Notre Dame Journal of Formal Logic
Volume VIII, Number 3, July 1967

UNSOLVABLE PROBLEMS FOR EQUATIONAL THEORIES

PETER PERKINS

1. *Introduction.* In 1954 R. Lyndon [7] gave an example of a seven-element groupoid whose identities cannot be deduced from any finite subset. That is, they are not "finitely based." In this paper we present some by-products of an unsuccessful attempt to find, or prove the non-existence of, an effective procedure which would determine of an arbitrary finite groupoid whether or not its identities have a finite basis. Included are the undecidability of certain questions of provability, equational completeness, consistency, and being the basis of the identities of some finite groupoid when asked of finite as well as recursive sets of equations.*

2. *Preliminaries.* We consider, for the most part, algebras of the type $\mathfrak{A} = (A_0, \oplus)$ with one binary operation $\oplus$ on a set A_0 and commonly called groupoids. The generalizations of the notions and definitions that follow to any number of finitary operations, including specified constants, are the obvious ones. Associated with $\mathfrak{A}$ is the language and deductive structure described below.

Language. 1) The set of *variables* is $\{w, x, y, z, w_1, x_1, \ldots\}$.
2) The set of *terms* is the smallest set containing the variables and such that if s and t are terms then $(s + t)$ is a term. the set of subterms of a variable v is $\{v\}$. The set of subterms of $(s + t)$ is the set consisting of $(s + t)$ together with the subterms of s and the subterms of t.
3) The set of *equations* is the set $\{s = t : s, t \text{ are terms}\}$.

Rules of deduction. Let r, s, t, u be terms. The following deductions may be made.

E1 *$s = t$ from $r = u$ if $s = t$ is the result of substituting a term for a variable throughout $r = u$.*

---

*These results form part of the author's doctoral dissertation at the University of California, Berkeley (1966), written with financial support from the Danforth Foundation, and under the kind direction of Professor Dana Scott of Stanford University.

Received August 14, 1966

E2 $s = s$ *from the empty set.*
E3 $s = t$ *from* $t = s$.
E4 $(r + s) = (u + s)$ *from* $r = u$.
E5 $(s + r) = (s + u)$ *from* $r = u$.
E6 $s = t$ *from* $s = r$ *and* $r = t$.

Let E be a set of equations. A finite sequence of equations $e_1, e_2, \ldots, e_n$ is a *proof of* e_n *from* E if each e_i is either an element of E or it is deduced from equations occurring earlier in the sequence by one of the rules of deduction. e is a *theorem of* E or is *provable from* E if there exists a proof of e from E. In this case we write $E \vdash e$.

It is not difficult to show that the following is a derived rule of the system, and, in fact, it could replace collectively **E4**, **E5**, and **E6**.

DE1 $s = t$ *from* $r = u$ *and* $r' = t$ *where* r *is a subterm of* r' *and* s *is the result of replacing* r *by* u *at one occurrence in* r'.

When we talk about the "decision problem" for a set of equations we will always mean the problem of deciding which equations are deducible from E. Familiarity with the notions involved in the definitions and notations given below will be assumed. See, for example, [1]. For quick reference we list the symbols on the left which we use exclusively for the notions given here.

E	- a set of equations.
s, t	- terms.
v	- variable.
$\mathsf{c}(E)$	- the *closure* of E, is the set of all theorems of E.
F_p/E	- the *relatively free algebra* on p generators determined by E, that is, the algebra whose elements are congruence classes given by $s \equiv_E t$ iff $E \vdash s = t$ and whose operations are the natural ones, where s, t involve only variables from a pre-assigned set of cardinality p.
CF_p	- the *completely free term algebra* on p generators is F_p/ϕ.
f, g, h	- assignment functions which are the natural extensions of maps from variables onto elements of an algebra to maps from terms onto elements of an algebra.
$s = t$ *holds* in $\mathfrak{A}$ or $\mathfrak{A}$ is a *model* of $s = t$	- if $f(s) = f(t)$ for all f appropriate for $\mathfrak{A}$. $\mathfrak{A}$ is a model of E if $\mathfrak{A}$ is a model of E for all $e \in E$.
$\mathsf{I}(\mathfrak{A})$	- the *identities of* $\mathfrak{A}$, is the set of all equations holding in $\mathfrak{A}$, that is, the *equational theory of* $\mathfrak{A}$.
$\mathsf{I}_n(\mathfrak{A})$	- the identities of $\mathfrak{A}$ which involve no more than n variables.
$\mathsf{F}_p(\mathfrak{A})$	- the *free* $\mathfrak{A}$ *algebra* on p generators, is $\mathsf{F}_p/\mathsf{I}(\mathfrak{A})$.
$s \leqslant t$	- means s is a subterm of t. Use $<$ for proper subterm.
ρ	- a *rank* function from terms to integers.

$\rho(v) = 0$ all v.
$\rho((s + t)) = 1 + \max\{\rho(s), \rho(t)\}$.

$\mathrm{var}(s)$ - the set of variables occurring in s.

$\mathrm{occ}(v, s)$ - the number of occurrences of v in s.

E is *finitely based* - if there exists a finite set E_0 such that $\mathsf{c}(E_0) = \mathsf{c}(E)$. If E is finitely based there exists a finite set $E_0 \subseteq E$ such that $\mathsf{c}(E_0) = \mathsf{c}(E)$.

$\mathfrak{A}$ is finitely based - if $\mathsf{I}(\mathfrak{A})$ is.

Notice that the existence of F_ω/E gives us a completeness theorem in the sense that $E \vdash e$ iff every model of E is a model of e. Furthermore, the congruence determined by E on CF_ω is the least congruence on CF_ω which includes $E^* = \{\langle s, t\rangle : s = t \in E\}$ and preserves substitution. In order to develop another characterization of provability we define two classes of operators which map terms onto terms.

$$\mathsf{L}_t(u) = (t + u) \qquad \mathsf{R}_t(u) = (u + t)$$

The class of L, R-*operators* is the least class containing L_t and R_t for all terms t and closed under composition.

Theorem 1. *$E \vdash s = t$ iff there exists a sequence $\mathsf{T}_i(s_i) = \mathsf{T}_i(t_i)$, $i = 1, \ldots, n$ such that*

1) *Each T_i is an L, R-operator.*
2) *Each $s_i = t_i$ or $t_i = s_i$ is a substitution instance of a member of E or else s_i is t_i.*
3) *$\mathsf{T}_1(s_1)$ is s.*
4) *$\mathsf{T}_n(t_n)$ is t.*
5) *$\mathsf{T}_i(t_i)$ is $\mathsf{T}_{i+1}(s_{i+1})$, $i = 1, \ldots, n-1$.*

We shall call such a sequence a T-*sequence* for $s = t$.

Proof: Both directions follow easily from a proof theoretic, inductive argument on the length of a given proof sequence in one direction and the length of the given T-sequence in the other. Q.E.D.

Theorem 1 alone allows us to easily construct many sets of equations that are not finitely based. We need only be sure that for any finite subset $E_0 \subseteq E$ there will exist some member $s = t \in E$ such that s has no subterm which is a substitution instance of a side of some member of E_0. For example, let $\mathsf{D}(t)$ be $(t + t)$ and D^n be D composed with itself in n times. Let $E = \{\mathsf{L}_x\mathsf{D}^n(x) = \mathsf{R}_x\mathsf{D}^n(x) : n = 1, 2, \ldots\}$. F_ω/E is not finitely based.

3. *Recursive sets of equations*. As we mentioned in the introduction, the attempt to determine if the set of non-finitely based finite algebras is decidable was unsuccessful. In fact, it is not known if this set is recursively enumerable. In spite of the fact that such questions about finite algebras are apparently difficult, related questions about recursive sets of equations can be settled rather quickly without the necessity of translating some known unsolvable word problem. We give in this section an example of a recursive set of equations in one binary operation symbol and no constants whose decision problem is unsolvable. The effective

unrecognizability of various properties of recursive sets of equations of the above type is then demonstrated. All results are based on an algebra constructed by J. Kalicki [3] together with the existence of a recursive set R of pairs of natural numbers whose second coordinates form a non-recursive set R' [5] [8]. Let such an R be given (and kept fixed). We make the following definitions.

Ox stands for x.
$(n+1)x$ stands for $(nx + nx)$.

Similarly for a binary operation within an algebra.

$H = \{2^m 3^n 5^n | \langle m, n\rangle \in R\}$
$K_p = \{2^m 3^n 5^p | \langle m, n\rangle \in R\}$, $p = 1, 2, 3, \ldots$

$E_p(R)$ or simply E_p shall be the following set of equations.

1) $1x + x = 1y + y$
2) $(m+1)x + mx = 2^n x + x$ for each $\langle m, n\rangle \in R$.
3) $hx + x = 1x + x$ for each $h \in H$.
4) $kx + x = x$ for each $k \in K_p$.

D shall be the set of equations in 1) and 2) only.

$\mathbf{K}(B,C)$ where B and C are any disjoint sets of natural numbers with $1 \notin C$, shall be a class of models of the type $\mathfrak{A} = \langle A_0, \oplus\rangle$ with $A_0 = \{a_1, a_2, \ldots\}$, and for each $i = 1, 2, \ldots$

$a_{i+1} \oplus a_i = a_1$
$a_i \oplus a_i = a_{i+1}$
$a_{i+b} \oplus a_i = a_1$ for all $b \in B$.
$a_{i+c} \oplus a_i = a_i$ for all $c \in C$.
$a_i \oplus a_j$ is arbitrary otherwise.

Note that $na_i = a_{i+n}$.

Lemma 2. *$D \vdash (r+1)x + rx = (u+1)x + ux$ for all $r, u = 0, 1, \ldots$*

Proof: By repeated substitution of $1x$ for x in 1).

Theorem 3. *D has an unsolvable decision problem.*

Proof: Let e_q be $2^q x + x = 1x + x$ and claim that $D \vdash e_q$ iff $q \in R'$. Certainly if $q \in R'$, Lemma 2 and the appropriate instance of 2) yield $D \vdash e_q$. If $q \notin R'$, we can take $B = \{2^n | n \in R'\}$ and $C = \{2^n | n \notin R'\}$ so that any of the Kalicki models $\mathbf{K}(B,C)$ are models of D in which e_q does not hold. For example, $2^q a_2 \oplus a_2 = a_{2+2^q} \oplus a_2 = a_2$ while $1a_2 \oplus a_2 = a_1$. Consequently, e_q is not provable from D. Q.E.D.

Theorem 4. *There is no effective method for determining whether or not an arbitrary recursive set of equations in one binary operation symbol and no constants 1) has a solvable decision problem 2) is consistent 3) has a finite basis.*

Proof: 1) and 2) Consider the classes E_p, $p = 1, 2, \ldots$ of sets of

equations. If $p \in R'$, then $H \cap K_p \neq \phi$ so that $E_p \vdash 1x + x = x$, $x = y$. That is, if $p \in R'$, then E_p is decidable, inconsistent, and has a finite basis. If $p \notin R'$, then with e_q as in the previous theorem $E_p \vdash e_q$ iff $q \in R'$. For, if $q \in R'$, as in the previous theorem, $E_p \vdash e_q$ while if $q \notin R'$, we take $B = H \cup \{2^n | n \in R'\}$ and $C = K_p \cup \{2^n | n \notin R'\}$. Again, any $\mathbf{K}(B,C)$ satisfies E_p but not e_q. Thus, e_p is consistent and undecidable.

3) We need only show that in case $p \notin R'$ then E_p does not have a finite basis. Suppose $E_0 \subseteq E_p$ is a finite basis for E_p Let H_0 be the finite subset of H involved in E_0 via equations of type 3), let J be the set of all powers of 2, $B = H_0 \cup J$, and $C = (H - H_0) \cup K_p$. Since $H \cap J = \phi$, any $\mathbf{K}(B,C)$ is a model of E_0 but not of $hx + x = 1x + x$ when $h \in H - H_0$. For such an h would give $ha_2 \oplus a_2 = a_{2+h} \oplus a_2 = a_2$ while $1a_2 \oplus a_2 = a_{2+1} \oplus a_2 = a_1$. So E_0 could not be a basis. Q.E.D.

Theorem 5. *There is no effective method for determining whether or not an arbitrary recursive set of equations in one binary operation symbol and no constants is 1) equationally complete or 2) the basis of a finite algebra.*

Proof: Define $F_p(R)$ or simply F_p to be the following.

$$
\begin{array}{ll}
1x + x = 1y + y & \\
(hx + x) + y = (1x + x) + y & \text{for each } h \in H. \\
(kx + x) + y = x + y & \text{for each } k \in K_p. \\
y + (hx + x) = y + (1x + x) & \text{for each } h \in H. \\
y + (kx + x) = y + x & \text{for each } k \in K_p.
\end{array}
$$

As before, if $p \in R'$ then $H \cap K_p \neq \phi$ so we have

$$
\begin{array}{l}
F_p \vdash x + y = (1x + x) + y = (1y + y) + y;\ x + y = z + y \\
F_p \vdash y + x = y + (1x + x) = y + (1y + y);\ y + x = y + w \\
F_p \vdash x + y = z + y = z + w
\end{array}
$$

Thus, all models of F_p are constant algebras, F_p is equationally complete and, in fact, the basis of any finite constant algebra. If $p \notin R'$ any $\mathbf{K}(B,C)$ with $B = H$ and $C = K_p$ is a model of F_p. But in the $\mathbf{K}(B,C)$, $a_i \oplus a_j$ was arbitrary for $i < j$ so we could make the models commutative or not as we wish and thus, F_p is not equationally complete. Also note that no equation of the type $nx = (n + k)x$ can be proved from F_p since none such holds in the above $\mathbf{K}(B,C)$'s. Any finite model would have to have some such equation holding and hence F_p could not be the basis of a finite algebra. Q.E.D.

4. *A finite set of equations with unsolvable decision problem.* As we will see in Section 5, the results of Section 5 can be improved in the sense that we get similar results concerning finite sets of equations although not always with one binary operation symbol and no constants. In this section, however, we shall show how to construct such a set which is finite and has unsolvable decision problem.

Let $\mathfrak{P}$: $\{a, b; U_i = V_i, 1 \leq i \leq n\}$ be a finite presentation of a semigroup throughout this section. If any of the U_i's or V_i's is either a or b, we call $\mathfrak{P}$ *singular*, otherwise non-singular. Most of this section is devoted to proving the following theorem.

Theorem 6. *The word problem for any finite, non-singular, semigroup presentation on two generators and n relations can be effectively reduced to the decision problem for a set of n equations in two variables and one binary operation symbol.*

The existence of such a presentation with unsolvable word problem will lead us to the result mentioned in the opening paragraph. First consider the following rules of deduction for relations. We begin numbering with **R2** in order that an exact comparison with the rules **Ei** of Section 2 can be made. If A, B, and C are arbitrary words in a and b then the following deductions are possible.

R2 $A = A$ *from the empty set.*
R3 $A = B$ *from* $B = A$.
R4 $AC = BC$ *from* $A = B$.
R5 $CA = CB$ *from* $A = B$.
R6 $A = B$ *from* $A = C$ *and* $C = B$.

If R is a set of relations then the notion of $R \vdash A = B$ is defined in the same way as $E \vdash s = t$ was defined in Section 2. Preliminary to associating relations with equations we want to assign to each word in a and b, which we shall call a $\mathfrak{P}$-*word*, a special $\mathbf{L},\mathbf{R}$-operator. (Recall the definition from Section 2.) Abbreviate the operators $\mathbf{L}_x$ and $\mathbf{R}_x$ by $\mathbf{L}$ and $\mathbf{R}$. To each $\mathfrak{P}$-word W we assign an operator $\overline{W}$ by:

$\overline{a}$ is $\mathbf{R}^2$
$\overline{b}$ is $\mathbf{L}^2$
$\overline{Wa}$ is $\overline{W}\mathbf{R}^2$
$\overline{Wb}$ is $\overline{W}\mathbf{L}^2$

For example, if W is ba then $\overline{W}(y)$ is $(x + (x + ((y + x) + x)))$.

Now, $\mathbf{E}(\mathfrak{P})$ shall be $\{U_i(y) = V_i(y)\}$, $1 \leqslant i \leqslant n$. We call t a $\mathfrak{P}$-*term* if t is $\overline{W}(y)$ for some $\mathfrak{P}$-word W. $s = t$ is a $\mathfrak{P}$-*equation* if s and t are $\mathfrak{P}$-terms, and it is *balanced* if it is a $\mathfrak{P}$-equation or if neither s nor t is a $\mathfrak{P}$-term. Note that a term is a $\mathfrak{P}$-term iff it can be expressed as $\mathbf{T}(y)$ where $\mathbf{T}$ is an alternating composition of operators of the form $\mathbf{L}^{2m}$ and $\mathbf{R}^{2n}$.

Lemma 7. $\overline{UV} = \overline{U}\overline{V}$

Proof: By induction on the length of V and association of composition.

Lemma 8. *The six element algebra* $\mathfrak{A} = \langle A_0, \oplus \rangle$ *given by the following table is a model of* $\mathbf{E}(\mathfrak{P})$.

	1	2	3	4	5	0
1	2	3	5	0	3	0
2	3	0	0	0	0	0
3	4	0	0	0	0	0
4	3	0	0	0	0	0
5	0	0	0	0	0	0
0	0	0	0	0	0	0

Proof: Let $t = u \in \mathbf{E}(\mathfrak{P})$ and f be any assignment function. If $f(x) = 1$, then $f(t) = f(u) = 0$. So assume $f(x) = 1$. If $f(y) = 1, 3$ then $f(t) = f(u) = 3$. If $f(y) = 0, 2, 4, 5$, then $f(t) = f(u) = 0$ since $\mathfrak{P}$ is non-singular and hence both left and right associations must occur in t and in u. Q.E.D.

Lemma 9. *If* $\mathbf{E}(\mathfrak{P}) \vdash t = u$ *then* $t = u$ *is balanced.*

Proof: Suppose t is a $\mathfrak{P}$-term. $\mathrm{var}(t) = \mathrm{var}(u) = \{x, y\}$ since this is a property of $\mathbf{E}(\mathfrak{P})$ easily seen to be preserved under deduction. By the previous lemma $t = u$ must hold in $\mathfrak{A}$. Since t is not identically 0 in $\mathfrak{A}$ and $(x + y) + (z + w)$ is, we know that u must also be strings of x's and y's alternately associated left and right. But, if y appears in u at other than the lowest level, an assignment $f(x) = 1$ and $f(y) = 3$ would imply $f(t) = 3$ and $f(u) = 0$. Finally, if the strings of x's between changes of association were not of even length, the just mentioned assignment would yield the same contradiction. Q.E.D.

Lemma 10. $R \vdash U = V$ iff $\mathbf{E}(\mathfrak{P}) \vdash \overline{U}(y) = \overline{V}(y)$.

Proof: For the only if part use induction on the length n of a proof sequence for $U = V$. If $n = 1$, then $\overline{U}(y) = \overline{V}(y)$ is a proof from $\mathbf{E}(\mathfrak{P})$. Suppose the statement is true for all relations having proofs of length $< k + 1$. Let $U = V$ be the last line of a proof of length $k + 1$. If it is an element of R, we revert to the case $n = 1$. If it was deduced using **R2, R3,** or **R6,** the inductive hypothesis together with rules **E2, E3,** and **E6** suffice. If $U = V$ was deduced using **R4,** then U is AC, V is BC and $A = B$ occurs earlier in the proof. Write a proof of $\overline{A}(y) = \overline{B}(y)$ from $\mathbf{E}(\mathfrak{P})$ then substitute $\overline{C}(y)$ for y getting $\overline{A}(\overline{C}(y)) = \overline{B}(\overline{C}(y))$ which is $\overline{AC}(y) = \overline{BC}(y)$ by Lemma 7. Finally, if **R5** was used, U is CA, V is CB, and $A = B$ occurs earlier. Write a proof for $\overline{A}(y) = \overline{B}(y)$, follow it with $\overline{C}(\overline{A}(y)) = \overline{C}(\overline{A}(y))$ and use derived rule **DE1** to get a proof of $\overline{CA}(y) = \overline{CB}(y)$ from $\mathbf{E}(\mathfrak{P})$

Now we prove the converse. Related to a proof of $\overline{U}(y) = \overline{V}(y)$ is a **T**-sequence of equations $\mathbf{T}_i(s_i) = \mathbf{T}_i(t_i)$ $i = 1, \ldots, n$ referred to in Section 2. $\mathbf{T}_1(s_1)$ is $\overline{U}(y)$ so Lemma 9 tells us that both sides of all the equations in the **T** sequence must be $\mathfrak{P}$-terms. Consequently, the s_i and t_i, being both subterms and substitution instances of $\mathfrak{P}$-terms, must themselves be $\mathfrak{P}$-terms. Furthermore, the substituents must have been $\mathfrak{P}$-terms and have been substituted for y rather than x in a member of $\mathbf{E}(\mathfrak{P})$. Since $\mathbf{T}_i(s_i)$ and s_i are both $\mathfrak{P}$-terms, $\mathbf{T}_i$ must be an even **L,R**-operator, that is, $\mathbf{T}_i$ is $\overline{D}_i$ for some $\mathfrak{P}$-word D_i. If $s_i = t_i$ of the **T** sequence is the result of substituting $\overline{C}_i(y)$ for y in $\overline{A}_i(y) = \overline{B}_i(y)$, then we convert the **T** sequence into a proof of $U = V$ from R by replacing the i^{th} equation by the four relations $A_i = B_i$, $A_iC_i = B_iC_i$, $D_iA_iC_i = D_iB_iC_i$ and $D_1A_1C_1 = D_iB_iC_i$. The last line will be $D_1A_1C_1 = D_nB_nC_n$ and the sequence will be a proof sequence for $U = V$.

The proof of Theorem 6 is now complete. As a matter of fact, if we consider the encoding used by M. Hall in [2] which reduces the word problem of an arbitrary finite presentation with n relations to that for a non-singular finite presentation on two generators and n relations, we get a stronger result.

Theorem 11. *The word problem of any finite semigroup presentation with n relations can be effectively reduced to the decision problem of a set of n equations in two variables and one binary operation symbol.*

Trakhtenbrot [9] gives a presentation due to G. S. Tsentin with unsolvable word problem using only seven relations. Thus, we finally state the following theorem.

Theorem 12. *A set of seven equations in two variables and one binary operation symbol can be constructed whose decision problem is unsolvable.*

5. *More unsolvable problems concerning finite sets of equations.* In this section we shall prove four unsolvability results about finite sets of equations in two binary operation symbols and two constants. We then indicate how, at least for the consistency question, the result can be improved to finite sets of equations in one binary operation symbol and no constants. Let $\mathfrak{P}$ and $\mathbf{E}(\mathfrak{P})$ be as in Section 4 and further assume $\mathfrak{P}$ has unsolvable word problem and hence $\mathbf{E}(\mathfrak{P})$ has unsolvable decision problem for $\mathfrak{P}$-equations. If W is a $\mathfrak{P}$-word, then we write $W(x, y)$ for the term $\overline{W}(y)$, and $W(G, H)$ will have its usual meaning as a term of an element of an algebra depending on which meaning G and H have.

Theorem 13. *There is no effective method for determining whether or not an arbitrary set of equations in two binary operation symbols and two constants 1) is consistent 2) has solvable decision problem 3) is equationally complete 4) is the basis of a finite algebra.*

Proof: 1) and 2); For each pair of $\mathfrak{P}$-words, U and V define the set of equations *PUV1* to be the set $\mathbf{E}(\mathfrak{P})$ along with

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

Certainly if $e\colon U(x, y) = V(x, y)$ is provable from $\mathbf{E}(\mathfrak{P})$ then *PUV1* is inconsistent and decidable. On the other hand, if it is not provable we shall show that for any $\mathfrak{P}$-words U_1 and V_1, $e_1\colon U_1(x, y) = V_1(x, y)$ is provable from $\mathbf{E}(\mathfrak{P})$ iff it is provable from *PUV1*. The only if part is obvious since $\mathbf{E}(\mathfrak{P}) \subseteq$ *PUV1*. Now, suppose not $\mathbf{E}(\mathfrak{P}) \vdash e_1$. Since we are currently in the not $\mathbf{E}(\mathfrak{P}) \vdash e$ case we know that $\mathfrak{A} = \mathbf{F}_\omega/\mathbf{E}(\mathfrak{P})$ is a model of $\mathbf{E}(\mathfrak{P})$ in which neither e nor e_1 hold. Let $\mathfrak{A} = \langle A_0, \oplus\rangle$ and $a_1, a_2, a_3, a_4, \varepsilon A_0$ be such that $a_3 = U(a_1, a_2) \neq V(a_1, a_2) = a_4$. Extend $\mathfrak{A}$ to $\overline{\mathfrak{A}} = \langle A_0, \oplus, \odot, a_1, a_2\rangle$ where

$a \odot a_3 = a$ for all $a \varepsilon A_0$.
$a \odot a_4 = a_2$ for all $a \varepsilon A_0$.
$\odot$ defined arbitrarily otherwise.
$\oplus$ defined as in $\mathfrak{A}$.

$\overline{\mathfrak{A}}$ is clearly a model of *PUV1*, but not of e_1 which establishes in this case the consistency of *PUV1*, and the equivalence of provability of $\mathfrak{P}$-equations from $\mathbf{E}(\mathfrak{P})$ and from *PUV1*, which then gives us our result.

Proof of 3) and 4); For each pair of $\mathfrak{P}$-words U and V let *PUV2* be $\mathbf{E}(\mathfrak{P})$ along with

$$
\begin{aligned}
c_1 \cdot U(c_1, c_2) &= c_1 . \\
c_1 \cdot V(c_1, c_2) &= c_2 . \\
(x \cdot y) \cdot U(c_1, c_2) &= x \quad y . \\
(x \cdot y) \cdot V(c_1, c_2) &= c_2 . \\
(x \cdot y) \cdot U(c_1, c_2) &= x + y \\
(x \cdot y) \cdot V(c_1, c_2) &= c_2
\end{aligned}
$$

Again let e: $U(x, y) = V(x, y)$. If $\mathbf{E}(\mathfrak{P}) \vdash e$, it is easy to see that $PUV2 \vdash c_1 = c_2 = x + y = x \cdot y$ so that *PUV2* is a basis for the identities of any algebra (of the right type) whose two operations are the same constant function and also that *PUV2* is equationally complete.

If not $\mathbf{E}(\mathfrak{P}) \vdash e$ construct the model $\overline{\mathfrak{A}}$ just as in the proof of 1) and 2) and note that it is also a model of *PUV2*. Thus, $U(c_1, c_2) = V(c_1, c_2)$ is not provable from *PUV2* but the constant algebras mentioned above demonstrate that it is consistent with *PUV2*.

Still assuming not $\mathbf{E}(\mathfrak{P}) \vdash e$, we want to show that *PUV2* could not be the basis of a finite algebra. Suppose otherwise and let x^2 denote $(x \cdot x)$ and x^{k+1} denote $(x^k \cdot x)$. We see that some equation of the form $x^{n+k} = x^n$ must be deducible from *PUV2*. This is impossible since in $\overline{\mathfrak{A}}, \odot$ was arbitrary except on a_3 and a_4 so we could complete the definition of $\odot$ in a way that would prevent any such equation from holding. Hence the two properties 3) and 4) are possessed by *PUV2* iff $\mathbf{E}(\mathfrak{P}) \vdash U(x, y) = V(x, y)$, which again gives us our desired result. Q.E.D.

Finally we prove the following improvement of the consistency result.

Theorem 14. *There is no effective method for determining whether or not an arbitrary finite set of equations in one binary operation symbol and no constants is consistent.*

Proof: (detailed outline) We will indicate how to effectively associate with any finite set E of equations with finitary operation symbols, another finite set $\overline{E}$ of equations in just one binary operation symbol such that E has a model iff $\overline{E}$ does. Then, using Theorem 13, Theorem 14 will follow.

Let $f_1, \ldots, f_N$ be the operation symbols involved in E with f_i being n_i-ary. Use $+$ for the binary operation symbol of $\overline{E}$. Define N terms of the $\overline{E}$ type in one variable to be used as constants and another N terms to help imitate the f_1 as follows.

x^2 is $(x + x)$ and x^3 is $(x^2 + x)$.
$\mathbf{C}_i(x)$ is $\mathbf{W}_i(x^2, x^2)$ $i = 1, \ldots, N$ where $\mathbf{W}_i(x, y)$ are distinct $\mathfrak{P}$-terms of the same length.
$\mathbf{G}_i(x_1, \ldots, x_{n_i})$ is $(\ldots (x_1^3\ x_2^3) \ldots, x_{n_i}^3)$

Associate inductively terms of E type with terms of $\overline{E}$ type by:

$\overline{v}$ is v for all variables
$\overline{f_i(t_1, \ldots, t_{n_i})}$ *is* $\mathbf{C}_i(x) + \mathbf{G}_i(\overline{t}_1, \ldots, \overline{t}_{n_i})$ $i = 1, \ldots, N$

Now, $\overline{E}$ is to include $\mathbf{C}_i(x) = \mathbf{C}_i(y)$, $i = 1, \ldots, N$ together with $\overline{s} = \overline{t}$ for

each $s = t \in E$. If $\bar{E}$ has a model $\bar{\mathfrak{A}} = \langle \bar{A}_0, \oplus \rangle$ we define $\mathfrak{A} = \langle A_0, \mathbf{F}_1, \ldots, \mathbf{F}_n \rangle$ by $A_0 = \bar{A}_0$, $\mathbf{F}_i(a_1, \ldots, a_{n_i}) = \mathbf{c}_i \oplus \mathbf{G}_i(a_1, \ldots, a_{n_i})$ where $\mathbf{c}_i$ is the constant value $\mathbf{C}_i(x)$ in $\bar{A}_0$. It is easy to see that $\mathfrak{A}$ is a model of E. Simply show by induction on terms that any assignment function has the same value on t as on $\bar{t}$.

Suppose now that $\mathfrak{A}$ is a model of E. Can we use it to construct a model of $\bar{E}$? Certainly we can assume $A_0 = \{1, 2, 3, \ldots\}$. Choose primes $p, q > N$ and *tentatively* define $m \oplus n = p^m q^n$. Each $\mathbf{C}_i(x)$ is, of course, the sum of two subterms say $\mathbf{B}_i(x) + \mathbf{D}_i(x)$ where one of these two is x^2, that is, $(x + x)$. Check that

1) no subterms of $\mathbf{C}_j(n)$ is $\mathbf{B}_i(k) \oplus \mathbf{D}_i(k)$ unless $i = j$ and $n = k$.
2) no subterm of $i \oplus \mathbf{G}_i(a_1, \ldots, a_{n_i})$ is $\mathbf{B}_j(k) \oplus \mathbf{D}_j(k)$.
3) no subterm of $\mathbf{C}_j(n)$ is $i \oplus \mathbf{G}_i(a_1, \ldots, a_{n_i})$.
4) no subterm of $i \oplus \mathbf{G}_i(a_1, \ldots, a_{n_i})$ is $j \oplus \mathbf{G}_j(b_1, \ldots, b_{n_j})$ unless $i = j$ and $a_k = b_k$ $k = 1, \ldots, n_i$.

Consequently it makes sense to redefine $\oplus$ by

$$m \oplus n \begin{cases} i & \text{if for some } k,\ m \text{ is } \mathbf{B}_i(k),\ n \text{ is } \mathbf{D}_i(k). \\ a & \text{if } m \text{ is } i,\ n \text{ is } \mathbf{G}_i(a_1, \ldots, a_{n_i}) \text{ and } \mathbf{F}_i(a_1, \ldots, a_{n_i}) = a. \\ & \text{as before otherwise} \end{cases}$$

Again, one checks by induction on terms that t and $\bar{t}$ have identical values under any assignment in A_0 to their variables. Thus, if $\mathfrak{A}$ is a model of E then $\bar{\mathfrak{A}}$ is a model of $\bar{E}$. Q.E.D.

Finally, in contrast to Theorem 14, we point out there does exist an effective method for determining whether or not an arbitrary finite set of semigroup equations (i.e. containing the associative law) in one binary operation symbol is consistent.

BIBLIOGRAPHY

[1] P. M. Cohn, *Universal Algebra*, New York, Harper & Row, 1965.

[2] M. Hall, The word problem for semigroups with two generators. *J. Symbolic Logic*, vol. 14, pp. 115-118, 1949.

[3] J. Kalicki, The number of equationally complete classes of equations. *Nederl. Akad. Wetensch. Proc.* Ser. A, vol. 58, No. 5, pp. 660-662, 1955.

[4] J. Kalicki, On comparison of finite algebras, *Proc. Amer. Math. Soc.*, vol. 3, pp. 36-40, 1952.

[5] S. C. Kleene, *Introduction to Metamathematics*, Princeton, New Jersey, D. Van Nostrand Co., Inc., 1952.

[6] R. C. Lyndon, Identities in two valued calculi, *Trans. Amer. Math. Soc.*, vol. 71, pp. 457-465, 1951.

[7] R. C. Lyndon, Identities in finite algebras, *Proc. Amer. Math. Soc.*, vol. 5, pp. 8-9, 1954.

[8] W. E. Singletary, Personal communication.

[9] B. A. Trakhtenbrot, *Algorithms and Automatic Computing Machines*, Translated from the Russian, Boston, D. C. Heath and Co., 1963.

College of the Holy Cross
Worcester, Massachusettes