BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 5, September 1978

WORD PROBLEMS

BY TREVOR EVANS[1]

Introduction. In studying fundamental groups of manifolds, Dehn [4] in 1911 investigated some special cases of a problem which is now known as *the word problem for groups*. Let G be a group generated by a finite set of elements $a, b, c, \ldots$. Each element in G is a product of these generators and their inverses, for example, $a^{-1}bacb^{-1}c$. We call such expressions $w(a, b, c, \ldots)$ *words* in the generators. G is assumed to ge given by a finite set of equations or *defining relations* $r(a, b, c, \ldots) = 1$ which the generators satisfy. The question Dehn proposed was to find a uniform test or mechanical procedure (i.e. an *algorithm*) which enables us to decide whether $w = 1$ for an arbitrary word $w(a, b, c, \ldots)$ in G. We say that the word problem is *solvable* for the group G if there is such an algorithm.

A different version of the same kind of problem was posed by Thue a year or two later [35]. Consider an "abstract language" L having a finite alphabet $a, b, c, \ldots$. A word in L is a finite sequence of symbols from the alphabet, for example, *baabccba*. A language L (usually called a *Thue system*) is defined on the alphabet $a, b, c, \ldots$ by a *dictionary*, a finite set of pairs of words. If a word w is of the form usv, where u, v are words and s is a word which occurs in the dictionary paired with a word t, then we say that w can be *transformed* by the dictionary into the word utv and we write $usv \to utv$. If there is a finite sequence of transformations $w \to \cdots \to w'$ connecting two words w, w', then we say that w, w' are *equivalent* in L. Thue's problem, which we may call *the word problem for the language* L, asks for an algorithm for deciding whether two words in the language are equivalent. We say that the word problem is *solvable* for L if there is such an algorithm.

These two problems are examples of the same general situation. We have an algebra $\mathfrak{A}$ which is generated by elements $a, b, c, \ldots$. The elements of the algebra are represented by expressions (*words*) involving the generators and the operations. The algebra satisfies certain axioms and is characterized by certain basic relations $r = r'$ where the r, r' are words. We wish to find some effective test for deciding whether two words $w(a, b, c, \ldots), w'(a, b, c, \ldots)$ represent the same element of the algebra, i.e. whether $w = w'$ follows from the axioms and the relations $r = r'$. The question of the existence of such an algorithm is called *the word problem* for the algebra. Obviously the word problem for groups is of this type. The word problem for the language L becomes such a question if we view L as a semigroup given by generators

An invited address delivered to the American Mathematical Society in Nashville, Tennessee, November 8, 1974; received by the editors November 7, 1977.

AMS (MOS) subject classifications (1970). Primary 02F47, 02E10; Secondary 08A15, 08A25.

[1]The author's research was supported in part by NSF grants MPS73-08531 A02 and MCS76-06986.

$a, b, c, \ldots$ with a defining relation $r(a, b, c, \ldots) = r'(a, b, c, \ldots)$ for every (r, r') in the dictionary.

Word problems arise naturally in the structure theory of algebras given by generators and relations. Groups are the obvious example. Similarly, in the development of a theory of nonassociative multiplicative systems given by generators and relations (Evans [8], [9]) word problems need to be solved. Whitman's solution of the word problem for free lattices [36] is an important tool in their study. The direct way to attack such problems is via *normal forms*, uniquely determined words which represent the equivalence classes of equal words (e.g. *reduced words* in free groups). This approach is common in many aspects of the structure theory of algebras and often great ingenuity is required in constructing such normal forms. There is an excellent account of this in P. Hall [18] and a comprehensive survey article by Bergman [1] describes numerous applications of a particular approach (the *Diamond Lemma*) to obtaining normal forms. A description of this aspect of the word problem is also given in Evans [12].

In one sense, a normal form theorem gives the most concrete and satisfying solution to a word problem. However, we want to look at algorithms and word problems from a different point of view. Are there purely algebraic properties which will allow us to construct an algorithm for solving the word problem? In §§2, 3 and 4 we give examples of such situations. If a finitely presented (f.p.) algebra has enough finite homomorphic images to enable any two elements to be finitely separated, then we can construct an algorithm for solving the word problem for that algebra. An embeddability property of partial algebras in a variety allows us to construct an algorithm for solving the word problem for f.p. algebras in the variety. A f.p. simple algebra has a solvable word problem. This last result is one aspect of a remarkable theorem for groups and semigroups recently proved by Boone and Higman [3] which would seem to be the first example of a purely algebraic property (being embeddable in a simple subgroup of a f.p. group) which is actually *equivalent* to the existence of an algorithm for solving the word problem. In §4 we explore some universal algebraic aspects of their theorem. For example, a finitely generated algebra has a solvable word problem if and only if it can be embedded in a finitely generated simple algebra whose defining relations are recursively enumerable.

The study of word problems for their own sake, rather than as a tool in the structure theory of algebras, is a consequence of the profound work of Church, Markov, Post, Turing and others on the meaning which should be attached to the intuitive notion of *algorithm*. Without a precise definition of *algorithm* it makes no sense to say that a decision problem is *unsolvable*, i.e. that an algorithm for solving the problem does not exist. No such dilemma exists if the problem is solvable–we simply produce the algorithm.

Post [33] in 1947 was the first to show the unsolvability of one of these algorithmic problems in algebra when he proved that the word problem for semigroups is unsolvable. Later Novikov [31] 1955, and Boone [2] 1959, showed that the word problem for groups is also unsolvable. Except for incidental remarks we will not deal with these deep results of unsolvability–as we remarked earlier, we are concerned with situations where the word

problem is solvable. Of course, word problems are only one example of decision problems in algebra. Dehn in 1911 also considered the *conjugacy problem* for groups, i.e. to decide whether two elements of a f.p. group are conjugate, and the *isomorphism problem*, i.e. to decide whether two f.p. groups are isomorphic.

Although we have already used the term *algorithm* frequently, we have not attempted to define it but have treated it as synonymous with the informal notion of *effective procedure* (given by some finite set of unambiguous instructions). The notion will be left informal throughout our discussion, i.e. we assume Church's thesis, that if pressed to do so, we could describe our algorithms in the formal language of Turing machines or recursive function theory. We will also use the term *recursively enumerable* informally. This describes a subset of the natural numbers which is the range of a *recursive* or *Turing-computable* function, i.e. a function for which we have an algorithm for calculating its values. We will equate *recursively enumerable subset* of an explicitly enumerated countable set (such as the set of all words in an algebra) with the informal notion of a subset for which we have an effective precedure for generating its elements.

1. Some algebraic preliminaries. We will work within a finitely *presented variety of algebras*. By an *algebra* $\mathcal{A} = (A, \Omega)$ we mean a nonempty set A and a finite set Ω of finitary operations f: $A^n \to A$, $n = 1, 2, 3, \ldots$, each n-ary operation being a mapping of A^n into A. Examples of algebras which we will use are (i) groupoids, having one binary operation $x \cdot y$, (ii) groups, having one binary operation $x \cdot y$ and one unary operation x^{-1}, (iii) rings, having two binary operations $x \cdot y$, $x + y$ and one unary operation $-x$, (iv) lattices having two binary operations $x \vee y$, $x \wedge y$, (v) quasigroups having three binary operations $x \cdot y$, $x \setminus y$, x/y. In the above examples, we have used the usual infix notation for the values of the operations. However, for a general algebra with an unspecified set of finitary operations, we will use ordinary functional notation and write $f(x_1, x_2, \ldots, x_n)$ for the value of the n-ary operation f at $(x_1, x_2, \ldots, x_n)$.

By a *variety* (or *equationally defined class*) of algebras $\mathbf{V}$, we mean the class of all algebras having some specified set of operations Ω and such that these operations satisfy some specified set of axioms, each of which is in the form of an *identity*, i.e. a universally quantified equation $u(x_1, x_2, x_3, \ldots) = v(x_1, x_2, x_3, \ldots)$ involving the operations and variables. An algebra $\mathcal{A} = (A, \Omega)$ is in $\mathbf{V}$ if the identities of $\mathbf{V}$ are satisfied by the operations and elements of $\mathcal{A}$. We will only concern ourselves with *finitely presented* varieties where the operations are finite in number and finitary in scope and where the defining identities are also finite in number. The reader may keep in mind, as examples, the varieties of groups, semigroups, abelian groups, rings, commutative rings, lattices, modular lattices, quasigroups, loops and groupoids.

In a variety $\mathbf{V}$ we can describe algebras in terms of generators $g_1, g_2, g_3, \ldots$ and relations $r_1 = r_1', r_2 = r_2', r_3 = r_3', \ldots$. In such a $\mathbf{V}$-algebra $\mathcal{A}$, an element is represented by an expression built up from $g_1, g_2, g_3, \ldots$ and the operations of $\mathbf{V}$, i.e. a *word* in the generators. The r_1, r_1' in the defining identities of $\mathcal{A}$ are words in the generators $g_1, g_2, g_3, \ldots$. The defining

identities of V are equations $u(x_1, x_2, x_3, \ldots) = v(x_1, x_2, x_3, \ldots)$. where the u, v are words in variables $x_1, x_2, x_3, \ldots$. The elements of $\mathcal{Q}$ are equivalence classes of words in the generators where two words $w(g_1, g_2, g_3, \ldots)$, $w'(g_1, g_2, g_3, \ldots)$ are equivalent if there is a finite sequence of substitutions (using the identities of V and the relations of $\mathcal{Q}$) which transforms w into w'.

As a simple example, consider the variety V of groupoids defined by the identities $x = x^2$ and $x \cdot xy = y$, for all x, y. Let $\mathcal{Q}$ be the V-algebra generated by a, b with defining relations $ba = ab \cdot b$. We have

$$\begin{aligned}(ab \cdot ba)(bb \cdot (b \cdot aa)) &\to (ab \cdot (ab \cdot b))(bb \cdot (b \cdot aa)) \\ &\to b(bb \cdot (b \cdot aa)) \to b(b \cdot (b \cdot aa)) \\ &\to b \cdot aa \to ba \to ab \cdot b.\end{aligned}$$

Hence, $(ab \cdot ba)(bb \cdot (b \cdot aa)) = ab \cdot b$ in $\mathcal{Q}$.

There is another way to approach equality of words in an algebra. If $\mathcal{G}$ is a group presented in terms of generators $g_1, g_2, g_3, \ldots$ and relations $r_1 = 1$, $r_2 = 1$, $r_3 = 1, \ldots$, we may regard $\mathcal{G}$ as the quotient of the free group $\mathcal{F}$ on $g_1, g_2, g_3, \ldots$ by the normal subgroup $\mathcal{N}$ generated by $r_1, r_2, r_3, \ldots$. Then $w = 1$ in $\mathcal{G}$ if w lies in this normal subgroup. This approach makes it clear that, for a f.p. group, we can actually describe an effective procedure for listing all equations $w = 1$ which hold in $\mathcal{G}$. In other words, the set of all words w such that $w = 1$ holds in $\mathcal{G}$ is a recursively enumerable subset of the set of all words in $\mathcal{F}$.

In general, let $\mathcal{Q}$ be a f.p. algebra in a variety V, with generators $g_1, g_2, g_3, \ldots$ and defining relations $r_1 = r_1'$, $r_2 = r_2'$, $r_3 = r_3', \ldots$. Let us denote by $\mathbf{V}^{\Phi}$ the variety of all algebras of the same operation type as V, i.e. having the same operations as V but defined by the empty set of identities. Let $\mathcal{F}$ be the free algebra in $\mathbf{V}^{\Phi}$ generated by $g_1, g_2, g_3, \ldots$. $\mathcal{Q}$ can be regarded as the quotient algebra $\mathcal{F}/\theta$ where θ is the congruence on $\mathcal{F}$ generated by all pairs (r_i, r_i') and all instances (u, v) of the defining identities of V (where arbitrary words in $g_1, g_2, g_3, \ldots$ replace the variables). We can give an effective procedure for generating θ. That is, there is an algorithm for listing all equations $w = w'$ which hold in $\mathcal{Q}$; the subset of all (w_i, w_i') such that $w_i = w_i'$ in $\mathcal{Q}$ is a recursively enumerable subset of the set of all pairs of words in $\mathcal{F}$.

The *word problem* for the algebra $\mathcal{Q}$ is the question of the existence of an algorithm for deciding whether $w = w'$ in $\mathcal{Q}$ for an arbitrary pair of words w, w' in the generators of $\mathcal{Q}$. The word problem is *solvable* for $\mathcal{Q}$ if there is such an algorithm, *unsolvable* otherwise.

We will use the following technique for solving the word problem several times. We have seen that we can effectively generate all equations which hold in the f.p. algebra $\mathcal{Q}$. Thus, if $w = w'$ in $\mathcal{Q}$, this equation will appear in this enumeration after a finite number of steps. Suppose that we have also some effective way of listing all inequations $w \neq w'$ which are true in $\mathcal{Q}$. If we combine these two procedures, enumerating the equations and the inequations, then for any pair of words w, w', after a finite number of steps either $w = w'$ or $w \neq w'$ will appear. Hence, we have an algorithm for solving the word problem for $\mathcal{Q}$. Of course, this is nothing more than the equivalence

of the properties of a subset S of the natural numbers (i) S and its complement S' are recursively enumerable, (ii) S is recursive (a subset is *recursive* if there is an algorithm for deciding whether a number belongs to it).

We will use in the last section the notion of a *recursively presented* algebra $\mathfrak{A}$. By this we mean that the generators are either finite or countably infinite (labelled by the natural numbers, say) and that the defining relations form a recursively enumerable set. We note that in a recursively presented algebra $\mathfrak{A}$ the set of all equations $w = w'$ holding in $\mathfrak{A}$ is also recursively enumerable.

To conclude this survey of basic ideas, we mention a number of other decision problems in the theory of varieties of algebras.

1. Let $\mathfrak{A}$ be a f.p. **V**-algebra. Is there an algorithm for deciding for an arbitrary element x in $\mathfrak{A}$ and f.g. subalgebra $\mathfrak{B}$, whether $x \in \mathfrak{B}$? This is called the *generalized word problem* for $\mathfrak{A}$.

2. Is there an algorithm for deciding whether two f.p. **V**-algebras are isomorphic? This is the *isomorphism problem* for **V**.

3. Is there an algorithm for deciding whether a f.p. **V**-algebra is free?

4. Is there an algorithm for deciding, for an n-generator free **V**-algebra, whether a set of n elements is a free generating set?

There are, of course, decision problems not involving algebras given by generators and relations which occur naturally in the context of varieties; e.g. can we decide whether two finite **V**-algebras satisfy the same identities? (solvable, Kalicki [**20**]); can we decide whether the identities of a finite **V**-algebra are finitely based? (unknown, even for the variety of groupoids); can we decide whether a finite **V**-algebra is equationally complete? (solvable, Scott [**34**]); can we decide whether a variety contains any nontrivial finite algebras? (unsolvable, McKenzie [**27**]).

2. Finite quotients and the word problem. Let $\mathfrak{A}$ be a f.p. algebra in a variety **V** such that, for any elements $x \neq y$ in $\mathfrak{A}$, there is a homomorphism α: $\mathfrak{A} \to \mathfrak{B}$ onto a finite algebra such that $x\alpha \neq y\alpha$ in $\mathfrak{B}$. In other words, any pair of distinct elements in $\mathfrak{A}$ can be "finitely separated." $\mathfrak{A}$ is then said to be *residually finite*. This property allows us to construct an algorithm for solving the word problem for $\mathfrak{A}$. (See Evans [**10**], although Malcev [**25**] was apparently the first to note this. Dyson [**5**] considered this procedure for the case of groups.)

THEOREM. *A f.p. residually finite algebra has a solvable word problem.*

PROOF. Let $\mathfrak{A}$ be a f.p. algebra in a f.p. variety **V** and let $u(g_1, g_2, g_3, \ldots)$, $v(g_1, g_2, \ldots, g_n)$ be two words in the generators of $\mathfrak{A}$. There is an effective enumeration of all equations $r(g_1, g_2, g_3, \ldots) = s(g_1, g_2, g_3, \ldots)$ which follow from the defining relations of $\mathfrak{A}$. For example, we may imagine this done by a machine M_1 which systematically lists all pairs of words (w, w') in the congruence on $F_n(\mathbf{V}^\Phi)$ which is generated by the defining identities of **V** and the defining relations of $\mathfrak{A}$. If $u = v$ holds in $\mathfrak{A}$, then this equation will eventually be produced by M_1.

Now assume that $\mathfrak{A}$ is residually finite. We may imagine a second machine M_2 which systematically constructs all finite algebras in **V** and computes for each one all homomorphisms of $\mathfrak{A}$ into it. If $u \neq v$ in $\mathfrak{A}$, then because of the

residual finiteness of $\mathcal{A}$, in one of these homomorphisms the images u and v will be distinct. Combining the two machines, we see that after a finite number of steps either machine M_1 stops because $u = v$ has appeared in its enumeration, or machine M_2 stops because it has found a finite homomorphic image of $\mathcal{A}$ which separates u and v. In any case, the algorithm stops after a finite number of steps, giving an answer to the question: is $u = v$ in $\mathcal{A}$?

Since f.p. abelian groups, commutative semigroups (Malcev [25]), commutative rings (Orzech and Ribes [32]), nilpotent groups (Gruenberg [14]), commutative Moufang loops (Evans [11]) are residually finite, these algebras all have solvable word problems. Also f.p. lattices, loops, quasigroups (and algebras in various subvarieties of the variety of quasigroups) are residually finite (Evans [10]) but solvability of the word problem for these algebras is more appropriately discussed in the context of embedding partial algebras (§3).

It is interesting to note that the above theorem fails (for groups) if *finitely presented* is replaced by *f.g. recursively presented.* Meskin [28] has given an example of such a group with an unsolvable word problem.

Residual finiteness is only one of a number of *finite separability* properties which implies positive solutions to various decision problems. Let $\mathbf{V}$ be a variety and π a property of subsets of $\mathbf{V}$-algebras, e.g. being finite, being a finitely generated subalgebra, etc. We say that an algebra $\mathcal{A}$ has the *finite separability property with respect to* π if for any x in $\mathcal{A}$ and π-subset S of $\mathcal{A}$ such that $x \notin S$, there is a homomorphism of $\mathcal{A}$ onto a finite algebra α: $\mathcal{A} \to \mathcal{A}\alpha$ such that $x\alpha \notin S\alpha$. In other words, x and S can be *finitely separated.* We say that $\mathbf{V}$ has the finite separability property with respect to π if every finitely presented algebra in $\mathbf{V}$ has the property. If π is the property of being finite, this reduces to *residual finiteness*. If π is the property of being a finitely generated subalgebra, this is usually called simply *finite separability*. If $\mathbf{V}$ is the variety of groups and π is "being a conjugacy class," the property is usually called *conjugacy separable.*

The proof that residual finiteness implies solvability of the word problem has the following generalization. Let π be a property of subsets of a f.p. algebra $\mathcal{A}$ such that any π-subset can be generated in some effective manner and let $\mathcal{A}$ be finitely separable with respect to the property π. Then there is an algorithm for deciding whether an element of $\mathcal{A}$ belongs to a π-subset of $\mathcal{A}$. As a special case, we have the following theorem.

THEOREM. *If a f.p. algebra has the finite separability property, then the algebra has a solvable generalized word problem.*

There are a number of algebras to which this theorem applies. In [17], M. Hall showed that if $\mathcal{F}$ is a f.g. free group, $\mathcal{K}$ any f.g. subgroup and x an element of $\mathcal{F}$ not in $\mathcal{K}$, then there is a subgroup $\mathcal{K}$ of finite index in $\mathcal{F}$ which does not contain x but which includes $\mathcal{K}$. Since $\mathcal{K}$ contains a normal subgroup of finite index it follows that f.g. free groups have the finite separability property. In [14], Gruenberg proved that f.g. nilpotent groups have this property (this is easy to show for f.g. abelian groups). Free semigroups have the finite separability property and other classes of semigroups with this property have been described by Golubov [15] and

Lesohin [23]. Rather surprisingly, free rings do not have the finite separability property. If $\mathfrak{F}$ is the free ring on one generator x, then in any homomorphism of $\mathfrak{F}$ onto a finite ring, the subring generated by $2x$ and $x + 2x^2$ maps onto the image of $\mathfrak{F}$. Since x does not belong to the subring, it follows that x and the subring cannot be finitely separated. (This example is due to K. Mandelberg.)

Using the property that any finite partial algebra can be embedded, one can show that f.p. loops, quasigroups, groupoids (and algebras in various subvarieties of these) have the finite separability property (Lindner and Evans [24]). In view of this, it is reasonable to conjecture that f.p. lattices have this property although this is not known even for free lattices.

It does not seem to be known whether the generalized word problem is solvable for free rings but it is easy to construct an example (based on the one for groups by Mihailova [29]) of the direct sum of two free rings which has an unsolvable generalized word problem. Let $\mathfrak{F}$ be the free ring on two generators x, y and let $\mathfrak{R} = \mathfrak{F} \oplus \mathfrak{F}$. Let $\mathbb{S} = \langle x, y; r_i = r_i', i = 1, 2, 3, \ldots \rangle$ be a f.p. semigroup on the generators x, y such that $\mathbb{S}$ has an unsolvable word problem and let $\mathbb{S}^*$ be the subring of $\mathfrak{R}$ generated by (x, x), (y, y) and (r_i, r_i'), $i = 1, 2, 3, \ldots$. Then, for any pair of words $u, v \in \mathbb{S}$, $(u, v) \in \mathbb{S}^*$ if and only if $u = v$ in $\mathbb{S}$. (We remark that the word problem is also unsolvable for f.p. rings–take the semigroup ring over Z of any semigroup with an unsolvable word problem.)

If $\mathfrak{F}$ is an n-generator free algebra in a variety $\mathbf{V}$ which is residually finite and has the finite separability property, then any set of n elements of $\mathfrak{F}$ which maps onto a free generating set in every homomorphism of $\mathfrak{F}$ onto a finite relatively free $\mathbf{V}$-algebra, is itself a free generating set for $\mathfrak{F}$ (Lindner and Evans [24]). By the same argument as before we can prove the following.

THEOREM. *Let $\mathfrak{F}$ be an n-generator free $\mathbf{V}$-algebra which is residually finite and has the finite separability property. Then there is an algorithm for deciding whether a set of n elements in $\mathfrak{F}$ is a free generating set.*

Groups and loops satisfy the hypotheses of this theorem. So do groupoids, semigroups, lattices, although in these cases, it is trivial to obtain the conclusion directly.

It would be interesting to know whether there is a test similar to that used in the above theorem for deciding whether a set of elements is part of a free generating set for a $\mathbf{V}$-free algebra $\mathfrak{F}$ and, in particular, if an element w of $\mathfrak{F}$ maps onto a primitive element in every homomorphism of $\mathfrak{F}$ onto a relatively free $\mathbf{V}$-algebra, what finite separability conditions are needed on $\mathfrak{F}$ to guarantee that w is then primitive in $\mathfrak{F}$.

We conclude this section by mentioning what seems to be a very difficult problem. Let $\mathbf{V}$ be a variety in which f.p. algebras are residually finite (guaranteeing that they have plenty of finite homomorphic images). Are there further properties of $\mathbf{V}$ which will imply that a f.p. $\mathbf{V}$-algebra is completely determined by its finite homomorphic images? I.e. given two nonisomorphic f.p. $\mathbf{V}$-algebras, there is some finite homomorphic image of one which is not a homomorphic image of the other. This is the case for abelian groups but at present this is the only known example. Such a property implies a positive

solution to the isomorphism problem for **V**. We conjecture that for varieties with the embeddability property discussed in the next section (every finite partial algebra can be finitely embedded), this property of being "finitely determined" holds.

3. Partial algebras and the word problem. Let **V** be a variety with operations Ω and let $\mathbf{V}^{\Phi}$ be the variety having the same set of operations Ω but defined by the empty set of identities. For example, if **V** is the variety of semigroups, then $\mathbf{V}^{\Phi}$ is the variety of groupoids. A *partial* $\mathbf{V}^{\Phi}$*-algebra* $\mathcal{P} = (P, \Omega)$ is a set of elements P in which each n-ary operation of Ω is defined on a subset of P^n. By a *partial* **V**-algebra $\mathcal{P}$ we mean a partial $\mathbf{V}^{\Phi}$-algebra (P, Ω) which satisfies the defining identities of **V**, insofar as they can be applied to the partial operations of $\mathcal{P}$. In Figure 1 (i) we show the table for a partial algebra in the variety of groupoids defined by the identities $x^2 = x$, $xy = yx$, and Figure 1 (ii) shows the tables for a partial lattice.

·	a	b	c
a	a		b
b		b	
c	b		c

(i)

∨	a	b	c	d
a	a		a	a
b		b		b
c	a		c	a
d	a	b	a	d

∧	a	b	c	d
a	a	d	c	d
b	d	b		d
c	c		c	
d	d	d		d

(ii)

FIGURE 1

An obvious question to ask for a variety **V** is whether a partial **V**-algebra can be completed to (embedded in) a **V**-algebra. By the *embeddability problem* for a variety **V**, we mean the problem of deciding, for an arbitrary finite partial **V**-algebra, whether or not it actually is part of some **V**-algebra, i.e. embeddable in a **V**-algebra. There is a close connection between this decision problem and the word problem (Evans [7]). In fact, they are equivalent.

THEOREM. *The embeddability problem is solvable for a variety* **V** *if and only if the word problem is solvable for* **V**.

The proof of this depends on two lemmas.

(i) *Given a f.p.* **V***-algebra* $\mathcal{Q}$ *and two words* u, v *in the generators, we can construct an isomorphic f.p. algebra* $\mathcal{B}$ *in which the generators and relations have the form of a partial* **V***-algebra and* u, v *correspond to generators of* $\mathcal{B}$ *in the isomorphism.*

(ii) *If* $\mathcal{P}$ *is a finite partial* **V***-algebra and we regard* $\mathcal{P}$ *as a presentation of a* **V***-algebra* $\langle \mathcal{P} \rangle$ *in terms of generators and relations then* $\mathcal{P}$ *can be embedded in a* **V***-algebra if and only if no two elements of* $\mathcal{P}$ *are equivalent in* $\langle \mathcal{P} \rangle$.

A useful feature of this theorem lies in the fact that for some varieties any partial **V**-algebra can be embedded. In particular, this is true for the varieties of lattices and loops (Evans [6]), and for many varieties of quasigroups and groupoids which correspond to combinatorial designs–the embedding of a partial algebra in one of these varieties corresponds to the completion of a partial design (Lindner and Evans [24]).

We describe briefly the algorithm for solving the word problem for a f.p. algebra in a variety with the property that any finite partial V-algebra can be embedded in a V-algebra. Let $\mathcal{A}$ be generated by $a_1, a_2, \ldots, a_m$ with defining relations $r_i = r_i'$, $i = 1, 2, \ldots, n$. Let w_1, w_2 be two words in the generators of $\mathcal{A}$. We wish to decide whether $w_1 = w_2$ in $\mathcal{A}$.

We begin by introducing new generators $b_1, b_2, b_3, \ldots$ for every word in the a_i which occurs as a subword of r_i, r_i', w_1 or w_2. This enables us to rewrite the defining relations of $\mathcal{A}$ so that each relation is either of the form $b_i = b_j$ or $f(b_i, b_j, b_k, \ldots) = b_t$ where f is an operation of $\mathcal{A}$.

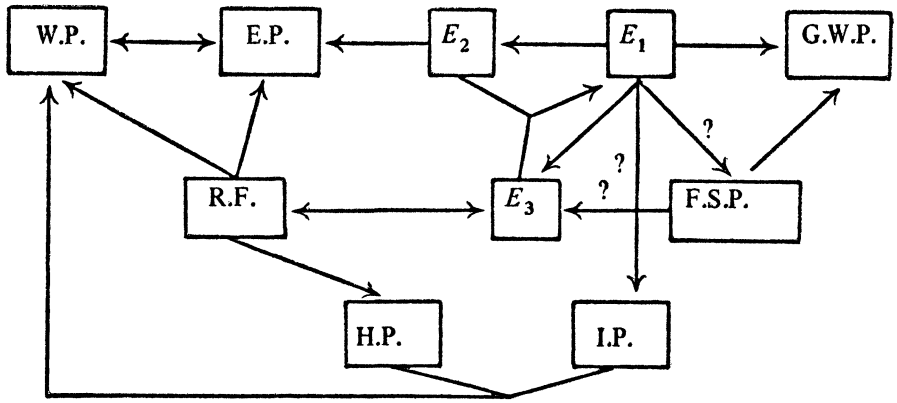
By applications of the identities of V and the defining relations of $\mathcal{A}$ we alternately remove redundant generators and introduce new relations of the form $f(b_i, b_j, b_k, \ldots) = b_t$. We arrive at a presentation for $\mathcal{A}$ which has the form of a partial V-algebra $\mathcal{P}$. In doing this, the b_i, b_j corresponding to w_1, w_2 may have been identified, in which case we know that $w_1 = w_2$ in $\mathcal{A}$. If, on the other hand, b_i, b_j remain distinct in $\mathcal{P}$, since $\mathcal{P}$ can be isomorphically embedded in a V-algebra, then $b_i \neq b_j$ in the V-algebra freely generated by $\mathcal{P}$ and so $w_1 \neq w_2$ in $\mathcal{A}$. A more detailed account of this procedure is given in [6].

In many varieties, unfortunately, it is not true that every finite partial V-algebra can be embedded and so this algorithm cannot be applied. Conditions on a variety V which imply embeddability of finite partial V-algebras have been studied by Gluhov and Gvaramija (e.g. [16]).

Are there varieties for which there is an algorithm for deciding embeddability so that we can approach the word problem this way? For example, perhaps one can show that in a variety V, if any finite partial V-algebra can be embedded, then necessarily it can be embedded in a finite V-algebra. (Call this the *finite embeddability property* for V.) This leads to an algorithm for deciding embeddability but unfortunately it is only a different version of one we already know (by virtue of the following theorem).

THEOREM (EVANS [10]). *A variety has the finite embeddability property if and only if every f.p.* V*-algebra is residually finite.*

Most varieties for which it is known that every finite partial algebra can be embedded have the further property of finite embeddability. The following table and chart summarize what is known about these properties for some standard varieties and illustrate the interconnections. We will use the abbreviations *W.P.* for "word problem solvable," *E.P.* for "embedding problem solvable," *G.W.P.* for "generalized word problem solvable," *F.S.P.* for "finite separability property," *R.F.* for "residual finiteness," *I.P.* for "isomorphism problem solvable" and *H.P.* for "hopfian property." In addition, E_1 will denote the property of a variety that every finite partial algebra is finitely embeddable, E_2 the property that every finite partial algebra is embeddable, and E_3 the finite embeddability property. Obviously, $E_1 \wedge E_2 \Leftrightarrow E_3$. Recall that an algebra is hopfian if it is not isomorphic to a proper quotient of itself. If the isomorphism problem is solvable for f.p. algebras in V and such algebras are hopfian, then we can decide whether an equation $w = w'$ holds in a V-algebra $\mathcal{A}$ by comparing for isomorphism $\mathcal{A}$ and $\mathcal{A} \cup \{w = w'\}$.



VARIETY	E_1	E_2	R. F.	W. P.	G. W. P.	F. S. P.	I. P.
			The first entry in each column refers to free V-algebras; the second to f. p. V-algebras.				
Groups	X	X	√, X	√, X	√, X	√, X	√, X
Rings	X	X	√, X	√, X	?, X	X, X	√, X
Abelian groups	X	X	√, √	√, √	√, √	√, √	√, √
Commutative rings	X	X	√, √	√, √	?, ?	X, X	√, ?
Semigroups	X	X	√, X	√, X	√, X	√, X	√, X
Commutative semigroups	X	X	√, √	√, √	√, √	√, √	√, ?
Lattices	√	√	√, √	√, √	?, ?	?, ?	√, ?
Modular lattices	X	X	?, X	?, X	?, X	?, X	√, ?
Loops, quasigroups Steiner quasigroups Totally symmetric quasigroups	√	√	√, √	√, √	√, √	√, √	√, √
Inverse property loops	X	√	?, ?	√, √	√, √	?, ?	√, √

4. The word problem and simple algebras. Boone and Higman [3] have recently proved the remarkable result 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. In one direction, the Boone-Higman theorem is a variation and mild extension of the universal-algebraic result that a finitely presented simple algebra has a solvable word problem (Kuznecov [21]; see also Malcev [26, p. 209]).

The Kuznecov theorem (for groups) goes as follows. Let G be a nontrivial f.p. simple group with generators $g_1, g_2, \ldots, g_n$ and let w be a word in the generators. Let $u_1 = 1, u_2 = 1, u_3 = 1, \ldots$ be some effective enumeration of the consequences of the defining relations of G. If $w = 1$ in G, then $w = 1$ will eventually appear in this enumeration. Let G^* be the group obtained from G by adding the extra defining relation $w = 1$. Let $v_1 = 1, v_2 = 1, v_3 = 1, \ldots$ be some effective enumeration of the consequences of the

defining relations of G^*. Since G is simple, if $w \neq 1$ in G, then G^* is trivial and so the equations $g_1 = 1, g_2 = 1, \ldots, g_n = 1$ will eventually appear in this second enumeration. We now perform these two enumerations alternately, step by step. Eventually, after a finite number of steps, either $w = 1$ will appear or all of $g_1 = 1, g_2 = 1, \ldots, g_n = 1$ will appear. The algorithm stops when one of these occurs.

Note that the above procedure describes an effective algorithm only when we know that the simple group is nontrivial. However, since a trivial group has a solvable word problem it is true that every f.p. simple group has a solvable word problem. In this theorem we may take G to be recursively rather than finitely related.

The universal algebra version of the easy part of the Boone-Higman theorem is as follows (Evans, Mandelberg and Neff [13]):

THEOREM. *Let $\mathfrak{A}$ be a subalgebra of a simple subalgebra $\mathfrak{K}$ of a recursively presented algebra $\mathfrak{K}$. Then $\mathfrak{A}$ has a solvable word problem.*

To prove the other half of the Boone-Higman theorem, the finitely generated group is first embedded in a recursively presented simple group which is then embedded in a finitely generated group and the concluding thrust of the proof is in the use of the deep result of Higman [19] that a finitely generated recursively related group can be embedded in a finitely presented group. A similar embedding result holds for semigroups (Murskii [30]) and using this Boone and Higman obtain the analogue for semigroups of their theorem for groups.

We outline the procedure used by Boone and Higman.

Let $\mathfrak{A} = (A, \Omega)$ be a V-algebra. We construct a V-algebra $\mathfrak{A}^+ = (A^+, \Omega)$ with the following properties.

(i) $\mathfrak{A}$ is a subalgebra of $\mathfrak{A}^+$,

(ii) if θ is any congruence on $\mathfrak{A}^+$ and there exists a pair of distinct elements a_1, a_2 in A satisfying $a_1 \equiv a_2\ (\theta)$, then $x \equiv y\ (\theta)$ for every pair of elements x, y, in A.

(iii) if $\mathfrak{A}$ is recursively presented and has a solvable word problem then $\mathfrak{A}^+$ is recursively presented and has a solvable word problem.

If we define $\mathfrak{A}_0 = \mathfrak{A}$, $\mathfrak{A}_{i+1} = (\mathfrak{A}_i)^+$, then the algebra $\mathfrak{K} = \bigcup_{i=0}^{\infty} \mathfrak{A}_i$ is simple and contains $\mathfrak{A}$.

It follows that $\mathfrak{K}$ will also be recursively presented and have a solvable word problem. Hence, for any variety **V** for which we can carry out the construction from $\mathfrak{A}$ to $\mathfrak{A}^+$ satisfying conditions (i), (ii), (iii) above, we have the following version of the Boone-Higman result.

I. A recursively presented V-algebra $\mathfrak{A}$ has a solvable word problem if and only if it can be embedded in a recursively presented simple V-algebra $\mathfrak{K}$.

If the variety **V** has the further property

(iv) any countable V-algebra can be effectively embedded in a finitely generated V-algebra,

then we have a rather closer approximation to the Boone-Higman theorem.

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

In Evans, Mandelberg, Neff [13] this version of the Boone-Higman result is given for lattices, rings of characteristic p, groupoids and loops. Of course such results miss the main flavour of the original result–algorithmic notions occur in both sides of the equivalence whereas the main impact of the Boone-Higman result is that a purely algorithmic property *solvability of the word problem* is shown to be equivalent to a purely algebraic property *embeddability in a simple subgroup of a f.p. group*.

One cannot expect a complete analogue of the Boone-Higman theorem for familiar varieties of algebras other than perhaps rings which are algebras over Z_p or Q. Although the word problem is solvable for f.p. abelian groups, commutative rings, and commutative semigroups, such algebras are not in general embeddable in simple algebras of the same type. Nor does embeddability of a ring in a simple ring have anything to do with whether it has a solvable word problem.

Even if this stage of the Boone-Higman theorem can be carried through and the algebra embedded in a recursively presented simple algebra, the analogue of the second stage, embedding in a finitely presented algebra, it is not possible in many cases, for example, groupoids, loops, lattices, commutative rings and semigroups, abelian groups, nilpotent groups, and commutative Moufang loops.

Our final theorem is an attempt at a Boone-Higman type theorem in universal algebra terms. However, it still retains the flaw that algorithmic notions appear on both sides of the equivalence. The main point of this theorem is that if we do not mind embedding in a recursively related algebra, then we may as well consider the whole problem in the context of varieties defined by the empty set of identities since an identity may be replaced by a recursive set of defining relations.

Now let $\mathbf{V}$ be an arbitrary f.p. variety and let $\mathbf{V}^\Phi$ be the variety of all algebras of the similarity type of $\mathbf{V}$.

THEOREM. *A finitely generated* $\mathbf{V}$*-algebra has a solvable word problem if and only if it can be embedded in a finitely generated simple* $\mathbf{V}^\Phi$*-algebra which is recursively related.*

To prove this we note that by the Kuznecov theorem a f.g. simple recursively related algebra has a solvable word problem and so we only have to prove that if $\mathcal{A}$ is a f.g. $\mathbf{V}$-algebra with a solvable word problem, then it can be embedded in f.g. recursively related simple $\mathbf{V}^\Phi$-algebra. We illustrate this for the case where $\mathbf{V}$ is a variety of groupoids i.e. having just one binary operation. Note that since $\mathcal{A}$ has a solvable word problem it has a recursively enumerable set of defining relations. We turn $\mathcal{A}$ into a $\mathbf{V}^\Phi$-algebra by adding to the defining relations of $\mathcal{A}$ all equations we get from the defining identities of $\mathbf{V}$ by substituting words in the generators of $\mathcal{A}$ for the variables. $\mathcal{A}$ is now a f.g. recursively related $\mathbf{V}^\Phi$-algebra.

We now construct an algebra $\mathcal{K}$ having the generators and relations of $\mathcal{A}$ as part of its presentation. $\mathcal{K}$ has the further generators $b_1, b_2, c_1, c_2, c_3, \ldots$ (disjoint from the generators of $\mathcal{A}$). Let $w_1, w_2, w_3, \ldots$ be some effective enumeration of all words in the generators of $\mathcal{A}$. To define $\mathcal{K}$ we add further relations to those for $\mathcal{A}$. Some of these such as $b_1^2 = w_1$, $b_2^2 = c_1$, $w_1 b_1 = b_2$,

$b_2c_i = c_{i+1}$, $b_1c_i = w_{i+1}$, $i = 1, 2, 3, \ldots$, guarantee that $\mathfrak{K}$ is generated by b_1. Others are chosen to ensure that $\mathfrak{K}$ is simple. Among these relations: $w_ic_j = b_1$ if $w_i = w_j$ in $\mathfrak{A}$, $w_ic_j = b_2$ if $w_i \neq w_j$ in $\mathfrak{A}$ for $i, j = 1, 2, 3, \ldots$. Since the word problem is solvable in $\mathfrak{A}$, the sets of (i, j) such that $w_i = w_j$ in $\mathfrak{A}$ and $w_i \neq w_j$ in $\mathfrak{A}$ are recursively enumerable and so the defining relations for $\mathfrak{K}$ form a recursively enumerable set.

The complete list of defining relations for $\mathfrak{A}$ is given below. For $i, j = 1, 2, 3, \ldots$,

$$b_1b_1 = w_1, \quad b_1b_2 = b_1, \quad c_1c_i = w_i, \quad b_1w_i = b_1,$$
$$b_2b_1 = b_1, \quad b_2b_2 = c_1, \quad b_2c_i = c_{i+1}, \quad b_2w_i = w_i,$$
$$c_ib_1 = c_ib_2 = c_ic_i = c_iw_j = b_1, \quad c_ic_j = b_2 \quad \text{if } i \neq j,$$
$$w_ib_1 = b_2, \quad w_ib_2 = b_1, \quad w_ic_j = \begin{cases} b_1 & \text{if } w_i = w_j \text{ in } \mathfrak{A}, \\ b_2 & \text{if } w_i \neq w_j \text{ in } \mathfrak{A}. \end{cases}$$

It follows that (i) $\mathfrak{K}$ is finitely generated, (ii) $\mathfrak{K}$ is simple, (iii) $\mathfrak{K}$ is recursively presented. It only remains to show that $\mathfrak{A}$ is isomorphically embedded in $\mathfrak{K}$. We do this by a normal form theorem solving the word problem for $\mathfrak{K}$ (relative to its solution for $\mathfrak{A}$) and showing that $w_i = w_j$ in $\mathfrak{K}$ if and only if $w_i = w_j$ in $\mathfrak{A}$.

Since this paper was prepared my attention has been drawn to an announcement by Kuznecov [22] in which he states that a finitely presented algebra $\mathfrak{A}$ has a solvable word problem if and only if $\mathfrak{A}$ can be embedded in a finitely presented simple algebra $\mathfrak{B}$ where "embedded" here means that the sets of elements of $\mathfrak{A}$, $\mathfrak{B}$ are the same but the set of operations of $\mathfrak{A}$ is a subset of the set of operations of $\mathfrak{B}$. Both $\mathfrak{A}$ and $\mathfrak{B}$ lie in finitely presented varieties. No details of the proof are given.

ADDED IN PROOF.

(i) The statement in the introduction that the Boone-Higman theorem is the first example of a purely algebraic property which is equivalent to solvability of the word problem should be modified. The equally interesting theorem that a group has a solvable word problem if and only if it is embeddable in every algebraically closed group is due to B. H. Neumann, *The isomorphism problem for algebraically closed groups*, in Word Problems (North-Holland, 1973) and A. Macintyre, *On algebraically closed groups*, Ann. of Math. **96** (1972), 53–97.

(ii) The theorem stated in §4 appears in *An algebra has a solvable word problem if and only if it is embeddable in a simple algebra*, Algebra Universalis (1978).

REFERENCES

1. G. Bergman, *The diamond lemma in ring theory*, Advances in Math. (to appear).
2. W. Boone, *The word problem*, Ann. of Math. (2) **70** (1959), 207–265.
3. W. Boone and G. Higman, *An algebraic characterization of groups with soluble word problem*, J. Austral. Math. Soc. (Hanna Neumann memorial volume) **2** (1974), 41–53.
4. M. Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Ann. **71** (1911), 116–144.
5. V. H. Dyson, *The word problem and residually finite groups*, Notices Amer. Math. Soc. **11** (1964), 743.
6. T. Evans, *The word problem for abstract algebras*, J. London Math. Soc. **26** (1951), 64–71.
7. _____, *Embeddability and the word problem*, J. London Math. Soc. **28** (1953), 76–80.

8. _____, *On multiplicative systems defined by generators and relations.*I, *Normal form theorems*, Proc. Cambridge Philos. Soc. **47** (1951), 637–649.

9. _____, *On multiplicative systems defined by generators, and relations.*II, *Monogenic loops*, Proc. Cambridge Philos. Soc. **49** (1953), 579–589.

10. _____, *Some connections between residual finiteness, finite embeddability and the word problem*, J. London Math. Soc. (2) **1** (1969), 399–403.

11. _____, *Identities and relations in commutative Moufang loops*, J. Algebra **31** (1974), 508–513.

12. _____, *Some solvable word problems*, Proc. Conf. on Decision Problems in Algebra (Oxford, July 1976), North-Holland, Amsterdam (to appear).

13. T. Evans, K. Mandelberg and M. F. Neff, *Embedding algebras with solvable word problems in simple algebras. Some Boone-Higman type theorems*, Proc. Logic Colloq. (Univ. of Bristol, July 1973), North-Holland, Amsterdam, 1975, 259–277.

14. K. W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc. (3) **7** (1957), 29–62.

15. E. A. Golubov, *Finite approximability, finite separability, and semi-group-theoretic constructions*, First All-Union Symposium on the Theory of Semigroups, 18–23, Ural Gos. Univ., Sverdlosk, 1969. (Russian)

16. M. M. Gluhov and A. A. Gvaramija, *A solution of the fundamental algorithmic problems in certain classes of quasigroups with identities*, Sibirsk. Mat. Z. **10** (1969), 297–317; English transl., Siberian Math. J. **10** (1969), 211–224.

17. M. Hall, Jr., *Coset representations in free groups*, Trans. Amer. Math. Soc. **67** (1949), 421–432.

18. P. Hall, *Some word problems*, J. London Math. Soc. **33** (1958), 482–496.

19. G. Higman, *Subgroups of finitely presented groups*, Proc. Roy. Soc. Edinburgh Sect. A262 (1961), 455–475.

20. J. Kalicki, *On comparison of finite algebras*, Proc. Amer. Math. Soc. **3** (1952), 36–40.

21. A. V. Kuznecov, *O problemah tozdestva i funkcionalnoi polnoty dlja algebraiceskin system*, in Trudy 3-go Vsesojuznono Mat. S″ezda, Vol. 2. (Dokl. Akad. Nauk SSSR, Moscow, 1956), 145–146.

22. _____, Uspehi Mat. Nauk., 3rd issue (1958), 240.

23. M. M. Lesohin, *Approximability of semigroups and separability of subsemigroups*, Interuniv. Sci. Sympos. General Algebra, Tartu Gos. Univ., Tartu, 1966, 52–62. (Russian)

24. C. C. Lindner and T. Evans, *Finite embedding theorems for partial designs and algebras*,Coll. Sem. de Math. Superieures, Univ. of Montreal Press, Montreal, 1977.

25. A. I. Malcev, *On homomorphisms onto finite groups*, Učen Zap. Ivanovsk Ped. Inst. **18** (1958), 49–60.

26. _____, *The metamathematics of algebraic systems*, Studies in Logic, North-Holland, Amsterdam, 1971.

27. R. McKenzie, *On spectra and the negative solution of the decision problem for identities having a finite non-trivial model*, J. Symbolic Logic **40** (1975), 186–196.

28. S. Meskin, *A finitely generated residually finite group with an unsolvable word problem*, Proc. Amer. Math. Soc. **43** (1974), 8–10.

29. K. A. Mihailova, *The occurrence problem for direct products of groups*, Dokl. Akad. Nauk SSSR **119** (1958), 1103–1105. (Russian)

30. V. L. Murskii, *Isomorphic embedding of a semi-group with an enumerable set of defining relations in a finitely presented semi-group*, Mat. Zametki **1** (1967), 217–224.

31. P. S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov, **44** (1955); English transl., Amer. Math. Soc. Transl. (2) **9** (1958), 1–122.

32. M. Orzech and L. Ribes, *Residual finiteness and the Hopf property in rings*, J. Algebra **15** (1970), 81–88.

33. E. L. Post, *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic **12** (1947), 1–11.

34. D. Scott, *Equationally complete extensions of finite algebras*, Indag. Math. **18** (1956), 35–38.

35. A Thue, *Probleme über Veranderungen von Zeichenreihen nach gegebenen Reglen*, Skr. Vid. Kristiana I. **10** (1914).

36. P. Whitman, *Free lattices*, Ann. of Math. (2) **42** (1941), 325–329.

DEPARTMENT OF MATHEMATICS, EMORY UNIVERSITY, ATLANTA, GEORGIA 30322