mathrm{lh}(D)$ so we have the desired sequence by [30, II.3.5.3].

5.1.7. We define the notion of an expansion as follows

$$\dfrac{\begin{matrix}(\neg(A\to B))\\ D\\ \bot\end{matrix}}{A\to B}\quad\mapsto\quad \cfrac{\cfrac{\cfrac{\cfrac{\begin{matrix}(\neg\cancel{(A\to B)}^{3})\\ D\\ \bot\end{matrix}}{\neg\neg(A\to B)}{}^{3}\qquad \cfrac{\cfrac{\cancel{\neg B}^{2}\quad \cfrac{\cancel{A\to B}^{4}\quad \cancel{A}^{4}}{B}}{\bot}}{\neg(A\to B)}{}^{1}}{\bot}}{B}{}^{2}}{A\to B}{}^{4}$$

$$\dfrac{\begin{matrix}(\neg\forall x\, A(x))\\ D\\ \bot\end{matrix}}{\forall x\, A(x)}\quad\mapsto\quad \cfrac{\cfrac{\cfrac{\cfrac{\begin{matrix}(\neg\cancel{\forall x\, A(x)}^{2})\\ D\\ \bot\end{matrix}}{\neg\neg\forall x\, A(x)}{}^{2}\qquad\cfrac{\cfrac{\cancel{\neg A(u)}^{3}\quad \cfrac{\cancel{\forall x\, A(x)}^{1}}{A(u)}}{\bot}}{\neg\forall x\, A(x)}{}^{1}}{\bot}}{A(u)}{}^{3}}{\forall x\, A(x)}$$

$$\dfrac{\begin{matrix}D_1\\ \forall x\, A(x,a)\end{matrix}\qquad \begin{matrix}D_2\\ a\ominus b\end{matrix}}{\forall x\, A(x,b)}\quad\mapsto\quad \cfrac{\cfrac{\cfrac{\begin{matrix}D_1\\ \forall x\, A(x,a)\end{matrix}}{A(u,a)}\qquad\begin{matrix}D_2\\ a\ominus b\end{matrix}}{A(u,b)}}{\forall x\, A(x,b)}$$

$$\dfrac{\begin{matrix}D_1\\ A(a)\to B(a)\end{matrix}\qquad \begin{matrix}D_2\\ a\ominus b\end{matrix}}{A(b)\to B(b)}$$

$$\mapsto\quad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\begin{matrix}D_1\\ A(a)\to B(a)\end{matrix}\qquad \cfrac{\cancel{A(b)}^{1}\quad \cancel{a\ominus b}^{2}}{A(a)}}{B(a)}\quad \cancel{a\ominus b}^{2}}{B(b)}}{A(b)\to B(b)}{}^{1}}{a\ominus b\to(A(b)\to B(b))}{}^{2}\qquad \begin{matrix}D_2\\ a\ominus b\end{matrix}}{A(b)\to B(b)}$$

The immediate expandibility and expandibility relations are defined similarly to

[30, II.3.4.1 and II.3.4.2]. The expandibility relation is denoted "$<$" (the converse of $>$ will never be used).

5.1.8. We define a propositional system NE_1^* in which we shall simulate NE_1. The formulae of NE_1^* are built up from propositional parameters $U, \dots$, the propositional constants $\perp$ and E^*, $\rightarrow$, and the unary connective constant $\forall^*$. The rules of NE_1^* are $\rightarrow I$, $\rightarrow E$, $\perp$,

$$(\forall^* I) \quad \frac{A}{\forall^* A},$$

$$(\forall^* E) \quad \frac{\forall^* A}{A},$$

and

$$(=^*) \quad \frac{A \qquad E^*}{A},$$

together with the axiom $\forall^* E^*$.

The notions of reduction, expansion, and normal derivation are defined for NE_1^* just like those for NE_1^*. The corresponding reducibility and expandibility relations are denoted "$>^*$" and "$^*<$" resp.

5.1.9. Lemma. *For each NE_1-derivation D there is an NE_1^*-derivation D^* such that*

(a) $D^* >^* D_1 \Leftrightarrow$ *there is a* D_2 *s.t.* $D_1 = D_2^*$ *and* $D > D_2$,
(b) $D^* {}^*< D_1 \Leftrightarrow$ *there is a* D_2 *s.t.* $D_1 = D_2^*$ *and* $D < D_2$,
(c) D^* *is normal* $\Leftrightarrow D$ *is normal, and*
(d) $\mathrm{lh}\,(D^*) = \mathrm{lh}\,(D)$.

Proof. To obtain D^* from D perform the following operations (in the order given);

(i) replace each maximal occurrence of a pseudo-term by 0,

(ii) replace each subformula occurrence of $0 = 0$ by E^* and each subformula occurrence of $V0 \cdots 0$ by U (in such a way that the correspondence $V \mapsto U$ is $1-1$),

(iii) replace $\forall x$ throughout by $\forall^*$.

The relation between D and D^* will be further analyzed in Section 6; in (a)–(d) we have just listed the properties used below.

5.1.10. In this section a substitution θ is a map from propositional parameters to propositional formulae such that $\mathrm{dom}\,\theta =_{df} \{U : \theta U \neq U\}$ is finite. We adopt freely the definitions of Section 4 for this notion of a substitution, and write "pm" for "rel" (note that here $\mathrm{lg} = \mathrm{lh}$).

5.1.11. Lemma. *Suppose that $F = F_1 \cdots F_n$ is a sequence of finite sets of formulae and there is some unifier of F, then there is a θ such that*

(a) *θ unifies F,*
(b) *for any unifier ϕ of F there is a ϕ' s.t. $\phi \restriction F = (\phi'\theta) \restriction F$, and*
(c) $\mathrm{lh}(\theta) \leq \mathrm{lh}(F)^m$ *where* $m = 2^{\mathrm{pm}(F)}$.

Proof. Although like 4.2.1 we give the proof in order to see how the strengthening is achieved. Let $F^1 =_{\mathrm{df}} F$; we define F^i, θ^i s.t.

(i) $F^{i+1} = \theta^i F^i$,
(ii) $\mathrm{pm}(F^{i+1}) = \mathrm{pm}(F) - i + 1$,
(iii) for some k, θ^k unifies F^k,
(iv) if ϕ unifies F^i then $\phi = \phi\vartheta_i$, and
(v) $\mathrm{lh}(\theta^i) = \mathrm{lh}(F^i)$.

Given such θ^i the desired θ is $\theta^k \cdots \theta^1$.

Suppose that F^i has been defined, $F^i = F^i_1 \cdots F^i_n$, and $\mathrm{card}(F^i_j) \neq 1$. Select A_1, A_2 from F^i_j such that $A_1 \neq A_2$. Assuming A_1 and A_2 are written in Polish notation, let B_1 resp. B_2 be the subformulae beginning with the first symbols at which they differ. It follows from (i), (iv), and the assumption that F has a unifier that F^i has a unifier. Hence either B_1 or B_2 is a propositional parameter. W.l.o.g. suppose that $B_1 = U$. Now if $\phi A_1 = \phi A_2$, then $\phi U = \phi B_2$ and U does not occur in B_2. Thus it suffices to put $\theta^i =_{\mathrm{df}} \mathrm{Sub}^{B_2}_U$.

5.1.12. Proposition. *For each NE_1^*-derivation D there is an NE_1^*-derivation D^+ and a substitution θ such that*

(a) *$D = \theta D^+$, and*
(b) *if A occurs in D^+, then $\mathrm{lh}(A) \leq 3^n$ where $n = 2^{3 \cdot \mathrm{lh}(D)+1} + 1$.*

Proof. Just like 4.2.2.

5.1.13. Lemma. *Suppose that for NE_1^*-derivations D_1 and D_2, and the substitution θ we have $D_1 = \theta D_2$, then*

(a) *if $D_2 {}^*\!< D$, then $D_1 {}^*\!< \theta D$,*
(b) *if $D_2 >^* D$, then $D_1 >^* \theta D$,*
(c) *D_1 is normal $\Leftrightarrow$ D_2 is normal, and*
(d) $\mathrm{lh}(D_1) = \mathrm{lh}(D_2)$.

Proof. Obvious.

5.1.14. Lemma. *Suppose that D is an NE_1^*-derivation such that each of its $\bot$ and $=^*$ inferences have prime conclusions, then there is a normal D^0 such that $D \geq^* D^0$.*

Proof. Just like 5.1.6.

5.1.15. Lemma. *Suppose that D is an NE_1^*-derivation such that if A occurs in D, then $\mathrm{lh}(A) \leqslant n$, then there is a D^0 of length $\leqslant 7 \cdot n \cdot \mathrm{lh}(D)$ such that $D^* \preccurlyeq D^0$ and the conclusion of any $\perp$ or $=^*$ inference in D^0 is prime.*

Proof. Plain.

5.1.16. Proposition. *For each NE_1-derivation D_1 there are D_2 and D_3 such that*

(a) $D_1 \preccurlyeq D_2$,
(b) $\mathrm{lh}(D_2) \leqslant 2_2^{l(\mathrm{lh}(D_1))}$ *for a suitable linear function l,*
(c) $D_2 \succcurlyeq D_3$, *and*
(d) D_3 *is normal.*

Proof. Consider the following diagram:

$$\begin{array}{ccccc}
D_1 & \overset{*}{\mapsto} & D_1^* & \overset{\theta}{\hookleftarrow} & D_1^{*+} \\
\curlywedge\ 5.1.9 & & \overset{*\ \ddot{o}}{\curlywedge}\ 5.1.13 & & \overset{*}{\curlywedge}\ 5.1.15 \\
D_2 & \overset{*}{\mapsto} & \theta(D_1^{*+0}) & \overset{\theta}{\hookleftarrow} & D_1^{*+0} \\
\curlyvee^{5.1.9} & & \underset{*}{\curlyvee}\ ^{5.1.13} & & \underset{*}{\curlyvee}\ ^{5.1.14} \\
D_3 & \overset{*}{\mapsto} & \theta(D_1^{*+0.}) & \overset{\theta}{\hookleftarrow} & D_1^{*+0.}
\end{array}$$

where $\mathrm{lh}(D_1) = \mathrm{lh}(D_1^*) = \mathrm{lh}(D_1^{*+})$ by 5.1.9 and 5.1.13, $\mathrm{lh}(D_2) = \mathrm{lh}(\theta(D_1^{*+0})) = \mathrm{lh}(D_1^{*+0}) \leqslant 7 \cdot n \cdot \mathrm{lh}(D_1^{*+})$ where $n = 3^m$ for $m = 2^{3 \cdot \mathrm{lh}(D^*)+1} + 1$ by 5.1.9, 5.1.12, 5.1.13, and 5.1.15, and $D_1^{*+0.}$; hence by 5.1.13 $\theta(D_1^{*+0.})$ and by 5.1.9 D_3, is normal.

5.1.17. Proposition. *For F a finite set of equations, $\forall F \vdash^{n}_{NE_1} E \Rightarrow \mathrm{Sub}\, F \vdash^{2^{l(n)}_{2^2}}_{NE} E$ for a suitable linear function l.§*

Proof. By Lemmas 5.1.3 and 5.1.6, and Proposition 5.1.16.

5.2. Lower bound

5.2.1. For what follows we refer the reader to Section 1.3.4. Let F be as in 1.3.4 and set $CL^* =_{df} CL \cup F$.

5.2.2. Lemma. *There is a linear function l such that $\forall CL^* \vdash^{l(n)}_{NE_1} E_n$.*

Proof. First we construct auxilliary predicates R_i as follows;

$$R_1 =_{df} \lambda y\, \forall x (Px = (P(yx))),$$

§ By a more refined "unification" algorithm $2^{l(n)}_{2^2}$ can be replaced by $2^{l(n)}_{2}$.

and

$$R_{m+1} =_{df} \lambda y\, \forall z(R_m z \to R_m(yz)).$$

Next let $D(u, v)$ be an NE_1-derivation of $((Tu)v) = (u(uv))$ from $\forall CL^*$. We construct NE_1-derivations D_m, $2 \leqslant m$, of $R_m T$ from $\forall CL^*$ as follows; $D_2 =_{df}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x\, Px = (\overset{1}{P}(ux))}{Pt = (P(uv))} \qquad \dfrac{\forall x\, Px = \overset{1}{(}P(ux))}{(P(uv)) = (P(u(uv)))}}{Pv = (P(u(uv)))} \qquad D(u, v)}{Pc = (P((Tu)v))}}{\forall y\, Py = (P((Tu)y))}}{\forall x\, Px = (P(ux)) \to \forall y\, Py = (\overset{1}{P}((Tu)y))}}{R_2 T}\,\forall I$$

and $D_{m+2} =_{df}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x(R_m x \overset{2}{\to} R_m(ux))}{R_m(uv) \to R_m(u(uv))} \qquad \dfrac{\dfrac{\forall x(R_m x \overset{2}{\to} R_m(ux))}{R_m v \to R_m(uv)} \qquad R_m v}{R_m(uv)}}{R_m(u(uv)) \qquad D(u, v)}}{R_m((Tu)v)}\,{}^{1}}{R_m v \to R_m((Tu)v)}}{\forall y(R_m y \to R_m((Tu)y))}\,{}_{2}}{\dfrac{\forall x(R_m x \to R_m(ux)) \to \forall y(R_m y \to R_m((Tu)y))}{R_{m+2} T}\,\forall I.}$$

Now we construct NE_1-derivations D_m^k, $2 \leqslant m$, of $R_m T_k$ from $\forall CL^*$ with $\mathrm{lh}\,(D_m^k) \leqslant (\mathrm{lh}\,(D(u, v)) + 11)k$. If $k = 1$, then $D_m^k =_{df} D_m$, and if $k = j+2$, then $D_m^k =_{df}$

$$\dfrac{\dfrac{\begin{matrix} D_{m+1}^{j+1} \\ R_{m+1} T_{j+1} \end{matrix}}{R_m T \to R_m(T_{j+1} T)}\,\forall E \qquad D_m}{R_m T_{j+2}}$$

The desired NE_1-derivation of E_n from $\forall CL^*$ is

$$\dfrac{\dfrac{\begin{matrix} D_2^n \\ R_1 Q \to R_1(T_n Q) \end{matrix} \qquad R_1 Q}{R_1(T_n Q)}}{PQ = (P((T_n Q)Q))}\,\forall E$$

5.2.3. Proposition. *For finite sets of equations F; if $\forall F \mid\!\frac{n}{NE_1} E \Rightarrow \mathrm{Sub}\, F \mid\!\frac{m(n)}{NE} E$, then $2^1_{[n/k]} = O(m(n))$ for a suitable constant k.*

Proof. By Proposition 1.3.4 and Lemma 5.2.2.

5.3. *The sequential case*

5.3.1. By combining the remark in the proof of Proposition 4.2.3 with Lemma 5.1.4 it is easily seen from Section 5.2 that $\emptyset \vdash^{n}_{S_1+\text{cut}} \{A\} \Rightarrow \emptyset \vdash^{2^1_{2^{l(n)}}}_{S_1} \{A\}$ for a suitable linear function l.§

5.3.2. The analogue of Proposition 5.2.3 for S_1+cut is easier to prove than was Proposition 5.2.3.

6. Proof-search in and speed-up by second-order logic

6.1. *Preliminaries*

6.1.1. We consider formulae $A, B, C, \ldots$ of second-order logic built up from arbitrary individual terms, relation parameters (called "relation symbols" in Section 3), individual variables, relation (bound) variables $X, Y, Z, \ldots, \rightarrow, \bot$, and $\forall$ (in addition, for the calculus for equality, the relation constant $=$). We refer the reader to Prawitz [25] for additional syntactic conventions and distinctions (in order to retain "version 2" notation we define $\lambda x_1 \cdots x_n A(x_1, \ldots, x_n) a_1 \cdots a_n = A(a_1, \ldots, a_n)$).

6.1.2. The calculus N_2 (natural rules for second-order logic) is the calculus $C^{2\prime}$ of Prawitz [29] (version 1). It consists of the rules $\rightarrow I$, $\rightarrow E$, $\bot$, $\forall_1 I$ (called "$\forall I$" in Section 3), $\forall_1 E$ (called "$\forall E$" in Section 3),

$$(\forall_2 I) \qquad \frac{A(U)}{\forall X\, A(X)}$$

provided that U does not occur in any assumption, and

$$(\forall_2 E) \qquad \frac{\forall X\, A(X)}{A(T)}$$

for T a relation term of appropriate arity.

6.1.3. The calculus NE_2 (natural rules for second-order logic with equality) is N_2 together with the axiom and rule of equality.

6.1.4. Let $R =_{\text{df}} \lambda xy\, \forall X(Xx \rightarrow Xy)$.

Proposition. *There are linear functions l_1, l_2 such that*

(a) *if A is $=$-free, then* $\vdash^{n}_{NE_2} \text{Sub}^{=}_{U} A \Rightarrow \vdash^{l_1(n)}_{N_2} \text{Sub}^{R}_{U} A$, *and*

§ By a more refined "unification" algorithm $2^1_{2^{l(n)}_2}$ can be replaced by $2^1_{2^{l(n)}}$.

(b) *if A contains no pseudo-subformula of the form Rab, then* $\vdash^{h}_{N_2} \mathrm{Sub}^R_U A \Rightarrow \vdash^{l_2(n)}_{NE_2} \mathrm{Sub}^{=}_U A$.

Proof. (a) is straightforward, and (b) follows easily from the following properties of substitution;

(i) $\mathrm{Sub}^R_U \mathrm{Sub}^T_V A = \mathrm{Sub}^{\mathrm{Sub}^R_U T}_V \mathrm{Sub}^R_U A$, and
(ii) $\mathrm{Sub}^R_U \mathrm{Sub}^a_u A = \mathrm{Sub}^a_u \mathrm{Sub}^R_U A$.

6.2. *Existence of upper bound for speed-up by N_2*

6.2.1. An N_2-derivation is said to be normal if it satisfies (a), (b), and (c) of Section 5.1.2.

6.2.2. Lemma. *If F is a finite set of first-order formulae and A is first-order, then any normal N_2-derivation of A from F is an N_1-derivation.*

Proof. By induction over the length of a normal N_2-derivation of A from F.

6.2.3. Consider the reductions $\to$reduction, $\forall_1$ reduction, and $\forall_2$ reduction of Prawitz [30, Sections II.3.3.1.3, II.3.3.1.4, and III.5.3]; to these we add the following reduction

$\perp$reduction

$$\dfrac{\dfrac{\begin{matrix}(\neg A)\\ D_1\\ \perp\end{matrix}}{A} \qquad \begin{matrix}D_2\\ B\end{matrix}}{C}\,R \quad\mapsto\quad \dfrac{\begin{matrix}\dfrac{\dfrac{[\neg C]^2 \qquad \dfrac{[A]^1 \qquad \begin{matrix}D_2\\ B\end{matrix}}{C}\,R}{\perp}}{(\neg A)}\,1\\ D_1\\ \perp\end{matrix}}{C}\,2$$

where $R \in \{\to E, \forall_1 E, \forall_2 E\}$ with major premiss A (if $R \neq \to E$, then D_2 does not exist). The corresponding reducibility relation is denoted "$>$".

6.2.4. Two N_2-derivations D_1 and D_2 are isomorphic, in symbols $D_1 \doteq D_2$, if there is a bijection from the formula occurrences and inferences of D_1 onto those of D_2 which

(a) commutes with the conclusion,
(b) commutes with the calcelled assumption occurrences,
(c) commutes with the premisses, and
(d) commutes with the rule of inference, possibly ignoring subscripts on quantifier rules, of each inference in D_1.

6.2.5. Lemma. (a) *Length is a property of* $\doteq$*-types.*

(b) *There are only finitely many* $\doteq$*-types of length* $\leq n$.

(c) *If* $D_1 \doteq D_2$ *and* D_1 *immediately reduces to* D_3, *then there is a* $D_4 \doteq D_3$ s.t. D_2 *immediately reduces to* D_4.

Proof. Straightforward.

6.2.6. We extend the immediate reducibility relation and the reducibility relation to $\doteq$-types as follows; $D_1/\doteq$ imm.red. $D_2/\doteq =_{df}$ there is a $D_3 \doteq D_2$ s.t. D_1 imm. red. D_3, and $D_1/\doteq \succ D_n/\doteq =_{df}$ there are $D_2 \cdots D_{n-1}$ such that $D_i/\doteq$ imm. red. $D_{i+1}/\doteq$ for $1 \leq i \leq n-1$.

6.2.7. Proposition. *Suppose that* $\succ$ *is well-founded (as a relation on* N_2*-derivations) then there is a function m such that* $\vdash^{n}_{N_2} A \Rightarrow \vdash^{m(n)}_{N_1} A$ *for first-order A.*

Proof. For each N_2-derivation D_1 there are only finitely many D_2 such that D_1 imm. red. D_2 (the exact number is not fixed by what we have said so far about N_2-derivations; in particular, the relation term T in 6.1.2 is not uniquely determined by $\forall XA(X)$ and $A(T)$, although there are only finitely many possibilities for it), thus there are only finitely many $D_2/\doteq$ such that $D_1/\doteq$ imm. red. $D_2/\doteq$. Now if $\succ$ is well-founded on derivations, then it is well-founded on $\doteq$-types so there are only finitely many $D_2/\doteq$ such that $D_1/\doteq \succ D_2/\doteq$. In addition, if $D_1 \succ D_2$ and there is no D_3 such that $D_2 \succ D_3$, then D_2 is normal and $D_1/\doteq \succ D_2/\doteq$. Thus if $\succ$ is well-founded on derivations the desired function is given by

$$m(n) =_{df} \max \{\text{lh}(D_2/\doteq)\text{: there is a } D_1/\doteq \text{ of length} \leq n \text{ s.t. } D_1/\doteq \succeq D_2/\doteq\}$$

according to Lemmas 6.2.2 and 6.2.5.

6.2.8. We define a propositional system N_2^* in which we shall simulate N_2. The formulae of N_2^* are built up from propositional parameters (0-ary relation parameters) $U, V, W, \ldots$, propositional variables $X, Y, Z, \ldots$, $\perp$, $\rightarrow$, and $\forall$ (interpreted the universal quantifier over truth values). The rules of N_2^* are those of N_2 less $\forall_1 I$ and $\forall_1 E$. Unlike the case of 5.1.8, N_2^* is a subsystem of N_2 so notions defined for N_2 are defined for N_2^*.

6.2.9. Lemma. *For each* N_2*-derivation D there is an* N_2^**-derivation* D^* *such that* $D \doteq D^*$.

Proof. To obtain D^* from D perform the following operations (in the order given)

(i) replace each maximal occurrence of a pseudo-term by 0,

(ii) replace each subformula occurrence of $V0 \cdots 0$ by U and each pseudo-subformula occurrence of $Y0 \cdots 0$ by X (in such a way that the correspondences $V \mapsto U$, $Y \mapsto X$ are 1–1),

(iii) replace $\forall x$ throughout by $\forall X$ so that the choice of X results in a dummy quantifier,

(iv) replace $\forall Y$ by $\forall X$ according to the correspondence $Y \mapsto X$ of (ii).

6.2.10. Proposition. *If $>$ restricted to N_2^*-derivations is well-founded, then $>$ is well-founded.*

Proof. Lemmas 6.2.5 and 6.2.9.

6.2.11. Let M_2^* be the system obtained from N_2^* by dropping the rule $(\bot)$. It follows easily from appendix B of Prawitz [30] that $>$ restricted to M_2^*-derivations is well-founded. To prove that $>$ is well-founded we shall define a map w from N_2^*-derivations to M_2^*-derivations satisfying $D_1 > D_2 \Rightarrow w(D_1) > w(D_2)$.

6.2.12. Let $R =_{df} \lambda X \neg\neg X \to X$ and let A^R be the result of relativizing the (propositional) quantifiers in A to R. We define certain auxilliary N_2^*-derivations $N(A)$ as follows ($N(A)$ is a derivation of RA^R from assumptions of the form $R\bot$ and RU for U occurring in A); $N(U) =_{df} RU$, $N(\bot) =_{df} R\bot$, $N(A \to B) =_{df}$

$$\dfrac{\dfrac{\dfrac{N(B) \qquad \dfrac{\dfrac{\neg\neg(A \to B)^{R\,4} \qquad \dfrac{\dfrac{\neg B^{R\,2} \qquad \dfrac{(A \to B)^{R\,1} \quad A^{R\,3}}{B^R}}{\bot}}{\neg(A \to B)^R}\,{\scriptstyle 1}}{\bot}}{\neg\neg B^R}\,{\scriptstyle 2}}{B^R}}{A^R \to B^R}\,{\scriptstyle 3}}{\neg\neg(A \to B)^R \to (A \to B)^R}\,{\scriptstyle 4}$$

and $N(\forall X\, A(X)) =_{df}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}(RU)^{3}\\ N(A(U))\end{matrix} \qquad \dfrac{\dfrac{\neg\neg(\forall X\, A(X))^{R\,4} \qquad \dfrac{\dfrac{\neg A(U)^{R\,2} \qquad \dfrac{\dfrac{(\forall X\, A(X))^{R\,1}}{RU \to A(U)^R} \quad RU^{3}}{A(U)^R}}{\bot}}{\neg(\forall X\, A(X))^R}\,{\scriptstyle 1}}{\bot}}{\neg\neg A(U)^R}\,{\scriptstyle 2}}{A(U)^R}}{RU \to A(U)^R}\,{\scriptstyle 3}}{\forall X(RX \to A(X)^R)}}{\neg\neg(\forall X\, A(X))^R \to (\forall X\, A(X))^R}\,{\scriptstyle 4}$$

where (RU) is the set of all uncancelled occurrences of RU as an assumption in $N(A(U))$.

6.2.13. Lemma. *Suppose that (RU) is the set of all uncancelled occurrences of RU and the set of uncancelled assumption occurrences (RB^R) in $\mathrm{Sub}_U^{B^R} N(A(U))$ is defined by $(RB^R) = \mathrm{Sub}_U^{B^R}(RU)$, then $N(A(B)) =$*

$$\begin{array}{c} N(B) \\ (RB^R) \\ \\ \mathrm{Sub}_U^{B^R} N(A(U)) \end{array}$$

Proof. By induction on $\mathrm{lh}(A(U))$.

6.2.14. We now define the map w; w is to be regarded in the obvious way as a 1–1 map from the formula occurrences of D into those of $w(D)$.

$w(A) =_{\mathrm{df}} A^R$.

w commutes with $(\rightarrow I)$ and $(\rightarrow E)$.

$$\begin{array}{c} (\neg \not{A})^1 \\ D \\ \dfrac{\bot}{A}\,1 \end{array} \overset{w}{\mapsto} \dfrac{N(A) \qquad \begin{array}{c} (\neg \not{A}^R)^1 \\ w(D) \\ \dfrac{\bot}{\neg\neg A^R} \end{array}}{A^R}$$

where $(\neg A^R) = w''(\neg A)$.

$$\begin{array}{c} D \\ \dfrac{\forall X\, A(X)}{A(B)} \end{array} \overset{w}{\mapsto} \dfrac{\dfrac{\begin{array}{c} w(D) \\ (\forall X\, A(X))^R \end{array}}{RB^R \rightarrow A(B)^R} \qquad N(B)}{A(B)^R}$$

$$\begin{array}{c} D \\ \dfrac{A(U)}{\forall X\, A(X)} \end{array} \overset{w}{\mapsto} \begin{array}{c} (\not{R}U)^1 \\ w(D) \\ \dfrac{\dfrac{A(U)^R}{RU \rightarrow A(U)^R}\,1}{(\forall X\, A(X))^R} \end{array}$$

where (RU) is the set of all uncancelled occurrences of RU as an assumption in $w(D)$.

6.2.15. Lemma. *Suppose that (RU) is the set of all uncancelled occurrences of RU*

as an assumption in $w(D)$ and the set of uncancelled assumption occurrences (RB^R) in $\mathrm{Sub}_U^{B^R} w(D)$ is defined by $(RB^R) = \mathrm{Sub}_U^{B^R}(RU)$, then $w(\mathrm{Sub}_U^B D) =$

$$\begin{matrix} N(B) \\ (RB^R) \\ \underset{U}{\overset{B^R}{\mathrm{Sub}}}\, w(D) \end{matrix}$$

Proof. By induction on $\mathrm{lh}(D)$ using 6.2.13.

6.2.16. Lemma. *Suppose that (A) is a set of uncancelled assumption occurrences in D_2 and $(A^R) = w''(A)$, then*

$$\begin{matrix} D_1 & & w(D_1) \\ (A) & \overset{w}{\mapsto} & (A^R) \\ D_2 & & w(D_2) \end{matrix}$$

Proof. By induction on $\mathrm{lh}(D_1)$. Note that the lemma may fail if D_2 is not an N_2^*-derivation i.e. if A contains the proper parameter of a $\forall_2 I$ below it.

6.2.17. If D_2 is a reduction of D_1, then there is a function j, defined in the obvious way and uniquely determined by D_1 and D_2, from the uncancelled assumption occurrences of D_2 into those of D_1 which preserves the formula occurring. If D_1 imm. red. D_2, then there is such a j for D_1 and D_2 obtained from the one for the corresponding reduction by restriction and trivial extension (j may no longer be uniquely determined by D_1 and D_2). If $D_1 \cdots D_n$ is a reducibility sequence, then there is such a j for D_1 and D_n obtained from those for the immediate reducibilities $D_i \mapsto D_{i+1}$ by composition. We write $D_1\,\mathrm{red.}^j D_2$, D_1 imm. red.$^j D_2$, and $D_1 >^j D_n$ resp.

Lemma. *Suppose that for all N_2^*-derivations D_1, D_2 we have $D_1\,\mathrm{red.}^j D_2 \Rightarrow$ there is a j_w such that $w(D_1) >^{j_w} w(D_2)$ and $j_w = w \circ j \circ w^{-1}$ on assumption occurrences of $w(D_2)$ for which w^{-1} is defined, then D_1 imm. red. $D_2 \Rightarrow w(D_1) > w(D_2)$.*

Proof. Assume the hypothesis and prove the implication of the hypothesis with "imm. red.^{j}" in place of "red.^{j}" by induction over the inductive definition of D_1 imm. red.$^j D_2$.

We shall make no further mention of the functions j; however, the reader should keep in mind that it is the stronger conditions of the above lemma which must in fact be verified in what follows.

6.2.18. Proposition. D_1 red. $D_2 \Rightarrow w(D_1) > w(D_2)$.

Proof. *Case* 1:

$$
\dfrac{\dfrac{\begin{matrix}(\not{A})^1\\ D_1\\ B\end{matrix}}{A\to B}\,1 \qquad \begin{matrix}D_2\\ A\end{matrix}}{B}
\quad \overset{w}{\mapsto} \quad
\dfrac{\dfrac{\begin{matrix}(\not{A}^R)^1\\ w(D_1)\\ B^R\end{matrix}}{A^R\to B^R}\,1 \qquad \begin{matrix}w(D_2)\\ A^R\end{matrix}}{B^R}
\quad \text{red.}
$$

$$
\begin{matrix}w(D_2)\\ (A^R)\\ w(D_1)\\ B^R\end{matrix}
\quad \underset{6.2.16}{\overset{w}{\longleftarrow}} \quad
\begin{matrix}D_2\\ (A)\\ D_1\\ B\end{matrix}
$$

where $(A^R) = w''(A)$.

Case 2:

$$
\dfrac{\dfrac{\begin{matrix}D\\ A(U)\end{matrix}}{\forall X\, A(X)}}{A(B)}
\quad \overset{w}{\mapsto} \quad
\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}(\not{RU})^1\\ w(D)\\ A(U)^R\end{matrix}}{RU\to A(U)^R}\,1}{\forall X(RX\to A(X)^R)}}{RB^R\to A(B)^R} \qquad N(B)}{A(B)^R}
\quad \text{imm. red.}
$$

$$
\begin{matrix}
\dfrac{\dfrac{\begin{matrix}(\not{RB}^R)^1\\ \mathrm{Sub}_U^{B^R}\, w(D)\\ A(B)^R\end{matrix}}{RB^R\to A(B)^R}\,1 \qquad N(B)}{A(B)^R}
\quad \text{red.} \quad
\begin{matrix}N(B)\\ (RB^R)\\ \mathrm{Sub}_U^{B^R}\, w(D)\\ A(B)^R\end{matrix}
\quad \underset{6.2.15}{\overset{w}{\longleftarrow}} \\
\begin{matrix}\mathrm{Sub}_U^{B}\, D\\ A(B)\end{matrix}
\end{matrix}
$$

where (RU) is the set of all uncancelled occurrences of RU as an assumption in $w(D)$ and $(RB^R) = \mathrm{Sub}_U^{B^R}(RU)$.

Case 3:

$$\dfrac{\dfrac{\begin{matrix}[\neg(A\to B)]^1\\ D_1\\ \bot\end{matrix}}{A\to B}\,1 \qquad \begin{matrix}D_2\\ A\end{matrix}}{B} \quad \overset{w}{\longmapsto} \quad \dfrac{\dfrac{N(A\to B) \qquad \dfrac{\begin{matrix}[\neg(A\to B)^R]^1\\ w(D_1)\\ \bot\end{matrix}}{\neg\neg(A\to B)^R}\,1}{(A\to B)^R} \qquad \begin{matrix}w(D_2)\\ A^R\end{matrix}}{B^R}$$

imm. red.

$$\dfrac{\dfrac{\dfrac{N(B) \qquad \dfrac{\dfrac{\dfrac{\begin{matrix}[\neg(A\to B)^R]^1\\ w(D_1)\\ \bot\end{matrix}}{\neg\neg(A\to B)^R}\,1 \qquad \dfrac{\bot}{\neg(A\to B)^R}\,2}{\bot}}{\neg\neg B^R}\,3}{B^R}}{A^R\to B^R}\,4 \qquad \begin{matrix}w(D_2)\\ A^R\end{matrix}}{B^R}$$

where the derivation of $\bot$ above $\neg(A\to B)^R$ is

$$\dfrac{[\neg B^R]^3 \qquad \dfrac{[(A\to B)^R]^2 \qquad [A^R]^4}{B^R}}{\bot}$$

red.

$$\dfrac{N(B) \qquad \dfrac{\dfrac{\dfrac{\begin{matrix}[\neg(A\to B)^R]^1\\ w(D_1)\\ \bot\end{matrix}}{\neg\neg(A\to B)^R}\,1 \qquad \dfrac{\dfrac{[\neg B^R]^3 \qquad \dfrac{[(A\to B)^R]^2 \qquad \begin{matrix}w(D_2)\\ A^R\end{matrix}}{B^R}}{\bot}}{\neg(A\to B)^R}\,2}{\bot}}{\neg\neg B^R}\,3}{B^R}$$

imm. red.

$$\dfrac{N(B) \qquad \dfrac{\begin{matrix}\dfrac{\dfrac{[\neg B^R]^2 \qquad \dfrac{[(A\to B)^R]^1 \qquad \begin{matrix}w(D_2)\\ A^R\end{matrix}}{B^R}}{\bot}}{(\neg(A\to B)^R)}\,1\\ w(D_1)\\ \bot\end{matrix}}{\neg\neg B^R}\,2}{B^R}$$

$$\overset{w}{\underset{6.2.16}{\longmapsto}}\quad \begin{array}{c}\dfrac{\dfrac{\dfrac{\dfrac{[\neg B]^{2}\qquad \dfrac{[A\to B]^{1}\qquad \begin{array}{c}D_2\\ A\end{array}}{B}}{\perp}}{(\neg(A\to B))}\,1}{\begin{array}{c}D_1\\ \perp\end{array}}}{B}\,2\end{array}$$

where $(\neg(A\to B)^R)=w''(\neg(A\to B))$.

Case 4:

$$\dfrac{\dfrac{\begin{array}{c}[(\neg(\forall X\,A(X)))]^{1}\\ D\\ \perp\end{array}}{\forall X\,A(X)}\,1}{A(B)}\quad \overset{w}{\longmapsto}\quad \dfrac{\dfrac{N(\forall X\,A(X))\qquad \dfrac{\begin{array}{c}[(\neg(\forall X\,A(X))^R)]^{1}\\ w(D)\\ \perp\end{array}}{\neg\neg(\forall X\,A(X))^R}\,1}{\dfrac{(\forall X\,A(X))^R}{RB^R\to A(B)^R}}\qquad N(B)}{A(B)^R}$$

$$\text{imm. red.}\quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}[RU]^{4}\\ N(A(U))\end{array}\qquad \dfrac{\dfrac{\dfrac{\begin{array}{c}[(\neg\forall X\,A(X))^R]^{1}\\ w(D)\\ \perp\end{array}}{\neg\neg(\forall X\,A(X))^R}\,1\qquad \dfrac{\dfrac{[\neg A(U)^R]^{3}\qquad \dfrac{\dfrac{[(\forall X\,A(X))^R]^{2}}{RU\to A(U)^R}\qquad [RU]^{4}}{A(U)^R}}{\perp}\,2}{\neg(\forall X\,A(X))^R}}{\perp}}{\neg\neg A(U)^R}\,3}{A(U)^R}}{RU\to A(U)^R}\,4}{\forall X(RX\to A(X)^R)}}{RB^R\to A(B)^R}\qquad N(B)}{A(B)^R}\quad \text{imm. red.}$$

$$\dfrac{\mathrm{Sub}_U^{B^R} N(A(U)) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\genfrac{}{}{0pt}{}{(\neg(\forall X\, A(X))^R)^1}{w(D)}}{\bot}}{\neg\neg(\forall X\, A(X))^R}\,1 \qquad \dfrac{\dfrac{\neg A(B)^{R\,3} \quad \dfrac{\dfrac{(\forall X\, A(X))^{R\,2}}{RB^R \to A(B)^R} \quad RB^{R\,4}}{A(B)^R}}{\bot}}{\neg(\forall X\, A(X))^R}\,2}{\genfrac{}{}{0pt}{}{(RB^R)^4}{\bot}}}{\neg\neg A(B)^R}\,3}{\dfrac{\dfrac{A(B)^R}{RB^R \to A(B)^R}\,4 \qquad N(B)}{A(B)^R}} \qquad \text{red.}$$

$$\dfrac{\genfrac{}{}{0pt}{}{N(B)}{\genfrac{}{}{0pt}{}{(RB^R)}{\mathrm{Sub}_U^{B^R} N(A(U))}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\genfrac{}{}{0pt}{}{(\neg(\forall X\, A(X))^R)^1}{w(D)}}{\bot}}{\neg\neg(\forall X\, A(X))^R}\,1 \qquad \dfrac{\dfrac{\neg A(B)^{R\,3} \quad \dfrac{\dfrac{(\forall X\, A(X))^{R\,2} \quad N(B)}{RB^R \to A(B)^R \quad RB^R}}{A(B)^R}}{\bot}}{\neg(\forall X\, A(X))^R}\,2}{\bot}}{\neg\neg A(B)^R}\,3}{A(B)^R} \qquad \text{imm. red.}$$

$$\dfrac{\genfrac{}{}{0pt}{}{N(B)}{\genfrac{}{}{0pt}{}{(RB^R)}{\mathrm{Sub}_U^{B^R} N(A(U))}} \qquad \dfrac{\genfrac{}{}{0pt}{}{\dfrac{\dfrac{\neg A(B)^{R\,2} \quad \dfrac{\dfrac{(\forall X\, A(X))^{R\,1} \quad N(B)}{RB^R \to A(B)^R \quad RB^R}}{A(B)^R}}{\bot}}{(\neg(\forall X\, A(X))^R)}\,1}{w(D)}}{\bot}\,}{\neg\neg A(B)^R}\,2}{A(B)^R}$$

$\overset{w}{\Leftarrow}$ 6.2.13 6.2.15 6.2.16

$$\dfrac{\genfrac{}{}{0pt}{}{\dfrac{\dfrac{\neg A(B)^2 \quad \dfrac{\forall X\, A(X)^1}{A(B)}}{\bot}}{(\neg\forall X\, A(X))}\,1}{D}}{\dfrac{\bot}{A(B)}\,2}$$

where $(\neg(\forall X\, A(X))^{R}) = w''(\neg\forall X\, A(X))$, (RU) is the set of all uncancelled occurrences of RU as an assumption in $N(A(U))$, and $(RB^R) = \mathrm{Sub}_U^{B^R}(RU)$.

6.2.19. Proposition. *There is a function m s.t. $\vdash^{n}_{N_2} A \Rightarrow \vdash^{m(n)}_{N_1} A$ for first-order A.*

6.3. *Lower bound for speed-up by N_2*

6.3.1. Let F be the following set of formulae:

$$\forall x(x = x),$$
$$\forall x\, y(x = y \to y = x),$$
$$\forall x\, yz(x = y \to (y = z \to x = z)),$$
$$\forall x\, y(sx = sy \to x = y),$$
$$\forall x \neg sx = 0,$$

the universal closures of recursion equations for a finite set of primitive recursive functions (with function symbols $h_1 \cdots h_n$) sufficient to define the Kleene T-predicate quantifier-free, and

$$\forall x_1 \cdots x_m y_1 \cdots y_m (\mathop{\&}_{1 \leq i \leq m} x_i = y_i \to h_j x_1 \cdots x_m = h_j y_1 \cdots y_m)$$

for $1 \leq j \leq n$ and h_j m-ary.

Set

$$\mathbb{m} =_{\mathrm{df}} \underbrace{s \cdots s}_{m \text{ occurrences}} 0.$$

Define $\mathbb{N} = \lambda x\, \forall X(\forall yz(y = z \to (Xy \to Xz)) \to (X0 \to (\forall y(Xy \to Xsy) \to Xx)))$. Let w be a recursive enumeration (provably recursive in second-order Peano arithmetic) of the Gödel numbers of N_2-derivations of formulae of the form $\forall x(\mathbb{N}x \to \neg\forall y \neg T(\mathbb{m}, x, y))$ from F, and let the conclusion of $w(k)$ be $\forall x(\mathbb{N}x \to \neg\forall y \neg T(\mathbb{n}(k), x, y))$.

6.3.2. Lemma. *There is a provably recursive function of second-order Peano arithmetic l such that there is an N_2-derivation of $\&F \to \neg\forall y \neg T(\mathbb{n}(k), \mathbb{m}, y)$ of length $\leq l(w(k), m)$.*

Proof. Obvious.

6.3.3. Lemma. *There is a provably recursive function of second-order Peano arithmetic j such that $\vdash^{n}_{S_1} \{\&F \to \neg\forall y \neg T(\mathbb{k}, \mathbb{m}, y)\} \Rightarrow j(k, m, n)$ is the Gödel number of an S_1-derivation of $\vdash \{\&F \to \neg\forall y \neg T(\mathbb{k}, \mathbb{m}, y)\}$.*

Proof. Inspection of the proof of 3.3.2.

6.3.4. Lemma. *There is a provably recursive function of second-order Peano* *arithmetic p such that if i is the Gödel number of an S_1-derivation of $\vdash \{\&F \rightarrow \neg\forall y \neg T(\mathbb{k}, \mathbb{m}, y)\}$, then $\&F \rightarrow T(\mathbb{k}, \mathbb{m}, \mathbb{p}(i))$.*

Proof. Formalization of the inversion and midsequent theorems together with the definition of a valuation function for closed terms.

6.3.5. Proposition. *Suppose that for first-order A, $\vdash^{n}_{N_2} A \Rightarrow \vdash^{m(n)}_{N_1} A$, then m is not a provably recursive function of second-order Peano arithmetic.*

Proof. By 5.3.1 there is a provably recursive function of second-order Peano arithmetic q such that there is an S_1-derivation of $\vdash\{\&F \rightarrow \neg\forall y \neg(\mathbb{n}(k), \mathbb{k}, y)\}$ of length $\leqslant q(m(l(w(k), k)))$. Let $r(k) =_{\mathrm{df}} p(j(n(k), k, q(m(l(w(k), k)))))$, then if m is provably recursive then so is $r+1$. Let k_0 be such that $w(k_0)$ is an N_2-derivation of "$r+1$ is total recursive" from F (for any index for $r+1$), then $\&F \rightarrow T(\mathbb{n}(k_0), \mathbb{k}_0, \mathbb{r}(k_0))$ so by the usual properties of the T-predicate $r(k_0)+1 \leqslant r(k_0)$.

6.4. *Existence of upper bound for speed-up by* NE_2

6.4.1. An NE_2-derivation is called normal if it satisfies 5.1.2.

Lemma. *If F is a finite set of first-order formulae, A is a first-order formula, and D is a normal NE_2-derivation of A from F, then D is an NE_1-derivation.*

Proof. By induction on $\mathrm{lh}(D)$.

6.4.2. We add to the reductions of 6.2.3 the following:

= reduction

$$\dfrac{\begin{matrix} D_1 \\ A(a) \rightarrow B(a) \end{matrix} \qquad \begin{matrix} D_2 \\ a ⊜ b \end{matrix}}{A(b) \rightarrow B(b)} \quad \mapsto \quad \dfrac{\dfrac{\dfrac{\begin{matrix} D_1 \\ A(a) \rightarrow B(a) \end{matrix} \qquad \dfrac{[A(b)]^1 \qquad \begin{matrix} D_2 \\ b ⊜ a \end{matrix}}{A(a)}}{B(a)} \qquad \begin{matrix} D_2 \\ a ⊜ b \end{matrix}}{B(b)}\,{}_1}{A(b) \rightarrow B(b)}$$

provided that D_1 ends in $\rightarrow I$ or $A(b) \rightarrow B(b)$ is the major premiss of $\rightarrow E$,

$$\dfrac{\begin{matrix} D_1 \\ \forall x A(x, a) \end{matrix} \qquad \begin{matrix} D_2 \\ a ⊜ b \end{matrix}}{\forall x A(x, b)} \quad \mapsto \quad \dfrac{\dfrac{\dfrac{\begin{matrix} D_1 \\ \forall x A(x, a) \end{matrix}}{A(u, a)} \qquad \begin{matrix} D_2 \\ a ⊜ b \end{matrix}}{A(u, b)}}{\forall x A(x, b)}$$

provided D_1 ends in $\forall_1 I$ or $\forall x\, A(x, b)$ is the premiss of $\forall_1 E$, and

$$\dfrac{\begin{matrix} D_1 \\ \forall X\, A(X, a)\end{matrix} \qquad \begin{matrix} D_2 \\ a \ominus b\end{matrix}}{\forall X\, A(X, b)} \quad \mapsto \quad \dfrac{\dfrac{\dfrac{\begin{matrix} D_1 \\ \forall X\, A(X, a)\end{matrix}}{A(U, a)} \qquad \begin{matrix} D_2 \\ a \ominus b\end{matrix}}{A(U, b)}}{\forall X\, A(X, b)}$$

provided that D_1 ends in $\forall_2 I$ or $\forall X\, A(X, b)$ is the premiss of $\forall_2 E$. The corresponding reducibility relation is denoted "$>$".

The method of this section will be the same as that of Section 6.2. We shall be somewhat less explicit than in that section.

6.4.3. The notion of isomorphism between NE_2-derivations is defined as in 6.2.4 and denoted "$\doteq$".

6.4.4. We define a propositional system NE_2^* in which we shall simulate NE_2. NE_2^* is obtained from N_2^* of 6.2.8 by adding the proposition-constant E^* and the rule $=^*$ of 5.1.8. NE_2^* may be thought of as a subsystem of NE_2 by identifying E^* with $0=0$.

6.4.5. **Lemma.** *For each* NE_2*-derivation* D *there is an* NE_2^**-derivation* D^* *such that* $D \doteq D^*$.

Proof. Just like 4.2.9.

6.4.6. We shall define a map w from NE_2^*-derivations to N_2^*-derivations (where N_2^* is augmented by the propositional constant E^*) such that $D_1 > D_2 \Rightarrow w(D_1) > w(D_2)$. Let $R =_{\mathrm{df}} \lambda X E^* \to (X \to X)$. We define certain auxiliary N_2^*-derivations $S(A)$ as follows ($S(A)$ is a derivation of RA^R from assumptions of the form $R\bot$, RE^*, and RU for U occurring in A); $S(U) =_{\mathrm{df}} RU$, $S(\bot) =_{\mathrm{df}} R\bot$, $S(E^*) =_{\mathrm{df}} RE^*$, $S(A \to B) =_{\mathrm{df}}$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{S(B) \qquad [E^*]^3}{B^R \to B^R} \qquad \cfrac{[A^R \to B^R]^2 \qquad \cfrac{\cfrac{S(A) \qquad [E^*]^3}{A^R \to A^R} \qquad [A^R]^1}{A^R}}{B^R}}{B^R}}{A^R \to B^R}\,1}{(A^R \to B^R) \to (A^R \to B^R)}\,2}{E^* \to ((A^R \to B^R) \to (A^R \to B^R))}\,3$$

and

$S(\forall X\, A(X)) =_{\mathrm{df}}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{1}{(RU)}}{S(A(U))} \quad \overset{3}{E^*}}{A(U)^R \to A(U)^R} \qquad \dfrac{\overset{2}{(\forall X\, A(X))^R}}{RU \to A(U)^R} \quad \overset{1}{RU}}{A(U)^R}}{A(U)^R}\,1}{RU \to A(U)^R}}{(\forall X\, A(X))^R}\,2}{\dfrac{(\forall X\, A(X))^R \to (\forall X\, A(X))^R}{E^* \to ((\forall X\, A(X))^R \to (\forall X\, A(X))^R)}\,3}$$

where (RU) is the set of all uncancelled occurrences of RU as an assumption in $S(A(U))$.

6.4.7. Lemma. *Suppose that (RU) is the set of all uncancelled occurrences of RU as an assumption in $S(A(U))$ and the set of uncancelled assumption occurrences (RB^R) in $\mathrm{Sub}_U^{B^R} S(A(U))$ is defined by $(RB^R) = \mathrm{Sub}_U^{B^R}(RU)$, then $S(A(B)) =$*

$$\begin{array}{c} S(B) \\ (RB^R) \\ \mathrm{Sub}_U^{B^R} S(A(U)). \end{array}$$

Proof. By induction on $\mathrm{lh}\,(A(U))$.

6.4.8. We now define the map w; w is to be regarded in the obvious way as a 1–1 map from the formula occurrences of D into those of $w(D)$.

$w(A) =_{\mathrm{df}} A^R$.

w commutes with $(\to I)$, $(\to E)$, and $(\bot)$.

$$\dfrac{\begin{matrix} D_1 \\ A \end{matrix} \quad \begin{matrix} D_2 \\ E^* \end{matrix}}{A} \quad \overset{w}{\mapsto} \quad \dfrac{\dfrac{S(A) \qquad \begin{matrix} w(D_2) \\ E^* \end{matrix}}{A^R \to A^R} \qquad \begin{matrix} w(D_1) \\ A^R \end{matrix}}{A^R}$$

$$\dfrac{\begin{matrix} D \\ A(U) \end{matrix}}{\forall X\, A(X)} \quad \overset{w}{\mapsto} \quad \dfrac{\dfrac{\begin{matrix} \overset{1}{(RU)} \\ w(D) \\ A(U)^R \end{matrix}}{RU \to A(U)^R}\,1}{\forall X(RX \to A(X)^R)}$$

where (RU) is the set of all uncancelled occurrences of RU as an assumption in $w(D)$.

$$\begin{array}{c} D \\ \forall X\, A(X) \\ \hline A(B) \end{array} \quad \overset{w}{\mapsto} \quad \begin{array}{c} \begin{array}{cc} w(D) & \\ (\forall X\, A(X))^R & \\ \hline RB^R \to A(B)^R & S(B) \end{array} \\ \hline A(B)^R \end{array}.$$

6.4.9. Lemma. *Suppose that* (RU) *is the set of all uncancelled occurrences of* RU *as an assumption in* $w(D)$ *and the set of uncancelled assumption occurrences* (RB^R) *in* $\mathrm{Sub}_U^{B^R} w(D)$ *is defined by* $(RB^R) = \mathrm{Sub}_U^{B^R}(RU)$, *then* $w(\mathrm{Sub}_U^B D) =$

$$\begin{array}{c} S(B) \\ (RB^R) \\ \mathrm{Sub}_U^{B^R}\, w(D) \end{array}$$

Proof. By induction on $\mathrm{lh}(D)$ using 6.4.7.

6.4.10. Lemma. *Suppose that* (A) *is a set of uncancelled assumption occurrences in* D_2 *and* $(A^R) = w''(A)$, *then*

$$\begin{array}{ccc} D_1 & & w(D_1) \\ (A) & \overset{w}{\mapsto} & (A^R) \\ D_2 & & w(D_2) \end{array}$$

Proof. By induction on $\mathrm{lh}(D_2)$.

6.4.11. Proposition. D_1 red. $D_2 \Rightarrow w(D_1) > w(D_2)$.

Proof. There are six cases. The first two cases are just like cases 1 and 2 of 6.2.18 so we omit them.

Case 1

$$\begin{array}{c} \begin{array}{cc} \overset{1}{(\neg(A \not\to B))} & \\ D_1 & \\ \dfrac{\bot}{A \to B}\,1 & \begin{array}{c} D_2 \\ A \end{array} \end{array} \\ \hline B \end{array} \quad \overset{w}{\mapsto} \quad \begin{array}{c} \begin{array}{cc} \overset{1}{(\neg(A \not\to B)^R)} & \\ w(D_1) & \\ \dfrac{\bot}{A^R \to B^R}\,1 & \begin{array}{c} w(D_2) \\ A^R \end{array} \end{array} \\ \hline B^R \end{array} \quad \text{red.}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{[\neg B^R]^2 \qquad \cfrac{[A^R \to B^R]^1 \qquad \cfrac{w(D_2)}{A^R}}{B^R}}{\bot}}{(\neg(A^R \to B^R))}\,1}{w(D_1)\atop \bot}}{B^R}\,2 \quad \overset{w}{\underset{6.4.10}{\mapsto}} \quad \cfrac{\cfrac{\cfrac{\cfrac{[\neg B]^2 \qquad \cfrac{[A \to B]^1 \qquad \cfrac{D_2}{A}}{B}}{\bot}}{(\neg(A \to B))}\,1}{D_1\atop \bot}}{B}\,2$$

where $(\neg(A \to B)^R) = w''(\neg(A \to B))$.

Case 2

$$\cfrac{\cfrac{\cfrac{[(\neg\forall X\, A(X))]^1 \atop D}{\bot}}{\forall X\, A(X)}\,1}{A(B)} \quad \overset{w}{\mapsto} \quad \cfrac{\cfrac{\cfrac{\cfrac{[(\neg(\forall X\, A(X))^R)]^1 \atop w(D)}{\bot}}{(\forall X\, A(X))^R}\,1}{RB^R \to A(B)^R} \qquad S(B)}{A(B)^R}$$

$$\text{imm. red.} \quad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[\neg(RB^R \to A(B)^R)]^2 \qquad \cfrac{[(\forall X\, A(X))^R]^1}{RB^R \to A(B)^R}}{\bot}}{(\neg(\forall X\, A(X))^R)}\,1}{w(D) \atop \bot}}{RB^R \to A(B)^R}\,2 \qquad S(B)}{A(B)^R} \quad \text{red.}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[\neg A(B)^R]^3 \qquad \cfrac{[RB^R \to A(B)^R]^1 \qquad S(B)}{A(B)^R}}{\bot}}{\neg(RB^R \to A(B)^R)} \qquad \cfrac{[(\forall X\, A(X))^R]^2}{RB^R \to A(B)^R}}{\bot}}{(\neg(\forall X\, A(X))^R)}\,2}{\cfrac{w(D)}{\bot}}\,\cfrac{}{A(B)^R}\,3$$

$$
\succ\quad
\cfrac{\cfrac{[\neg A(B)^R]^2 \qquad \cfrac{\cfrac{[(\forall X\, A(X))^R]^1}{RB^R \to A(B)^R} \qquad S(B)}{A(B)^R}}{\cfrac{\bot}{\begin{array}{c}(\neg(\forall X\, A(X))^R)\\ w(D)\\ \bot\end{array}}\,1}}{A(B)^R}\,2
\qquad \overset{w}{\underset{6.4.10}{\leftarrow}} \qquad
\cfrac{\cfrac{[\neg A(B)]^2 \qquad \cfrac{[\forall X\, A(X)]^1}{A(B)}}{\cfrac{\bot}{\begin{array}{c}(\neg\forall X\, A(X))\\ D\\ \bot\end{array}}\,1}}{A(B)}\,2
$$

where $(\neg(\forall X\, A(X))^R) = w''(\neg\forall X\, A(X))$.

Case 3

$$
\cfrac{\begin{array}{c}D_1\\ A\to B\end{array} \qquad \begin{array}{c}D_2\\ E^*\end{array}}{A\to B}
$$

$$
\overset{w}{\mapsto}\qquad
\cfrac{\cfrac{S(A\to B) \qquad \begin{array}{c}w(D_2)\\ E^*\end{array}}{(A\to B)^R \to (A\to B)^R} \qquad \begin{array}{c}w(D_1)\\ (A\to B)^R\end{array}}{(A\to B)^R}
$$

$$
\text{imm. red.}\qquad
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{S(B) \qquad \begin{array}{c}w(D_2)\\ E^*\end{array}}{B^R\to B^R} \qquad \cfrac{[A^R\to B^R]^2 \qquad \cfrac{\cfrac{S(A) \qquad \begin{array}{c}w(D_2)\\ E^*\end{array}}{A^R\to A^R} \qquad [A^R]^1}{A^R}}{B^R}}{B^R}}{A^R\to B^R}\,1}{(A\to B)^R \to (A\to B)^R}\,2 \qquad \begin{array}{c}w(D_1)\\ (A\to B)^R\end{array}}{(A\to B)^R}
$$

$$
\text{red.}\qquad
\cfrac{\cfrac{\cfrac{S(B) \qquad \begin{array}{c}w(D_2)\\ E^*\end{array}}{B^R\to B^R} \qquad \cfrac{\begin{array}{c}w(D_1)\\ A^R\to B^R\end{array} \qquad \cfrac{\cfrac{S(A) \qquad \begin{array}{c}w(D_2)\\ E^*\end{array}}{A^R\to A^R} \qquad [A^R]^1}{A^R}}{B^R}}{B^R}}{A^R\to B^R}\,1
$$

$$\overset{w}{\leftarrow}\qquad \dfrac{\dfrac{\dfrac{\begin{matrix}D_1\\ A\to B\end{matrix}\qquad \dfrac{[A]^1\qquad \begin{matrix}D_2\\ E^*\end{matrix}}{A}}{B}\qquad \begin{matrix}D_2\\ E^*\end{matrix}}{B}}{A\to B}\,1$$

Case 4

$$\dfrac{\begin{matrix}D_1\\ \forall X\,A(X)\end{matrix}\qquad \begin{matrix}D_2\\ E^*\end{matrix}}{\forall X\,A(X)}\qquad \overset{w}{\mapsto}$$

$$\dfrac{\dfrac{S(\forall X\,A(X))\qquad \begin{matrix}w(D_2)\\ E^*\end{matrix}}{(\forall X\,A(X))^R\to(\forall X\,A(X))^R}\qquad \begin{matrix}w(D_1)\\ (\forall X\,A(X))^R\end{matrix}}{(\forall X\,A(X))^R}$$

imm. red.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}[(RU)]^1\\ S(A(U))\end{matrix}\qquad \begin{matrix}w(D_2)\\ E^*\end{matrix}}{A(U)^R\to A(U)^R}\qquad \dfrac{\dfrac{(\forall X\,A(X))^R}{RU\to A(U)^R}\qquad [RU]^1}{A(U)^R}}{A(U)^R}}{RU\to A(U)^R}\,1}{(\forall X\,A(X))^R}}{(\forall X\,A(X))^R\to(\forall X\,A(X))^R}\qquad \begin{matrix}w(D_1)\\ (\forall X\,A(X))^R\end{matrix}}{(\forall X\,A(X))^R}$$

red.

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}[(RU)]^1\\ S(A(U))\end{matrix}\qquad \begin{matrix}w(D_2)\\ E^*\end{matrix}}{A(U)^R\to A(U)^R}\qquad \dfrac{\dfrac{\begin{matrix}w(D_1)\\ (\forall X\,A(X))^R\end{matrix}}{RU\to A(U)^R}\qquad [RU]^1}{A(U)^R}}{A(U)^R}}{RU\to A(U)^R}}{(\forall X\,A(X))^R}$$

$$\overset{w}{\leftarrow}\qquad \dfrac{\dfrac{\dfrac{\begin{matrix}D_1\\ \forall X\,A(X)\end{matrix}}{A(U)}\qquad \begin{matrix}D_2\\ E^*\end{matrix}}{A(U)}}{\forall X\,A(X)}$$

where (RU) is the set of all uncancelled occurrences of RU as an assumption in $S(A(U))$.

6.4.12. Proposition. *There is a function m such that* $\vdash^{n}_{\mathrm{NE}_2} A \Rightarrow \vdash^{m(n)}_{\mathrm{NE}_1} A$ *for first-order A.*

6.5. Lower bound for speed-up by NE_2

6.5.1. Proposition. *Suppose that for finite sets of equations F* $\forall F \vdash^{n}_{\mathrm{NE}_2} E \Rightarrow \mathrm{Sub}\, F \vdash^{m(n)}_{\mathrm{NE}} E$*, then m is not a provably recursive function of second-order Peano arithmetic.*

Proof. W.l.o.g. assume that $m(0)=0$ and $m(n)<m(n+1)$. If m is a provably recursive function of second-order Peano arithmetic by [21, Section 8] there is a finite set of equations F such that

(1) $m(n^2)$ is finitely defined by F (with principal function symbol h),
(2) F is symmetric, and
(3) $\forall F \vdash_{\mathrm{NE}_2} \mathbb{N}u \to \mathbb{N}(hu)$, where $\mathbb{N} =_{\mathrm{df}} \lambda x\, \forall X(X0 \to (\forall y(Xy \to Xsy) \to Xx))$.

For what follows we refer the reader to Section 1.3.1. Now $\forall F^{+} \vdash_{\mathrm{NE}_2} \forall x(\mathbb{N}x \to fx=0)$ thus there is a linear function l such that $\forall F^{+} \vdash^{l(n)}_{\mathrm{NE}_2} f(s^{n+1}0)=0$ so $\mathrm{Sub}\, F^{+} \vdash^{m(l(n))}_{\mathrm{NE}} f(s^{n+1}0)=0$. Hence by Proposition 1.3.1 $m(n^2) \leqslant m(l(n))$ which is false for sufficiently large n.

6.6. Proof-search in N_2 *and* NE_2

6.6.1. Proposition. *There are functions* m_1, m_2 *such that*

(a) *if A is valid in all Henkin structures, then* $\vdash^{m_1(\mathrm{lh}(A))}_{N_2} A$*, and*
(b) *if A is valid in all Henkin structures (with equality), then* $\vdash^{m_2(\mathrm{lh}(A))}_{\mathrm{NE}_2} A$.

Proof. As in 3.3.3.

7. Proof-search in and speed-up by the theory of types

7.1. Preliminaries

7.1.1. The notion of type is defined as follows: o (individuals) and O (truth values) are types; if $w_1 \cdots w_n$ are types, then $(w_1, \ldots, w_n)$ is a type (n-ary relations with ith arguments in w_i).

7.1.2. We consider formulae $A, B, C, \ldots$ of type theory built up from individual constants $c, \ldots$, function symbols $f, g, h, \ldots$ (n-ary functions from individuals to individuals), typed parameters $U^{w}1, V^{w}2, W^{w}3, \ldots$, typed (bound) variables $X^{w_1}, Y^{w_2}, Z^{w_3}, \ldots$, perhaps the relation constant $=$, $\bot$, $\to$, $\forall$, and λ.

More precisely, we define the notion of a term of type w as follows: c is a term of type o; $\bot$ is a term of type O; $=$ is a term of type (o, o); U^{w} is a term of type

w; if $a_1 \cdots a_n$ are terms of type o and f has arity $= n$, then $fa_1 \cdots a_n$ is a term of type o; if $T_1 \cdots T_n$ are terms of type $w_1 \cdots w_n$ resp. and $w = (w_1, \ldots, w_n)$, then $U^w T_1 \cdots T_n$ is a term of type O; if A and B are terms of type O, then so is $A \to B$; if $A(U^w)$ is a term of type O, then so is $\forall X^w A(X^w)$; if $A(U_1^{w_1}, \ldots, U_n^{w_n})$ is a term of type O, then $\lambda X_1^{w_1} \cdots X_n^{w_n} A(X_1^{w_1}, \ldots, X_n^{w_n})$ is a term of type $(w_1, \ldots, w_n)$. A formula is just a term of type O.

If $w = \text{o}$ we write u for U^w and x for X^w. In addition, we shall delete type superscripts when no confusion can result.

7.1.3. The notion of simultaneous substitution $\mathrm{Sub}_{U_1 \cdots U_n}^{T_1 \cdots T_n}$ is defined as follows:

$$\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} U_i =_{\mathrm{df}} T_i; \qquad \mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} V =_{\mathrm{df}} V$$

for V not a U_i;

$$\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} c =_{\mathrm{df}} c; \qquad \mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} \bot =_{\mathrm{df}} \bot; \qquad \mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} = \, =_{\mathrm{df}} =;$$

$\mathrm{Sub}_{U_1 \cdots U_n}^{T_1 \cdots T_n}$ commutes with the logical operations, λ, and function symbol application;

$$\lambda X_1 \cdots X_n A(X_1, \ldots, X_n) T_1 \cdots T_n =_{\mathrm{df}} \mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} A(U_1, \ldots, U_n);$$

$$\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} U_i R_1 \cdots R_m =_{\mathrm{df}} T_i \Big(\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} R_1\Big) \cdots \Big(\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} R_m\Big);$$

$$\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} V R_1 \cdots R_m =_{\mathrm{df}} V \Big(\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} R_1\Big) \cdots \Big(\mathop{\mathrm{Sub}}_{U_1 \cdots U_n}^{T_1 \cdots T_n} R_m\Big)$$

for V not a U_i.

7.1.4. The calculus N_ω (natural rules for type theory) consists of N_0 together with

$$(\forall_w I) \quad \frac{A(U^w)}{\forall X^w A(X^w)}$$

provided that U^w does not occur in any assumption,

$$(\forall_w E) \quad \frac{\forall X^w A(X^w)}{A(T)}$$

for T a term of type w, and

$$(\mathrm{EXT}_w) \quad \frac{\mathrm{Sub}_U^{T_1} A \qquad \begin{array}{c}(T_1 U_1 \cdots U_n)\\ T_2 U_1 \cdots U_n\end{array} \qquad \begin{array}{c}(T_2 U_1 \cdots U_n)\\ T_1 U_1 \cdots U_n\end{array}}{\mathrm{Sub}_U^{T_2} A}$$

for T_1 and T_2 terms of type w and U_j occurring only in assumption occurrences in $(T_1 U_1 \cdots U_n) \cup (T_2 U_1 \cdots U_n)$.

7.1.5. The calculus NE_ω (natural rules for type theory with equality) consists of N_ω together with the axiom and rule of equality.

7.2. *Non-existence of bounds for proof-search*

7.2.1. Let N_ω^* (natural rules for higher type propositional calculus) result from N_ω by deleting the type o. It is well-known that N_ω^* is complete; we shall show that there is no function m such that for propositional (possibly higher type) formulae A, if A is valid, then $\vdash_{N_\omega^*}^{m(\mathrm{lh}(A))} A$.

7.2.2. Let ω be a propositional type. We define a propositional structure $M(w) = (M_0, \ldots, M_{w'}, \ldots)$ as follows; $M_0 =_{\mathrm{df}} \{\text{true}, \text{false}\}$; $M_{(w')} =_{\mathrm{df}}$ power set of $M_{w'}$, if $w' \neq w$; $M_{(w)} =_{\mathrm{df}}$ power set $(M_w \cup \omega)$; $M_{(w_1,\ldots,w_n)} =_{\mathrm{df}}$ power set of $M_{w_1} \times \cdots \times M_{w_n}$, for $2 \leq n$.

If $S_i \in M_{w_i}$, then the notation "$M(w), S_1, \ldots, S_n \vDash A(U_1^{w_1}, \ldots, U_n^{w_n})$" has the obvious meaning. We denote by "$T_{M(w),\ldots}$" the value of T in $M(w), \ldots$.

7.2.3. Lemma. $M(w), \ldots, T_{M(w),\ldots} \vDash A(\ldots, U) \Leftrightarrow M(w), \ldots \vDash A(\ldots, T)$.

Proof. By induction on $\omega \cdot \mathrm{lh}(w') + \mathrm{lh}(A(\ldots, U))$ where w' is the type of T.

Basis: $\mathrm{lh}(w') = \mathrm{lh}(A(\ldots, U)) = 1$. Obvious.

Induction step:

Case 1: $A(\ldots, U)$ 'begins" with $\rightarrow$ or $\forall$. Easy.

Case 2: $A(\ldots, U) = VR_1(\ldots, U) \cdots R_n(\ldots, U)$

Subcase 1: $V \neq U$. We have

$$M(w), \ldots, T_{M(w),\ldots}$$

$$\vDash A(\ldots, U) \Leftrightarrow M(w), \ldots, T_{M(w),\ldots}, R_1(\ldots, U)_{M(w),\ldots,T_{M(w'),\ldots}}, \cdots, R_n(\ldots, U)_{M(w),\ldots,T_{M(w),\ldots}}$$

$$\vDash VV_1 \cdots V_n \Leftrightarrow M(w), \ldots, R_1(\ldots, T)_{M(w),\ldots}, \cdots, R_n(\ldots, T)_{M(w),\ldots}$$

$$\vDash VV_1 \cdots V_n \Leftrightarrow M(w), \ldots \vDash VR_1(\ldots, T) \cdots R_n(\ldots, T).$$

Subcase 2: $V = U$. We have

$$M(w), \ldots, T_{M(w),\ldots}$$

$$\vDash A(\ldots, U) \Leftrightarrow M(w), \ldots, T_{M(w),\ldots}, R_1(\ldots, U)_{M(w),\ldots,T_{M(w),\ldots}}, \cdots, R_n(\ldots, U)_{M(w),\ldots,T_{M(w),\ldots}}$$

$$\vDash UV_1 \cdots V_n \Leftrightarrow M(w), \ldots, T_{M(w),\ldots}, R_1(\ldots, T)_{M(w),\ldots}, \cdots, R_n(\ldots, T)_{M(w),\ldots}$$

$$\vDash UV_1 \cdots V_n \Leftrightarrow M(w), \ldots, R_1(\ldots, T)_{M(w),\ldots}, \cdots, R_n(\ldots, T)_{M(w),\ldots}$$

$$\vDash TV_1 \cdots V_n \Leftrightarrow M(w), \ldots \vDash TR_1(\ldots, T) \cdots R_n(\ldots, T).$$

7.2.4. Proposition. *If* $\vdash_{N_\omega^*\text{-EXT}_{(w)}} A$, *then* $M(w) \vDash A$.

Proof. Straightforward using Lemma 7.2.3.

7.2.5. Let $\leftrightarrow =_{\mathrm{df}} \neg((\rightarrow) \rightarrow \neg(\rightarrow))$ and set $\mathrm{Inf}(w) =_{\mathrm{df}} \neg\forall X^{(w,w)} \forall Y(\forall Z_1 \neg \forall Z_2 \neg \forall Z_3(XZ_1Z_3 \leftrightarrow \forall Z_4(Z_1Z_4) \leftrightarrow Z_2Z_4)) \rightarrow \neg\forall Z \neg XZY)$ ($\mathrm{Inf}(w)$ says that w is infinite).

Proposition. *There is no function m such that for propositional A, if A is valid, then* $\vdash^{m(\mathrm{lh}(A))}_{N} A$.

Proof. Suppose that for each w of the form $(\cdots 0 \cdots)$ we have $\vdash^{n}_{N_0^*} \neg \mathrm{Inf}(w)$, then for some such w of length $\geq n+3$ there is a w' s.t. $w = (\cdots ((w')) \cdots)$ and $\vdash_{N_0^*\text{-}\mathrm{EXT}_{(w')}} \neg \mathrm{Inf}(w)$. Thus by Proposition 7.2.4 $M(w') \vDash \neg \mathrm{Inf}(w)$ which is plainly false.

7.3. *Non-existence of bounds for speed-up*

7.3.1. Let N_0^* be N_0 together with EXT_0; we shall show that there is no function m such that for quantifier-free A, $\vdash^{n}_{N_0^*} A \Rightarrow \vdash^{m(n)}_{N_0} A$.

7.3.2. Lemma. *Suppose that D is an N_0^*-derivation of $\mathrm{Sub}^B_U A$, where B is not a subformula of A, such that*

(1) *neither minor premiss of an instance of EXT_0 in D is a subformula of B, and*
(2) *B does not occur in D, then A is valid.*

Proof. By induction on $\mathrm{lh}(D)$.

7.3.3. Let

$$A_n =_{\mathrm{df}} \Big(\mathop{\&}_{1\leq i\leq n} U_i \rightarrow V \Big) \leftrightarrow \Big(\mathop{\&}_{1\leq i\leq n} ((U_i \rightarrow W_i) \rightarrow U_i) \rightarrow V \Big).$$

Lemma. $\vdash^{m}_{N_0^*} A_{2n} \Rightarrow m \geq n$.

Proof. Lemma 7.3.2.

7.3.4. Lemma. $\vdash^{14}_{N_\omega} A_n$.

Proof. Let

$$B_n =_{\mathrm{df}} \Big(\mathop{\&}_{1\leq i\leq n} U_i \rightarrow V \Big) \rightarrow \Big(\mathop{\&}_{1\leq i\leq n} ((U_i \rightarrow W_i) \rightarrow U_i) \rightarrow V \Big)$$

and

$$C_n =_{\mathrm{df}} \Big(\mathop{\&}_{1\leq i\leq n} ((U_i \rightarrow W_i) \rightarrow U_i) \rightarrow V \Big) \rightarrow \Big(\mathop{\&}_{1\leq i\leq n} U_i \rightarrow V \Big).$$

Set

$$D_{1,0} =_{\mathrm{df}} \frac{U}{(U \to W) \to U},$$

$$D_{2,0} =_{\mathrm{df}} \dfrac{\dfrac{\cancel{\neg U}^{2} \qquad \dfrac{(U \to W) \to U \qquad \dfrac{\dfrac{\dfrac{\cancel{\neg U}^{2} \quad \cancel{U}^{1}}{\bot}}{W}}{U \to W}\,{}_{1}}{U}}{\bot}}{U},$$

$$D_{1,n} =_{\mathrm{df}} \dfrac{\dfrac{\underset{1\leq i\leq n}{\&} \cancel{U_i \to V}^{2} \qquad \begin{matrix}(\cancel{U})^{1} \\ D_{1,0}\end{matrix} \qquad \begin{matrix}((U \to \cancel{W}) \to U)^{1} \\ D_{2,0}\end{matrix}}{\underset{1\leq i\leq n}{\&} ((U_i \to W_i) \to U_i) \to V}\,{}_{1}}{B_n}\,{}_{2},$$

and

$$D_{2,n} =_{\mathrm{df}} \dfrac{\dfrac{\underset{1\leq i\leq n}{\&} \cancel{((U_i \to W_i) \to U_i) \to V}^{2} \qquad \begin{matrix}((U \to \cancel{W}) \to U)^{1} \\ D_{2,0}\end{matrix} \qquad \begin{matrix}(\cancel{U})^{1} \\ D_{1,0}\end{matrix}}{\underset{1\leq i\leq n}{\&} U_i \to V}}{C_n}.$$

The desired N_{ω}^{*}-derivation of A_n is

$$\dfrac{\dfrac{\dfrac{\cancel{B_n \to \neg C_n}^{1} \qquad D_{1,n}}{\neg C_n} \qquad D_{2,n}}{\bot}}{\neg(B_n \to \neg C_n)}\,{}_{1}.$$

7.3.5. We now show that there is no function m such that for finite sets of of equations F, $\forall F \vdash^{n}_{\mathrm{NE}_\omega} E \Rightarrow \mathrm{Sub}\, F \vdash^{m(n)}_{\mathrm{NE}} E$.

The notion of a function term is defined as follows: f is a function term; if $a(u_1, \ldots, u_n)$ is an individual term, then $\lambda x_1 \cdots x_n a(x_1, \ldots, x_n)$ is a function term. Function terms may be substituted for function symbols under the definition $\lambda x_1 \cdots x_n a(x_1, \ldots, x_n) a_1 \cdots a_n = a(a_1, \ldots, a_n)$.

Lemma. $\{\forall x_1 \cdots x_n \;\; a(x_1, \ldots, x_n) = b(x_1, \ldots, x_n),\;\; A(\lambda x_1 \cdots x_n \;\; a(x_1, \ldots, x_n))\}$ $\vdash^{2n+3}_{\mathrm{NE}_\omega} A(\lambda x_1 \cdots x_n\; b(x_1, \ldots, x_n))$.

Proof. Let g be a new n-ary function symbol; there is a formula B such that $\mathrm{Sub}_U^{\lambda X x_1 \cdots x_n X(g x_1 \cdots x_n)} B = A(g)$ and B does not contain g. Let $D_0 =_{\mathrm{df}}$

$$\cfrac{\cfrac{\forall x_1 \cdots x_n\, a(x_1, \ldots, x_n) = b(x_1, \ldots, x_n)}{\forall x_2 \cdots x_n\, a(u_1, \ldots, x_n) = b(u_1, \ldots, x_n)}}{\begin{array}{c}\vdots\end{array}} \qquad \frac{Ua(u_1, \ldots, u_n) \qquad a(u_1, \ldots, u_n) = b(u_1, \ldots, u_n)}{Ub(u_1, \ldots, u_n)}$$

and $D_1 =_{\mathrm{df}}$

$$\cfrac{\cfrac{\forall x_1 \cdots x_n\, a(x_1, \ldots, x_n) = b(x_1, \ldots, x_n)}{\forall x_2 \cdots x_n\, a(u_1, \ldots, x_n) = b(u_1, \ldots, x_n)}}{\begin{array}{c}\vdots\end{array}} \qquad \frac{Ub(u_1, \ldots, u_n) \qquad a(u_1, \ldots, u_n) = b(u_1, \ldots, u_n)}{Ua(u_1, \ldots, u_n)}.$$

The desired derivation is

$$\frac{\mathrm{Sub}_U^{\lambda X x_1 \cdots x_n X a(x_1, \ldots, x_n)} B \qquad \overset{0}{\underset{D_0}{(Ua(u_1, \ldots, u_n))}} \qquad \overset{1}{\underset{D_1}{(Ub(u_1, \ldots, u_n))}}}{\mathrm{Sub}_U^{\lambda X x_1 \cdots x_n X b(x_1, \ldots, x_n)} B}.$$

7.3.6. Proposition. *There is no function* m *such that for finite sets of equations* F, $\forall F \vdash^{n}_{\mathrm{NE}_\omega} E \Rightarrow \mathrm{Sub}\, F \vdash^{m(n)}_{\mathrm{NE}} E$.

Proof. Let f and g be unary function symbols and set $F =_{\mathrm{df}} \{gfu = u\}$. Put

$$E_n =_{\mathrm{df}} \underbrace{gf \cdots gf}_{n \text{ times}} 0 = 0,$$

then by 1.3.3 with $m = \mathrm{lh}$ there is no fixed k such that $\mathrm{Sub}\, F \vdash^{k}_{\mathrm{NE}} E_n$ for all n; however, by Lemma 7.3.5 we have $\forall F \vdash^{7}_{\mathrm{NE}_\omega} E_n$.

Open problems

(1) Is there a polynomial $p(x)$ such that for finite sets of equations F, $F \vdash^{n}_{\mathrm{SE}} E \Rightarrow F \vdash^{p(n)}_{\mathrm{SE\text{-}cut}} E$?

(2) Is there a polynomial $p(x)$ such that for finite sets of equations F, if $\& F \to E$ is valid, then $F \vdash^{p(\mathrm{lh}(F) + \mathrm{lh}(E))}_{\mathrm{SE\text{-}cut}} E$?

(3) Is there a polynomial $p(x)$ such that for quantifier-free formulae A, if A is valid, then $\vdash^{p(\mathrm{lh}(A))}_{\mathrm{N}_0} A$?

(4) Are the relations $\vdash^{n}_{\mathrm{N}_1} A$ and $\vdash^{n}_{\mathrm{NE}_1} A$ decidable?

(5) Is there a recursive function m such that if A is valid in all Henkin structures, then $\vdash^{m(\mathrm{lh}(A))}_{\mathrm{N}_2} A$?

(6) Is there a recursive function m such that if A is valid in all Henkin structures with equality, then $\vdash^{m(\mathrm{lh}(A))}_{\mathrm{NE}_2} A$?

(7) Is there a recursive function m such that for first-order formulae A, $\vdash^{n}_{\mathrm{N}_2} A \Rightarrow \vdash^{m(n)}_{\mathrm{N}_1} A$?

(8) Is there a recursive function m such that for first-order formulae A, $\vdash^{n}_{\mathrm{NE}_2} A \Rightarrow \vdash^{m(n)}_{\mathrm{NE}_1} A$?

(9) Is there a recursive function m such that for finite sets of equations F, $\forall F \vdash^{n}_{\mathrm{NE}_2} E \Rightarrow \mathrm{Sub}\, F \vdash^{m(n)}_{\mathrm{NE}} E$?

Note that (1) → (2), (5) ↔ (6), and (8) → (7) w.r.t. the answer yes.

References

[1] C. Chang and Lee, Symbolic Logic and Mechanical Theorem Proving (Academic Press, New York, 1973).

[2] A. Church, The calculi of lambda-conversion, Ann. Math. Studies 6 (1941).

[3] Cook, The complexity of theorem proving procedures, Proc. Third ACM Symp. on Theory of Computing May 3–5 (1971).

[4] Cook and Reckhow, On the length of proofs in the propositional calculus, Proc. Sixth ACM Symp. on Theory of Computing April 30–May 2 (1974).

[5] H. Curry, Foundations of Mathematical Logic (McGraw-Hill, New York, 1963).

[6] H. Curry and R. Feys, Combinatory Logic, Vol. 1 (North-Holland, Amsterdam, 1958).

[7] H. Curry, J. Hindley and J. Seldin, Combinatory Logic, Vol. 2 (North-Holland, Amsterdam, 1972).

[8] G. Gentzen. The Collected Papers of Gerhard Gentzen edited by Szabo (North-Holland, Amsterdam, 1969).

[9] Girard, Interprétation fonctionelle et élimination des coupures de l'arithmetique d'order supérieur Thése de Doctorat d'État, Paris VII (1972).

[10] Herbrand, Logical Writings edited by Goldfarb (Harvard, 1971).

[11] J. Hindley, The principal type-scheme of an object in combinatory logic, Trans. A.M.S. 146 (1969).

[12] J. Hindley, An abstract form of the Church–Rosser theorem I, J. Symbolic Logic 34 (4) (1969).

[13] J. Hindley, An abstract form of the Church–Rosser theorem II, J. Symbolic Logic 39 (1) (1974).

[14] Howard, The formulae-as-types notion of construction, mimeographed (1969).

[15] Kozen, Lower bounds for natural proof systems, Proc. 18th Symp. on Found. of Comput. Sci. (IEEE) Oct. 31–Nov. 2 (1977).

[16] G. Kreisel. Elements of proof-theory, mimeographed, (1965).

[17] G. Kreisel, Hilbert's program and the search for automatic proof procedures, in: Symposium on Automatic Demonstration. Springer Lecture Notes 125 (Springer-Verlag, Berlin, 1970).

[18] G. Kreisel, Survey of proof-theory II, in J. E. Fenstad, ed., Proceedings of the Second Scandinavian Logic Symposium (North-Holland, Amsterdam, 1971).

[19] G. Kreisel, Perspectives in the philosophy of pure mathematics, in P. Suppes et al., eds., Logic, Methodology and the Philosophy of Science IV (North-Holland, Amsterdam, 1973).

[20] G. Kreisel, Mints, and Simpson, The use of abstract languages in elementary metamathematics: Some pedagogic examples, in: Logic Colloquium, Springer Lecture Notes 453 (Springer-Verlag, Berlin, 1975).

[21] G. Kreisel and Tait, Finite definability of number theoretic functions and parametric completeness of equation calculi, Z. Math. Logik Grundlagen Math. 7 (1961).

[22] G. Kreisel and G. Takeuti, Formally self-referential propositions for cut-free classical analysis and related systems, Dissertationes Math. CXVIII (1974).

[23] Lifšic, Specialization of the form of deduction in the predicate calculus with equality and function symbols, Proc. Steklov Inst. Math. 98 (1968).
[24] P. Martin-Löf, Hauptsatz for the theory of species, in: J. E. Fenstad, ed., Proceedings of the Second Scandinavian Logic Symposium (North-Holland, Amsterdam, 1971).
[25] P. Martin-Löf, Hauptsatz for intuitionistic simple type theory, in: P. Suppes et al., eds., Logic, Methodology and the Philosophy of Science IV (North-Holland, Amsterdam, 1973).
[26] Maslov, The inverse method for establishing deducibility for logical calculi, Proc. Steklov Inst. Math. 98 (1968).
[27] Mints, Variation in the deduction search tactics in sequential calculi, Sem. Math. V.A. Steklov Math. Inst. Leningrad 4 (1969).
[28] Parikh, Some results on the length of proofs, Trans. A.M.S. 177 (1973).
[29] D. Prawitz, Natural Deduction (Almqvist and Wiksell, 1965).
[30] D. Prawitz, Ideas and results in proof theory, in: J. E. Fenstad, ed., Proceedings of the Second Scandinavian Logic Symposium (North-Holland, Amsterdam, 1971).
[31] Richardson, Sets of theorems with short proofs, J. Symbolic Logic 39 (2) (1974).
[32] Robinson, A machine oriented logic based on the resolution principle, J.ACM 12 (1) (1965).
[33] R. Statman, Herbrand's theorem and Gentzen's notion of a direct proof, in: J. Barwise, ed., Handbook of Mathematical Logic (North-Holland, Amsterdam, 1977).
[34] R. Statman, Complexity of derivations from quantifier-free Horn formulae, in: R. O. Gandy and J. M. E. Hyland, eds., Logic Colloquium '76 (North-Holland, Amsterdam, 1977).
[35] R. Statman, Intuitionistic propositional logic is polynomial space complete, Theoret. Comput. Sci., to appear.
[36] R. Statman, Worst case exponential lower bounds for input resolution with paramodulation, SIAM Journal on Computing, to appear.
[37] Tait, Intensional interpretation of functionals of finite type I, J. Symbolic Logic 32 (2) (1967).
[38] Tseitin, On the complexity of derivation in the propositional calculus, Sem. Math. V.A. Steklov Math. Inst. Leningrad 8 (1970).