Notre Dame Journal of Formal Logic
Volume XIII, Number 1, January 1972
NDJFAM

NON-RECURSIVENESS OF THE SET OF FINITE SETS OF EQUATIONS WHOSE THEORIES ARE ONE BASED

DOUGLAS D. SMITH

Among the decision problems for finite sets of equations listed by A. Tarski [1] are six related problems, five of which were solved by Peter Perkins [2]. The solution for the one equation case of the remaining problem S_3, given below, follows closely the method (and notation) of Perkins, reducing the problem to the (unsolvable) word problem of a semigroup, but making a modification in a set of equations used by Perkins and introducing a transformation on terms which allows us to show that the equations do not "mix" (in the sense indicated by our lemma below). This property of "not mixing" was suggested by the work of W. E. Singletary on partial propositional calculi [3].

We assume the basic notions from [1]. Thus, for a set of equations $\mathbf{E}$, the equational theory of $\mathbf{E}$, $\mathrm{Th}(\mathbf{E})$, is one based iff there exists a single equation e such that $\mathrm{Th}(e) = \mathrm{Th}(\mathbf{E})$.

Theorem*. *The set of finite sets of equations whose equational theories are one based is not recursive. Specifically, there is no effective method for determining whether or not the equational theory of an arbitrary finite set of equations in two binary operation symbols and two constants is one based.*

Proof: Let $\beta:\{a, b; U_i = V_i, 1 \le i \le n\}$ be a finite presentation of a semigroup with unsolvable word problem. Let $\mathfrak{L}^+$ denote an equational language having one binary operation +. To each β-word (i.e., word in a and b) we make correspond a term $\mathrm{W}(x, y)$ in the language $\mathfrak{L}^+$, as follows:

$$\begin{array}{ll} \text{if } \mathrm{W} \text{ is } a, & \mathrm{W}(x,y) \text{ is } (y + x) + x \\ \text{if } \mathrm{W} \text{ is } b, & \mathrm{W}(x,y) \text{ is } x + (x + y) \\ \text{if } \mathrm{W} \text{ is } a\mathrm{W}_1, & \mathrm{W}(x,y) \text{ is } (\mathrm{W}_1(x,y) + x) + x \\ \text{if } \mathrm{W} \text{ is } b\mathrm{W}_1, & \mathrm{W}(x,y) \text{ is } x + (x + \mathrm{W}_1(x,y)). \end{array}$$

*In a letter received after our proof was completed, George F. McNulty indicates that he has a result from which ours follows.

Received July 17, 1970

Observe that for each β-word W, the variables occurring in $W(x,y)$ are precisely x and y. $\mathbf{E}(\beta)$ is defined to be the set $\{U_i(x, y) = V_i(x, y) \mid i \leq n\}$ of equations of $\mathfrak{L}^+$. Perkins showed that for any pair UV of β-words,

$$\{U_i = V_i \mid i \leq n\} \vdash U = V \text{ iff } \mathbf{E}(\beta) \vdash U(x, y) = V(x, y).$$

Let $\mathfrak{L}$ be a language having two binary operation symbols $+$ and $\cdot$, and two constants, c_1 and c_2. For each pair U, V of β-words we define a set of equations $\mathbf{P}UV$ in the language $\mathfrak{L}$. $\mathbf{P}UV$ consists of $\mathbf{E}(\beta)$ together with

$$U(c_1, c_2) \cdot x = x$$
$$V(c_1, c_2) \cdot x = V(c_1, c_2).$$

It will be shown that for each U, V, $\mathrm{Th}(\mathbf{P}UV)$ is one based iff $\mathbf{E}(\beta) \vdash U(x, y) = V(x, y)$. This, with Perkins' result above and the assumption that β has an unsolvable word problem, establishes the theorem.

Part 1. If $\mathbf{E}(\beta) \vdash U(x, y) = V(x, y)$ then $\mathbf{P}UV \vdash U(c_1, c_2) = V(c_1, c_2)$. Therefore $\mathbf{P}UV \vdash U(c_1, c_2) \cdot x = V(c_1, c_2) \cdot x$, so $\mathbf{P}UV \vdash x = V(c_1, c_2)$, hence $\mathbf{P}UV \vdash x = y$. Since $\mathbf{P}UV$ is inconsistent, $\mathrm{Th}(\mathbf{P}UV)$ is one based. We conclude that if $\mathbf{E}(\beta) \vdash U(x, y) = V(x, y)$, then $\mathrm{Th}(\mathbf{P}UV)$ is one based.

Part 2. Assume now that not $\mathbf{E}(\beta) \vdash U(x, y) = V(x, y)$. It must be shown that $\mathrm{Th}(\mathbf{P}UV)$ is not one based. We first make two observations.

(a) If $\mathbf{E}$ is any set of equations, and for some term t not identically x, $x = t \in \mathrm{Th}(\mathbf{E})$, then for some term s there is an equation of the form $y = s$ (or $s = y) \in \mathbf{E}$.

(b) Let $\mathfrak{A}$ be $\langle A, \oplus\rangle = F_\omega/\mathbf{E}(\beta)$, the relatively free algebra on ω generators determined by $\mathbf{E}(\beta)$. Since $U(x, y) = V(x, y)$ does not hold in $\mathfrak{A}$, there exist a_1, a_2, a_3, a_4 in A such that $a_3 = U(a_1, a_2) \neq V(a_1, a_2) = a_4$. If $\mathfrak{A}$ is expanded to $\overline{\mathfrak{A}} = \langle A, \oplus, \odot, a_1, a_2\rangle$ by defining $\oplus$ as in $\mathfrak{A}$, $a_3 \odot a = a$ for all $a \in A$, $a_4 \odot a = a_4$ for all $a \in A$, and $\odot$ arbitrarily otherwise, then $\overline{\mathfrak{A}}$ is a model of $\mathbf{P}UV$ and the sentence $U(c_1, c_2) \neq V(c_1, c_2)$, so that $\mathbf{P}UV$ is consistent and not $\mathbf{P}UV \vdash U(c_1, c_2) = V(c_1, c_2)$.

Definition. With each term t in the language $\mathfrak{L}$ we associate a term $t(UV)$ (depending on the pair U, V of β-words). The transformation sending t to $t(UV)$ is defined inductively as follows (where $t(iUV)$ abbreviates $t_i(UV)$: if t is a variable or a constant, $t(UV)$ is t; if t is a sum $t_1 + t_2$, $t(UV)$ is $t(1UV) + t(2UV)$; if t is a product $t_1 \cdot t_2$ and

(i) $\mathbf{P}UV \vdash t_1 = U(c_1, c_2)$, then $t(UV)$ is $t(2UV)$
(ii) $\mathbf{P}UV \vdash t_1 = V(c_1, c_2)$, then $t(UV)$ is $V(c_1, c_2)$
(iii) otherwise, $t(UV)$ is $t(1UV) \cdot t(2UV)$.

By (b) and the assumption that not $\mathbf{E}(\beta) \vdash U(x,y) = V(x,y)$, conditions (i) and (ii) are mutually exclusive.

Properties of the transformation. The proof of each of the properties below is by induction on the number, n, of operation symbols in t. Only the proof of (4) is given; it appears with the proof of our lemma following the proof of the theorem.

(1) $\mathbf{P}UV \vdash t = t(UV)$.
(2) If t has no occurrence of $\cdot$, $t(UV) \equiv t$.
(3) Let t have no occurrence of $\cdot$, and for terms $r_1, r_2, \ldots, r_n$ and variables $x_1, x_2, \ldots, x_n$ let $t[r_1/x_1, \ldots, r_n/x_n]$ denote the simultaneous substitution of $r_1, \ldots, r_n$ for $x_1, \ldots, x_n$ respectively. Then

$$t[r_1/x_1, \ldots, r_n/x_n]\,(UV) \equiv t[r(1UV)/x_1, \ldots, r(nUV)/x_n].$$

(4) If $R \subseteq \mathbf{P}UV$, s, t, p and q are terms, s a subterm of t, q the result of replacing one occurrence of s by p in t, and $R \vdash s(UV) = p(UV)$, then $R \vdash t(UV) = q(UV)$.

Lemma. *If* $\mathbf{P}UV \vdash s = t$, *then* $\mathbf{E}(\beta) \vdash s(UV) = t(UV)$ (*and conversely*).

Suppose now that $\mathrm{Th}(\mathbf{P}UV)$ is one based. Then by (a) and the fact that $U(c_1, c_2) \cdot x = x \in \mathbf{P}UV$, the base equation has the form $y = r$, and since $\mathbf{P}UV \vdash y = r$, we have by the lemma that $\mathbf{E}(\beta) \vdash y(UV) = r(UV)$, i.e., $\mathbf{E}(\beta) \vdash y = r(UV)$. Now by (a) and the fact that none of $U_i(x,y)$, $V_i(x,y)$ consist of a single variable, $r(UV) \equiv y$. It is easily verified from the definition of the transformation that either $y \equiv r$, or, for some $k \in \omega$, r is of the form $r_1 \cdot r_2 \cdot \ldots \cdot r_k \cdot y$ (right association) where for $i \leq k$, $\mathbf{P}UV \vdash r_i = U(c_1, c_2)$.

Therefore $y = x \cdot y \vdash y = r$. But $V(c_1, c_2) \cdot x = V(c_1, c_2)$ is not derivable from $y = x \cdot y$. (In fact, the equations in $\mathbf{E}(\beta)$ are also not derivable from $y = x \cdot y$.) Hence the assumptions that not $\mathbf{E}(\beta) \vdash U(x,y) = V(x,y)$ and $\mathrm{Th}(\mathbf{P}UV)$ is one based lead to a contradiction, proving our theorem.

Proof of (4). For $n = 0$, t is a constant or a variable and t is s, hence $t(UV) \equiv s(UV) \equiv t \equiv s$ and p is q so that $p(UV) \equiv q(UV)$; therefore if $R \vdash s(UV) = p(UV)$, then $R \vdash t(UV) = q(UV)$.

For $n > 0$, assume first t is $t_1 + t_2$. Then if s is t, the proof is as in the case $n = 0$. Otherwise q is $q_1 + q_2$, where, say, the occurrence of s in t to be replaced by p is a subterm of p_i and the result of this replacement is $q_i (i = 1$ or $2)$. If $R \vdash s(UV) = p(UV)$ then by hypothesis of induction $R \vdash t(iUV) = q(iUV)$ and for t_j ($j = 2$ or 1), the subterm of t not affected by the replacement, q_j is t_j, hence also $R \vdash t(jUV) = q(jUV)$; therefore we have both $R \vdash t(1UV) = q(1UV)$ and $R \vdash t(2UV) = q(2UV)$. Hence $R \vdash r(1UV) + t(2UV) = q(1UV) + q(2UV)$; that is $R \vdash t(UV) = q(UV)$.

Assume now that t is $t_1 \cdot t_2$. Then if s is t, the proof is as in the case $n = 0$. Otherwise q is $q_1 \cdot q_2$, where, say, the occurrence of s in t to be replaced by p is a subterm of $t_i (i = 1$ or $2)$ and q_i is the result. If $R \vdash s(UV) = p(UV)$ then by hypothesis of induction $R \vdash t(iUV) = q(iUV)$, and for t_j ($j = 2$ or 1), the subterm of t not affected by the replacement, t_j is q_j, so that also $R \vdash t(jUV) = q(jUV)$; therefore we have both $R \vdash t(1UV) = q(1UV)$ and $R \vdash t(2UV) = q(2UV)$. Now by property (1) and our assumption $R \subseteq \mathbf{P}UV$, we have also $\mathbf{P}UV \vdash t_1 = q_1$. Therefore either (i) $\mathbf{P}UV \vdash t_1 = U(c_1, c_2)$, hence $\mathbf{P}UV \vdash q_1 = U(c_1, c_2)$, so we have not only $R \vdash t(2UV) = q(2UV)$ but both $t(UV) \equiv t(2UV)$ and $q(UV) \equiv q(2UV)$, hence $R \vdash t(UV) = q(UV)$; or (ii) $\mathbf{P}UV \vdash t_1 = V(c_1, c_2)$, hence $\mathbf{P}UV \vdash q_1 = V(c_1, c_2)$, so we have $t(UV) \equiv V(c_1, c_2) \equiv q(UV)$, therefore $R \vdash t(UV) = q(UV)$; or, finally, (iii) neither $\mathbf{P}UV \vdash t_1 = U(c_1, c_2)$ nor $\mathbf{P}UV \vdash t_1 =$

$V(c_1, c_2)$, in which case neither $\mathbf{P}UV \vdash q_1 = U(c_1, c_2)$ nor $\mathbf{P}UV \vdash q_1 = V(c_1, c_2)$, so we have both $t(UV) \equiv t(1UV) \cdot t(2UV)$ and $q(UV) \equiv q(1UV) \cdot q(2UV)$ and since $R \vdash t(1UV) = q(1UV)$ and $R \vdash t(2UV), = q(2UV)$, $R \vdash t(UV) = q(UV)$.

Proof of the lemma. We make use of a characterization of derivability to be found (for the case of a language with only one binary operation) in Perkins' paper. We first define four classes of operators which map terms onto terms:

$$\mathrm{L}_w(w') = w + w' \quad \mathrm{R}_w(w') = w' + w$$
$$\mathcal{L}_w(w') = w \cdot w' \quad \mathcal{R}_w(w') = w' \cdot w.$$

The class of (left-right) operators is the least class containing the identity operator and L_w, R_w, $\mathcal{L}_w$, $\mathcal{R}_w$ for all terms w, and closed under composition. Now $\mathbf{P}UV \vdash s = t$ iff there exists a sequence $T_i s_i = T_i t_i$ $i = 1, \ldots, n$ such that (i) each T_i is a (left-right) operator, (ii) each $s_i = t_i$ or $t_i = s_i$ is a substitution instance of an equation in $\mathbf{P}UV$ or else s_i is t_i, (iii) $T_1 s_1$ is s, (iv) $T_n t_n$ is t, and (v) $T_i t_i$ is $T_{i+1} s_{i+1}$ for $i \leq n - 1$.

We assume that $\mathbf{P}UV \vdash s = t$, and that $T_i s_i = T_i t_i$ $i \leq n$ is a sequence described above. It will be enough to show that for each $i \leq n$, $\mathbf{E}(\beta) \vdash s(iUV) = t(iUV)$; indeed, by property (4), with $\mathbf{E}(\beta)$ for R, we will then have, for each $i \leq n$, $\mathbf{E}(\beta) \vdash (T_i s_i)(UV) = (T_i t_i)(UV)$, hence $\mathbf{E}(\beta) \vdash s(UV) = t(UV)$.

If s_i is t_i then $s(iUV) \equiv t(iUV)$ and, trivially, $\mathbf{E}(\beta) \vdash s(iUV) = t(iUV)$. Otherwise, let $p = q$ be an equation in $\mathbf{P}UV$ such that $s_i = t_i$ (or $t_i = s_i$) is a substitution instance of $p = q$. If $p = q$ is $U(c_1, c_2) \cdot x = x$, then for some term r, $s_i = t_i$ (or $t_i = s_i$) is $U(c_1, c_2) \cdot r = r$, so $s(iUV) \equiv t(iUV) \equiv r(UV)$ and therefore $\mathbf{E}(\beta) \vdash s(iUV) = t(iUV)$. If $p = q$ is $V(c_1, c_2) \cdot x = V(c_1, c_2)$, then for some term r, $s_i = t_i$ (or $t_i = s_i$) is $V(c_1, c_2)$, so (using property (2)) $s(iUV) \equiv t(iUV) \equiv V(c_1, c_2)$ and therefore $\mathbf{E}(\beta) \vdash s(iUV) = t(iUV)$. Finally, if $p = q \in \mathbf{E}(\beta)$ then $s_i = t_i$ (or $t_i = s_i$) is $p[r_1/x, r_2/y] = q[r_1/x, r_2/y]$ for some terms r_1, r_2. By substitution in $p = q$, $\mathbf{E}(\beta) \vdash p[r(1UV)/x, r(2UV)/y] = q[r(1UV)/x, r(2UV)/y]$ and since the symbol $\cdot$ does not occur in $p = q$, we have, by property (3) that $\mathbf{E}(\beta) \vdash p[r_1/x, r_2/y](UV) = q[r_1/x, r_2/y](UV)$, i.e., $\mathbf{E}(\beta) \vdash s(iUV) = t(iUV)$.

REFERENCES

[1] Tarski, A., "Equational logic and equational theories of algebras," in *Contributions to Mathematical Logic* (Proceedings of the Logic Colloquium, Hanover, 1966), pp. 275-288, North Holland, Amsterdam (1968).

[2] Perkins, Peter, "Unsolvable problems for equational theories," *Notre Dame Journal of Formal Logic*, vol. 8 (1967), pp. 175-185.

[3] Singletary, W. E., "Results regarding the axiomatization of partial propositional calculi," *Notre Dame Journal of Formal Logic*, vol. 9 (1968), pp. 193-211.

The Pennsylvania State University
University Park, Pennsylvania