LOWER BOUNDS ON HERBRAND'S THEOREM

R. STATMAN

Abstract. We give non Kalmar-elementary lower bounds on the elimination of quantifier inferences via Herbrand's theorem.

I. A special case of Herbrand's theorem says the following:

Let $X$ be a set of equations, $\forall X$ the set of universal closures of members of $X$, and $X^*$ the set of closed substitution instances of members of $X$; then, for all closed equations $E$,

$$\forall X \models E \iff X^* \models E.$$  

There is a recursive method of passing from any derivation of $E$ from $\forall X$ in the predicate calculus to a derivation of $E$ from $X^*$ in the equation calculus. This is a simple consequence of the soundness and completeness of the rules. One may also obtain such methods by analyzing familiar procedures for "unwinding" proofs such as cut-elimination and $\epsilon$-substitution. These latter methods preserve some of the structure of the original proof, in particular, the number of lines (i.e., inferences) in the equational proof is bounded by a function of a few simple features of the original. Knowledge of these functions can be of use in extracting bounds from prima facie nonconstructive proofs (see, e.g., [6, p. 110 (a)]).

Further analysis of such methods as cut-elimination and $\epsilon$-substitution shows that the number of lines in the equational proof is bounded by a function of the number of lines (only) in the original. In this note we shall give lower bounds on the number of lines for such unwindings. In particular, we shall give a finite set of equations (equational theory) $X$ and a sequence of equations $E_n$, such that $E_n$ is derivable from $\forall X$ in the predicate calculus (with equality) in a number of lines linear in $n$ (also, in a number of symbols linear in $n$, provided the predicate calculus is enriched to allow explicit definitions), but any finite subset $Y$ of $X^*$ satisfying $Y \models E_n$ has cardinality $\geq s(n)/2$, where $s(n)$ is the standard non-Kalmar-elementary function defined by $s(1) = 2$ and $s(n + 1) = 2^{s(n)}$ (see [5, p. 287]).

The fact that our lower bounds are not Kalmar-elementary (they lie in $S^4$ of the Grzegorczyk hierarchy; see [2]) has a special significance. Namely,
most familiar formulations of the predicate calculus (and the equation calculus) can be transformed into one another with at most a Kalmar-elementary change in length. Thus $\mathcal{E}^4$ lower bounds apply to all these formalizations.

In another paper we shall give $\mathcal{E}^4$ upper bounds for Gentzen's natural deduction rules [8]. By the above remark, $\mathcal{E}^4$ upper bounds apply to other familiar systems as well.

II. The equational theory consists of the axiom schemata for combinatory logic on $S$, $B$, $C$, and $I$ (corresponding to the $\lambda$-$I$ calculus) together with an axiom schema relating new constants $p$ and $q$. More precisely, we consider the language containing only the binary function symbol $( )$ (with association to the left) and the constants $S$, $B$, $C$, $I$, $p$, $q$, 0 and 1. Let $\mathcal{C} = \{Sxyz = (xz)(yz), Bxyz = x(yz), Cxyz = (xz)y, Ix = x\}$; the equational theory is $\mathcal{C} \cup \{px = p(qx)\}$.

Let $T = (SB)((CB)I)$, set $T_1 = T$, and put $T_{n+1} = T_nT$. The normal form of a term (if it exists) is its normal form with respect to the rules $(S)$, $(B)$, $(C)$ and $(I)$ of [1, pp. 152–153]. Let $E_n$ be the equation $pq = p((T_nq)q)$. For other notions concerning combinatory logic used below we refer the reader to [1], [3], and [4].

III. 1. First, we give a lower bound on the number of instances of $px = p(qx)$ needed to prove $E_n$ from $\mathcal{C}^*$. For this we need the following:

**Lemma.** Suppose that $X$ is a finite subset of $\{px = p(qx)\}^*$ such that $\mathcal{C}^* \cup X \vdash E_n$; then there is a finite subset $Y$ of $\{px = p(qx)\}^*$ such that $\mathcal{C}^* \cup Y \vdash E_n$, $|Y| \leq |X|$, and each term occurring in $Y$ is closed and in normal form.

**Proof.** Observe first that if $x$ occurs in $M$ then $[pN/x]M$ has a normal form $\Rightarrow pN$ has a normal form, and $[pN/x]M$ has a normal form $\Leftrightarrow [p(qN)/x]M$ has a normal form. Suppose that $\mathcal{C}^* \cup X \vdash E_n$. There is a derivation [7, 2.11 (iii) (b), 3.4, 3.5]

\[
\begin{align*}
   pq &= M_1 \quad E(1) \\
   pq &= M_2
\end{align*}
\]

\[
\begin{align*}
   pq &= M_1 \quad E(l) \\
   pq &= M_{l+1}
\end{align*}
\]
by the rule of substituting equals for equals ([7, 2.6 (1)]) with \( E(i) \in C^* \cup X, \) 
\( M_1 = p q, \) 
\( M_{i+1} = p((T_n q)q), \) and \( M_i \neq M_{i+1}. \) Since \( M_1 \) and \( M_{i+1} \) have normal forms it follows from the Church-Rosser theorem that each \( M_i \) has a normal form. Thus for each \( E(i) \in X \) each term occurring in \( E(i) \) has a normal form.

We now show:

**Theorem.** Suppose \( X \) is a finite subset of \( \{ px = p(qx) \}^* \) such that \( C^* \cup X \vdash E_n \) and each term occurring in \( X \) is closed and in normal form; then \( |X| > s(n)/2. \)

**Proof.** Suppose to the contrary that \( X = \{ pM_i = p(qM_i) \} : 1 < i < m < s(n)/2 \). Let \( q^i = q \) and \( q^{i+1} = qq^i \); then for some \( 1 < k < s(n) + 1 \) and for each \( 1 < i < m \) neither \( M_i \) nor \( qM_i \) is finite. We now define an extension \( C^+ \) of \( C \). \( C^+ \) is obtained from \( C \) by adding the infinitely many equations corresponding to the following reduction rules: if \( M \) is a closed term in normal form without \( p \) in function position, then

\[
pM \triangleright 0 \quad \text{if} \quad M = q^j \quad \text{for} \quad j < k,
\]

\[
pM \triangleright 1 \quad \text{otherwise.}
\]

By Theorem 3 of [4], \( C^+ \) has the Church-Rosser property so \( \forall C^+ \not\vdash 0 = 1. \) Let \( E_n^+ \) be the equation \( pq = pq^{a(n)+1} \); then \( \forall C^+ \not\vdash E_n^+ \) so, since \( pq^{a(n)+1} \) is the normal form of \( p((T_n q)q) \), \( \forall C^+ \not\vdash E_n. \)

It suffices to show that \( \forall C^+ \vdash pM_i = p(qM_i) \) for \( 1 < i < m. \)

**Case 1.** \( M_i \) does not contain \( p \) in function position. Either \( M_i \) is not of the form \( q^i \) for any \( j \) so \( pM_i = p(qM_i) \triangleright 1, \) or \( M_i \) is \( q^j \) and \( j, j + 1 < k \) so \( pM_i = p(qM_i) \triangleright 0 \) or \( k < j, j + 1 \) so \( pM_i = p(qM_i) \triangleright 1. \)

**Case 2.** \( M_i \) contains \( p \) in function position. \( M_i \) has a “normal form” in \( \forall C^+ \) containing 0 or 1 and without \( p \) in function position so \( pM_i = p(qM_i) \triangleright 1. \)

III. 2. Now suppose we have any system of rules sound for equational consequence and satisfying: there is a constant \( k \) such that any derivation with \( n \) assumptions has at least \( n/k \) lines. Let \( \vdash^* \) mean (relative) derivability in \( \leq n \) lines then

\[
(C \cup \{ px = p(qx) \})^* \vdash^* E_n \Rightarrow s(n)/(2 \cdot k) < m.
\]

IV. We now show how to informally prove \( E_n \) from \( \forall(C \cup \{ px = p(qx) \}) \) in a number of lines linear in \( n. \) These proofs can be formalized in any of the usual schematic systems of the predicate calculus with at most a linear increase in the number of lines. We argue as if we were in a model of \( \forall(C \cup \{ px = p(qx) \}). \)

Define a sequence of sets \( H_m \) as follows: \( H_1 = \{ y : \forall x px = p(yx) \} \) and \( H_{m+1} = \{ y : \forall z \in H_m yz \in H_m \}. \) Now \( \forall yx Txy = y(xy) \) and \( \forall x px = p(yx) \rightarrow \forall x px = p(y(xy)) \) so \( T \in H_2. \) More generally, \( \forall z \in H_m yz \in H_m \rightarrow \forall z \in H_m y(z) \in H_m \), so \( \forall y \in H_{m+1} T y \in H_{m+1} \) that is \( T \in H_{m+2}. \) Fi-
nally, for each $n$, $T \in H_{n+2}$, $T \in H_{n+1}$, ..., $T \in H_2$ so $T_n \in H_2$. Since $q \in H_1$, $T_nq \in H_1$; that is $pq = p((T_nq)q)$.

V. Analysis of the above proof yields $S^4$ lower bounds for a much simpler equational theory with a decidable word problem. We leave this to the reader. It would be interesting to find a natural equation theory, i.e., one which occurs in real mathematical life, which achieves these bounds.

REFERENCES


DEPARTMENT OF PHILOSOPHY, UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN 48104