Algebra Universalis, 8 (1978) 197–204 Birkhäuser Verlag, Basel

An algebra has a solvable word problem if and only if it is embeddable in a finitely generated simple algebra

TREVOR EVANS[1]

Introduction

We consider the word problem for recursively presented algebras in a variety V, given by a finite number of finitary operations and a finite number of identities. Kuznecov (see Malcev [6], p. 209) was apparently the first to note that a finitely generated simple V-algebra which is recursively presented has a solvable word problem. Hence, so does any recursively generated subalgebra of such an algebra. We prove a converse of this in the following form. Let V^* be the variety of all algebras of the same similarity type as V (i.e. having the same set of operations but defined by the empty set of identities).

THEOREM. *A V-algebra has a solvable word problem if and only if it can be embedded in a finitely generated simple V^*-algebra which is recursively presented.*

Boone and Higman [1] have shown that a finitely generated group has a solvable word problem if and only if it can be embedded in a simple group which is in turn embeddable in a finitely presented group. One cannot hope for an exact analogue of this for other varieties of algebras since a fundamental aspect of the result for groups is the use of the embedding theorem of Higman [4] that a finitely generated recursively presented group is embeddable in a finitely presented group. Using the analogue of this for semigroups (Murskii [7]), Boone and Higman prove in [1] the theorem for semigroups corresponding to their theorem for groups. There cannot be a Higman-type embedding theorem for lattices, non-associative systems such as loops and quasigroups, commutative rings, commutative semigroups, abelian groups, nilpotent groups, and commutative Moufang loops. The most plausible candidate for such a theorem would seem to

[1] This research was supported in part by NSF Grant GP-37506X
Presented by G. Grätzer. Received January 10, 1977. Accepted for publication in final form February 10, 1977.

be rings. However, even without this embedding theorem, K. Mandelberg, M. F. Neff and the author [2] were able to show for the varieties of (i) rings of characteristic p, (ii) loops, (iii) groupoids, (iv) lattices, that a finitely generated V-algebra (V, one of the above varieties) has a solvable word problem if and only if it can be embedded in a simple V-algebra which is embeddable in a finitely generated recursively presented V-algebra.

The main point of this paper is in the observation that if we allow embeddings in recursively related algebras there is a corresponding universal-algebraic result since an identity may be replaced by a recursive set of defining relations and we can consider the problem in the context of varieties defined by the empty set of identities. Of course, it is still of interest to obtain analogues of the Boone-Higman result in which a V-algebra is embedded in a finitely generated simple V-algebra (there is such a theorem for loops) or further analogues of the type in [2].

We remark finally that we will always assume that the varieties V we discuss contain no nullary operations and do not consist solely of unary operations. A non-trivial unary algebra cannot in general be embedded in a simple algebra.

Embedding an algebra in a simple algebra

Let V and V^* be as in the introduction. Let A be a V-algebra generated by a finite or countably infinite set $g_1, g_2, g_3, \ldots$. A will be said to be *recursively presented*, as a V-algebra, by these generators and a set of defining relations if, in terms of some effective enumeration $w_1, w_2, w_3, \ldots$ of the set W of all words in the generators, the set of defining relations is a recursively enumerable set of ordered pairs of words. We observe that A is also a V^*-algebra and that since each defining identity of V may be replaced by a recursive set of defining relations, A is also recursively presented as a V^*-algebra.

To construct the simple algebra K containing A, we begin by selecting some k-ary operation $\prod$ of A, for $k \geq 2$. The generators of K will be the generators of A and a countably infinite set $H = \{c_1, c_2, b_1, b_2, b_3, \ldots\}$. It will be convenient, in describing the defining relations of K, to use the notation $\sum(\langle x\rangle, y)$ as an abbreviation for the word $\sum(x, x, \ldots, x, y)$ where $\sum$ is any operation of V^* and x, y are any words in the generators of K. The defining relations of K are four types.

(1) The defining relations of A as a V^*-algebra.

(2) For $i, j = 1, 2, 3, \ldots$

$$\prod(\langle w_i\rangle, c_1)=c_2, \prod(\langle w_i\rangle, c_2)=c_1,$$

$$\prod(\langle w_i\rangle, b_j)=\begin{cases} c_1 & \text{if } w_i=w_j \text{ in } A, \\ c_2 & \text{if } w_i\neq w_j \text{ in } A, \end{cases}$$

$$\prod(\langle c_1\rangle, w_i)=c_1, \prod(\langle c_1\rangle, c_1)=w_1,$$

$$\prod(\langle c_1\rangle, c_2)=c_1, \prod(\langle c_1\rangle, b_i)=w_i,$$

$$\prod(\langle c_2\rangle, w_i)=w_i, \prod(\langle c_2\rangle, c_1)=c_1,$$

$$\prod(\langle c_2\rangle, c_2)=b_1, \prod(\langle c_2\rangle, b_i)=b_{i+1},$$

$$\prod(\langle b_i\rangle, w_j)=c_1, \prod(\langle b_i\rangle, c_1)=c_1,$$

$$\prod(\langle b_i\rangle, c_2)=c_1, \prod(\langle b_i\rangle, b_j)=\begin{cases} c_1 & \text{if } i=j, \\ c_2 & \text{if } i\neq j. \end{cases}$$

(3) For any words $u_1, u_2, \ldots, u_k \in W \cup H$ such that at least one is an element of H and $u_1, u_2, \ldots, u_{k-1}$ are neither (i) the same generator from H nor (ii) words in W which are equal in A, we take as a defining relation of K

$$\prod(u_1, u_2, \ldots, u_k)=c_1.$$

(4) For any n-ary operation $\sum$ of V^* other than $\prod$ and any words $u_1, u_2, \ldots, u_n \in W \cup H$ such that at least one u_i is a generator from H, we take as a defining relation of K

$$\sum(u_1, u_2, \ldots, u_n)=c_1.$$

We remark that if $\prod$ is a binary operation then the set of relations (3) above is vacuous. Of course, we can always regard V as having a binary operation by treating the derived operation $\prod(\langle x\rangle, y)$ as one of the fundamental operations of A but in V^* it will no longer be a derived operation. The effect of the relations (1) is to guarantee that A or some homomorphic image of A is contained in K and the relations (4) make every operation, other than $\prod$, constant outside A. In fact, relative to the presentation of A, the defining relations above are the complete operation tables for K.

LEMMA 1 *K is generated by c_1. If A has a solvable word problem, then K is recursively presented.*

Proof. K is generated by c_1 since $\prod(\langle c_1\rangle, c_1) = w_1$, $\prod(\langle w_1\rangle, c_1) = c_2$, $\prod(\langle c_2\rangle, c_2) = b_1$ and $\prod(\langle c_2\rangle, b_i) = b_{i+1}$, $\prod(\langle c_1\rangle, b_i) = w_i$, for $i = 1, 2, 3, \ldots$. We assume that in the enumeration $w_1, w_2, w_3, \ldots$, we know in particular which are the generators $g_1, g_2, g_3, \ldots$ and thus have an effective way of writing every generator of A as a word in c_1. Now, if A has a solvable word problem, so that we have a procedure for deciding if $w_i = w_j$ in A, then the defining relations we have given for K form a recursive set. Substituting the corresponding words in c_1 for the generators of K gives a recursive presentation for K in terms of the generator c_1.

The *length* of a word in the generators $g_1, g_2, g_3, \ldots, c_1, c_2, b_1, b_2, b_3, \ldots$ is defined by (i) each generator has length one (ii) if the words $u_1, u_2, \ldots, u_n$ have length $\lambda_1, \lambda_2, \ldots, \lambda_n$ respectively and $\sum$ is an n-ary operation in V, then the word $\sum(u_1, u_2, \ldots, u_n)$ has length $1+\lambda_1+\lambda_2+\ldots+\lambda_n$. The subwords $u_1, u_2, \ldots, u_n$ of the word $\sum(u_1, u_2, \ldots, u_n)$ are called its *principal subwords*.

LEMMA 2. *K is simple.*

Proof. We first show that any word u in K is equal to some w_i in W or one of $c_1, c_2, b_1, b_2, b_3, \ldots$ in H. This is certainly true for words of length one. Let u be $\sum(u_1, u_2, \ldots, u_n)$, of length λ, and assume the lemma true for words of length less than λ. The induction hypothesis applied to the principal subwords of u gives $\sum(u_1, u_2, \ldots, u_n) = \sum(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n)$ where $\bar{u}_i = u_i$ in K and $\bar{u}_i \in W \cup H$, $i = 1, 2, \ldots, n$. The defining relations (2), (3), (4) imply that $\sum(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n)$ is equal to a word in $W \cup H$. Induction completes the proof.

It follows from this result that in considering a non-trivial congruence on K, we may restrict ourselves to congruences which contain a pair (u, v) of words in $W \cup H$. Furthermore, since K may be generated by c_1 using only the operation $\prod$, all we need for the simplicity of K is that $\prod(\langle c_1\rangle, c_1) \equiv c_1(\theta)$ for any non-trivial congruence θ. All possibilities are covered by the following eight cases.

$w_i \equiv w_j(\theta)$ for some $w_i \neq w_j$ in A. (i)

Then $\prod(\langle w_i\rangle, b_i) \equiv \prod(\langle w_j\rangle, b_i)(\theta)$. By the defining relations (2), $c_1 \equiv c_2(\theta)$. Hence, $\prod(\langle c_1\rangle, c_1) \equiv \prod(\langle c_2\rangle, c_1)(\theta) \equiv c_1(\theta)$, again by (2).

$w_i \equiv c_1(\theta)$ for some w_i. (ii)

Then $\prod(\langle c_1\rangle, c_1) \equiv \prod(\langle c_1\rangle, w_i) \equiv c_1(\theta)$.

$w_i \equiv c_2(\theta)$. (iii)

Then $\prod(\langle w_i\rangle, w_i) \equiv \prod(\langle w_i\rangle, c_2)(\theta)$. That is, $w_k \equiv c_1(\theta)$ for some w_k. Case 2 now applies.

$$w_i \equiv b_j(\theta), \tag{iv}$$

Then $\prod(\langle w_i\rangle, w_i) \equiv \prod(\langle b_j\rangle, w_i)$. That is, $w_k \equiv c_1(\theta)$ for some w_k. Case 2 applies.

$c_1 \equiv c_2(\theta)$. This is covered by the argument for case 1. (v)

$c_1 \equiv b_i(\theta)$, for some i. (vi)

Then $\prod(\langle c_1\rangle, c_1) \equiv \prod(\langle b_i\rangle, c_1) \equiv c_1(\theta)$.

$c_2 \equiv b_i(\theta)$, for some i. (vii)

Then $\prod(\langle c_2\rangle, w_1) \equiv \prod(\langle b_i\rangle, w_1)(\theta)$. i.e. $w_1 \equiv c_1(\theta)$. Case 2 now applies.

$b_i \equiv b_j(\theta)$, for some $i \neq j$. (viii)

Then $\prod(\langle b_i\rangle, b_i) \equiv \prod(\langle b_i\rangle, b_j)(\theta)$. i.e. $c_1 \equiv c_2(\theta)$ and case 5 applies.

This concludes the proof that K is simple. It remains only to show that K contains A isomorphically. The next four lemmas are devoted to this and constitute a refinement of the result of the first paragraph in the proof of Lemma 2. We show that for any word u in K the word $\bar{u}$ in $W \cup H$ equal to u is unique (to within equality in A).

Let u be a word in K. By a *reduction* of u of type (2), (3), (4), we mean replacing a subword of u which is the left-hand side of a defining relation of K of type (2), (3), (4) by the corresponding right-hand side of the relation. By a *reduction* of type (5) we mean a similar use of the following relations which are consequences of the first three defining relations of type (2) and the defining relations (1) of A.

(5) For any $w_{i_1}, w_{i_2}, \ldots, w_{i_{k-1}} \in W$ such that $w_{i_1} = w_{i_2} = \cdots = w_{i_{k-1}}$ in A,

$$\prod(w_{i_1}, \ldots, w_{i_{k-1}}, c_1) = c_2, \prod(w_{i_1}, \ldots, w_{i_{k-1}}, c_2) = c_1,$$

$$\prod(w_{i_1}, \ldots, w_{i_{k-1}}, b_j) = \begin{cases} c_1 & \text{if} \quad w_{i_1} = w_j \quad \text{in} \quad A, \\ c_2 & \text{if} \quad w_{i_1} \neq w_j \quad \text{in} \quad A. \end{cases}$$

A word in K is *reduced* if no reductions of it are possible. A reduced word $\bar{u}$ is a *reduced form* of u if it can be obtained from u by a finite sequence of reductions.

LEMMA 3. *If u is a word in K and $u \to u'$, $u \to u''$ are two reductions of u with u', u'' different words, then either u' or u'' can be reduced to the other or there is a word u'' obtainable from both u', u'' by reductions.*

Proof. We use induction on the length of u. The statement is vacuously true for u of length one. Assume it true for words of length less than λ and let u be of length λ. Now u has the form $\sum(u_1, u_2, \ldots, u_n)$ where $u_1, u_2, \ldots, u_n$ are its principal subwords and $\sum$ is an operation of V. There are three cases to consider.

(i) The reductions take place in different principal subwords of u, say $u \to u'$ reduces u_i to u_i' and $u \to u''$ reduces u_j to u_j', $i<j$. We may take u''' as $\sum(u_1, \ldots, u_i', \ldots, u_j', \ldots, u_n)$.

(ii) Both reductions take place in the same principal subword of u, say u_i, reducing u_i to u_i' and u_i''. The lemma follows by the induction hypothesis applied to u_i since u_i', u_i'' can be reduced to a word u_i'''.

(iii) One of the reductions, say $u \to u'$ involves the whole of u and the other takes place in the principal subword u_i, reducing it to u_i'. By consideration of each type of reduction, we see that $\sum(u_1, \ldots, u_i', \ldots, u_n)$ can also be reduced to u'.

This completes the proof of the lemma. Note that it is impossible for both reductions $u \to u'$, $u \to u''$ to involve the whole of u.

LEMMA 4. *Every word in K has a unique reduced form, either some w_i or one of $c_1, c_2, b_1, b_2, b_3, \ldots$.*

Proof. We again use induction on length. If u is a word in K, we have to show that any two sequences of reductions $u \to u' \to \ldots$, $u \to u'' \to \ldots$ end in the same reduced form $\bar{u}$. The lemma is true for words of length one. Assume true for words of length less than λ and let u be of length λ. If u', u'' are the same word, the statement follows by the induction hypothesis since $\bar{u}'$ is the unique reduced form of u'. If u', u'' are different words, then by the induction hypothesis, they have unique reduced forms $\bar{u}'$, $\bar{u}''$. By Lemma 3, either a sequence of reductions of one of them contains the other in which case by induction $\bar{u}'$, $\bar{u}''$ are the same, or else there is a word u''' obtainable from u', u'' by reductions and then once again by induction $\bar{u}'$, $\bar{u}''$ are the same.

This concludes the proof of the lemma. We remark that the techniques used in Lemmas 3, 4 are similar to those in Theorem 2.1 in [3].

LEMMA 5. *Let u, v be words in K such that $u = v$ in K. Then, either*

(i) $\bar{u}, \bar{v} \in W$ and $\bar{u} = \bar{v}$ in A, or

(ii) $\bar{u}, \bar{v}$ are identical and belong to H.

Proof. The proof is by induction on the number n of applications of the defining relations (1), (2), (3), (4), (5) needed to transform u into v. The induction step is trivial and the only case requiring a detailed proof is $n = 1$. In this case, if the defining relation used is of type (2), (3), (4), (5), then one of u, v is obtained from the other by a reduction and the result follows from Lemma 4. If $n = 1$ and the transformation uses a relation of type (1), i.e. an application of the defining relations of A, we use induction on the length of u, as follows.

Let u be $\sum(u_1, u_2, \ldots, u_n)$ where $\sum$ is an n-ary operation and $u_1, u_2, \ldots, u_n$ are the principal subwords of u. If the application of the defining relation of A involves the whole of u, then both u and v are words in W and there is nothing to prove. Otherwise, the application of the defining relation takes place inside one of the principal subwords u_i, transforming it to v_i, so that v is $\sum(u_1, \ldots, v_i, \ldots, u_n)$. Consider the words $\sum(\bar{u}_1, \ldots, \bar{u}_i, \ldots, \bar{u}_n)$ and $\sum(\bar{u}_1, \ldots, \bar{v}_i, \ldots, \bar{u}_n)$. By Lemma 4, each of $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n, \bar{v}_i$ is either a w_j or one of $c_1, c_2, b_1, b_2, b_3, \ldots$. By our induction hypothesis either $\bar{u}_i, \bar{v}_i \in W$ and $\bar{u}_i = \bar{v}_i$ in A or else $\bar{u}_i, \bar{v}_i$ are identical and belong to H. At most one further reduction is possible for each of $\sum(\bar{u}_1, \ldots, \bar{u}_i, \ldots, \bar{u}_n)$ and $\sum(\bar{u}_1, \ldots, \bar{v}_i, \ldots, \bar{u}_n)$ and consideration of cases shows that the reduced forms $\bar{u}, \bar{v}$ obtained satisfy the conclusion of the lemma.

LEMMA 6. *A is embedded isomorphically in K.*

Proof. By Lemma 5, if $w_i, w_j \in W$, then $w_i = w_j$ in K if and only if $w_i = w_j$ in A.

This concludes the proof of one half of our main result.

THEOREM. *A recursively presented V-algebra has a solvable word problem if and only if it can be embedded in a one-generator recursively presented simple V^*-algebra.*

The other half of the proof is essentially due to Kuznecov (see Malcev [6], p. 209). Let K be a one-generator recursively related simple V^*-algebra. Let A be a subalgebra of K given by its generators $w_1, w_2, w_3, \ldots$ as words in the generator c of K. Let u, v be two words in A. An enumeration of the consequences of the defining relations of K will eventually yield $u = v$, if this equation holds in A. On the other hand, since K is simple, if $u \neq v$ in A, then an enumeration of the consequences of the defining relations of A and the added relation $u = v$ will yield the equations $\sum(c, c, \ldots, c) = c$ for every $\sum$ of K. Combining these enumerations, we have a procedure for solving the word problem for A.

Since this paper was submitted my attention has been drawn to an announcement by Kuznecov [5] in which he states that a finitely presented algebra A has a solvable word problem if and only if A can be embedded in a finitely presented simple algebra B where "embedded" here means that the sets of elements of A, B are the same but the set of operations of A is a subset of the set of operations of B. Both A and B lie in finitely presented varieties. No details of the proof are given.

REFERENCES

[1] W. W. BOONE and G. HIGMAN, *An algebraic characterization of groups with soluble word problem*, J. Australian Math. Soc. (Hanna Neumann memorial volume) *2*, 41–53.

[2] T. EVANS, K. I. MANDELBERG and M. F. NEFF, *Embedding algebras with solvable word problems in simple algebras. Some Boone-Higman type theorems*, Proc. of Logic Colloquium, Univ. of Bristol, July 1973, North-Holland Publ. Co., (1975), 259–277.

[3] T. EVANS, *On multiplicative systems defined by generators and relations, I. Normal form theorems*, Proc. Cambr. Phil. Soc., vol. *47* (1951), 637–649.

[4] G. HIGMAN, *Subgroups of finitely presented groups*, Proc. Royal Soc., A, vol. *262* (1961), 455–475.

[5] A. V. KUZNECOV, Usphemat. Nauk., 3rd issue (1958), 240.

[6] A. I. MALCEV, *The Metamathematics of Algebraic Systems*, Collected Papers: 1936–1967, North-Holland Publ. Co., 1971.

[7] V. L. MURSKII, *Isomorphic embedding of a semi-group with an enumerable set of defining relations in a finitely presented semi-group*, Matem. Sametki, vol. *1* (1967), 217–224.

Emory University
Atlanta, Georgia
U.S.A.