LOWER BOUNDS ON HERBRAND'S THEOREM

R. STATMAN¹

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 ,

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

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 ϵ -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 ϵ -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 $> s(n)/2$, 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 $\mathfrak{S}^4$ of the Grzegorzcyk hierarchy; see [2]) has a special significance. Namely,

---

Received by the editors April 3, 1978.

AMS (MOS) subject classifications (1970). Primary 02D99.

¹The author would like to thank the referee for useful comments on an earlier draft of this paper.

by the rule of substituting equals for equals ([7, 2.6 (1)]) with $E(i) \in \mathcal{C}^* \cup X$, $M_1 = pq$, $M_{l+1} = p((T_n q)q)$, and $M_i \neq M_{i+1}$. Since M_1 and M_{l+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 $\mathcal{C}^* \cup X \models E_n$ and each term occurring in X is closed and in normal form; then $|X| \geq s(n)/2$.*

PROOF. Suppose to the contrary that $X = \{pM_i = p(qM_i)\}: 1 \leq i \leq m < s(n)/2\}$. Let $q^1 = q$ and $q^{l+1} = qq^l$; then for some $1 < k \leq s(n) + 1$ and for each $1 \leq i \leq m$ neither M_i nor qM_i is q^k . We now define an extension $\mathcal{C}^+$ of $\mathcal{C}$. $\mathcal{C}^+$ is obtained from $\mathcal{C}$ 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

$$\begin{aligned} pM &\triangleright 0 && \text{if } M = q^j \text{ for } j < k, \\ &\triangleright 1 && \text{otherwise.} \end{aligned}$$

By Theorem 3 of [4], $\mathcal{C}^+$ has the Church-Rosser property so $\forall \mathcal{C}^+ \neq 0 = 1$. Let E_n^+ be the equation $pq = pq^{s(n)+1}$; then $\forall \mathcal{C}^+ \neq E_n^+$ so, since $pq^{s(n)+1}$ is the normal form of $p((T_n q)q)$, $\forall \mathcal{C}^+ \neq E_n$.

It suffices to show that $\forall \mathcal{C}^+ \models pM_i = p(qM_i)$ for $1 \leq i \leq m$.

Case 1. M_i does not contain p in function position. Either M_i is not of the form q^j 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 $\forall \mathcal{C}^+$ 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 $\vdash^n$ mean (relative) derivability in $\leq n$ lines then

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

IV. We now show how to informally prove E_n from $\forall(\mathcal{C} \cup \{px = p(qx)\})$ 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 $\forall(\mathcal{C} \cup \{px = p(qx)\})$.

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 $\forall yx Tyx = y(yx)$ and $\forall x px = p(yx) \rightarrow \forall x px = p(y(yx))$ so $T \in H_2$. More generally, $\forall z \in H_m yz \in H_m \rightarrow \forall z \in H_m y(yz) \in H_m$ so $\forall y \in H_{m+1} Ty \in H_{m+1}$ that is $T \in H_{m+2}$. Fi-

nally, for each n , $T \in H_{n+2}$, $T \in H_{n+1}$, $\dots$, $T \in H_2$ so $T_n \in H_2$. Since $q \in H_1$, $T_n q \in H_1$; that is $pq = p((T_n q)q)$.

V. Analysis of the above proof yields $\mathfrak{S}^4$ 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

1. H. B. Curry and R. Feys, *Combinatory logic*, Vol. 1, North-Holland, Amsterdam, 1968.
2. A. Grzegorzczuk, *Some classes of recursive functions*, *Rozprawy Mat.* **4** (1953).
3. R. Hindley, *An abstract form of the Church-Rosser theorem. I*, *J. Symbolic Logic* **34** (1969).
4. ———, *An abstract form of the Church-Rosser theorem. II*, *J. Symbolic Logic* **39** (1974).
5. S. C. Kleene, *Introduction to metamathematics*, Van Nostrand, Princeton, N.J., 1952.
6. G. Kreisel, *What have we learnt from Hilbert's second problem*, in *Proc. Sympos. Pure Math.*, vol. 28, Amer. Math. Soc., Providence, R.I., 1976.
7. R. Statman, *Herbrand's theorem and Gentzen's notion of a direct proof*, in Jon Barwise, ed., *Handbook of Mathematical Logic*, North-Holland, Amsterdam, 1977, pp. 897–912.
8. ———, *Proof-search and speed-up in the predicate calculus*, *Ann. Math. Logic* (to appear).

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