EMBEDDING THEOREMS FOR MULTIPLICATIVE SYSTEMS AND PROJECTIVE GEOMETRIES

TREVOR EVANS

Introduction. It has been shown in a recent paper (see [5]) that any countable group can be embedded in a group generated by two elements. We show here that any countable loop (quasigroup, groupoid) can be embedded in a loop (quasigroup, groupoid) generated by one element, any countable semigroup can be embedded in a semigroup generated by two elements, and any countable projective plane can be embedded in a projective plane generated by four points. No such embedding theorem exists for some systems, such as abelian groups, and some light is thrown on the general problem by the following theorem. Let $\mathfrak{A}$ be a class of algebras, (E_1) the property that there is a number m such that any countable $\mathfrak{A}$-algebra can be embedded in an $\mathfrak{A}$-algebra generated by m elements, (E_2) the property that there is a number n such that the free $\mathfrak{A}$-algebra on n generators contains a free subalgebra on a countable number of generators. Then if $\mathfrak{A}$ has property (E_1), it has also property (E_2) and $n \leqq m$.

1. **The embedding of loops.**[1] Let L be a countable loop with unit e and generated by $g_1, g_2, g_3, \cdots$. Denote by I the incomplete loop consisting of all elements of L and elements $a_1, a_2, a_3, \cdots$, the operations defined in I being those already defined in L together with the following:[2]

(i) $\quad e \cdot a_i = a_i \cdot e = a_i \qquad$ for $i = 1, 2, 3, \cdots$,

(ii) $\quad a_1 \cdot a_i = g_i \qquad$ for $i = 1, 2, 3, \cdots$,

(iii) $\quad a_1 \cdot g_i = a_{i+1} \qquad$ for $i = 1, 2, 3, \cdots$.

If L has k generators, we need only add elements $a_1, a_2, a_3, \cdots, a_k$ to L in constructing I, the operations being defined as before.

We now embed I in a loop G which is freely generated by I [2, Theorem 3.1; 3, Theorem 2.4]. It is obvious from the construction that G contains L and is generated by a_1.

THEOREM I. *Any countable loop can be embedded in a loop generated by one element.*

Presented to the Society, December 28, 1951; received by the editors December 18, 1951.

[1] See [2; 3], for definitions of the terms used in this section.

[2] Strictly speaking, for this to be an incomplete loop in the sense of [3] we should add the two operations (/) and (\). However, this makes no essential difference.

The above construction can be interpreted in a different way. Let F be the free loop generated by a with unit element e. Let K be the subloop of F generated by the free set of generators a^2, $a\cdot(a\cdot a^2)$, $a\cdot(a\cdot(a\cdot a^2)))$, $\cdots$.[3] Denote these generators by $w_1, w_2, w_3, \cdots$ and let $w_i \leftrightarrow g_i$ be a one-one correspondence between the generators of K and the generators of L. If we denote the defining relations of L by

$$r_i(g_1, g_2, g_3, \cdots) = e, \qquad i = 1, 2, 3, \cdots,$$

then the loop G constructed above is isomorphic to the factor loop of F defined by the relations

$$r_i(w_1, w_2, w_3, \cdots) = e, \qquad i = 1, 2, 3, \cdots.$$

To prove this we need only note that in G, $g_1 = a_1^2$, $g_2 = a_1\cdot(a_1\cdot a_1^2)$, $g_3 = a_1\cdot(a_1\cdot(a_1\cdot a_1^2)))$, $\cdots$ and that G is generated by $g_1, g_2, g_3, \cdots$ subject only to the relations

$$r_i(g_1, g_2, g_3, \cdots) = e, \qquad i = 1, 2, 3, \cdots.$$

It follows that if L is defined by n relations, it can be embedded in a one generator loop defined by n relations.

The subloop K of F has the following property. Let $\mathfrak{R}$ be a set of relations in K. Then, considering $\mathfrak{R}$ as relations in F, the set of all relations which follow from $\mathfrak{R}$ does not contain any in K which do not follow from $\mathfrak{R}$ by considering $\mathfrak{R}$ as relations in K only. More precisely, let N be a normal subloop of K and let N^F be the minimal normal subloop of F containing N. Then, by the same proof as [5, Theorem V], $N = K \cap N^F$.[4] In contrast to the situation for groups, however, any subloop of F can play the role of K in the above construction. We shall not pursue this point here but we discuss briefly, in the next section, the corresponding situation for semigroups.

The proof of Theorem I can be easily adapted, using the results of [3], to give the following theorem.

THEOREM IA. *Any countable quasigroup (groupoid, groupoid with unique division on one side) can be embedded in a quasigroup (groupoid, groupoid with unique division on one side) generated by one element.*

2. **The embedding of semigroups.** Let S be a countable semigroup generated by $g_1, g_2, g_3, \cdots$ with defining relations

(i) $$r_i(g_1, g_2, g_3, \cdots) = r_i'(g_1, g_2, g_3, \cdots), \qquad i = 1, 2, 3, \cdots.$$

Let w be a word in the generators of the form upv where u, v are

[3] See [2, p. 539] and [3, p. 647].

[4] The homomorphism theorems needed in the proof of this can be found in [1].

words, possibly empty,[5] and $p=q$ is one of the defining relations. Then the replacing of w by uqv is called an elementary transformation of the word w. Two words are equivalent if we can transform one into the other by a finite sequence of elementary transformations. The equivalence classes of words so defined are the actual elements of the semigroup.

Let F be the free semigroup generated by a, b and let K be the subsemigroup generated by bab, ba^2b, ba^3b, $\cdots$, where the ba^ib are in one-one correspondence $g_i \leftrightarrow ba^ib$ with the generators of S. This defines a one-one correspondence between the words of S and the words of K. The subsemigroup K has the following property.

LEMMA 2.1. *Let x, y be words in K and let $x=uyv$ where u, v are words in F. Then u, v belong to K.*

PROOF. Any word in K is of the form $ba^ibba^jb \cdots ba^mbba^nb$, that is, it begins and ends with b and in between we have alternately some power of a and b^2. This remark is sufficient to prove the lemma.

We now construct a semigroup G by imposing on F the relations

$$r_i(bab, ba^2b, ba^3b, \cdots) = r_i'(bab, ba^2b, ba^3b, \cdots), \quad i = 1, 2, 3, \cdots, \tag{ii}$$

corresponding to the relations (i) defining S. This introduces an equivalence relation between the words of F.

LEMMA 2.2. *If w is a word in K, then any word equivalent to w is also in K.*

PROOF. We note, first of all, that in the defining relations (ii) above both sides are words in K. Let $w=upv$, where $p=q$ is one of the relations (ii). By Lemma 2.1 the words u, v are in K. The effect of an elementary transformation on w is to replace it by uqv and this is in K. Any word equivalent to w is obtained by a sequence of such transformations.

Let us denote by w' the word in K corresponding to w in S under the mapping $g_i \leftrightarrow ba^ib$. We have the following lemma.

LEMMA 2.3. *Let u, v be two words in S. Then u', v' are equivalent in G if, and only if, u, v are equivalent in S.*

PROOF. We note, first of all, that to each defining relation $p=q$ of S there corresponds a defining relation $p'=q'$ of G and conversely.

(1) Let u, v be connected by one elementary transformation so

[5] That is, either one or both of the words u, v may be absent. We do not include the empty word among the words of S.

that $u=xpy$, $v=xqy$, where x, y are words in S and $p=q$ is a defining relation of S. Then, necessarily, $u'=x'p'y'$, $v'=x'q'y'$, and so u', v' are connected by one elementary transformation in G. A simple induction on the number of elementary transformations connecting u and v shows that if u, v are equivalent in S, then u', v' are equivalent in G.

(2) Let u', v' be connected by one elementary transformation in G so that $u'=sp't$, $v'=sq't$, where s, t are words in F and $p'=q'$ is one of the defining relations of G. Now u', p' are in K and so by Lemma 2.1 the words s, t are in K. Hence we can denote s, t by x', y' where x, y are words in S. Then $u=xpy$, $v=xqy$, where $p=q$ is one of the defining relations of S and so u, v are connected by one elementary transformation in S. A simple induction completes the proof of the lemma.

By the preceding lemmas we have a one-one correspondence $\{w\} \leftrightarrow \{w'\}$ between the equivalence classes $\{w\}$ of words in S and the equivalence classes $\{w'\}$ of G consisting of words in K. Since $(uv)' = u'v'$ this correspondence is an isomorphism between S and the subsemigroup of G generated by bab, ba^2b, ba^3b, $\cdots$.

THEOREM II. *Any countable semigroup can be embedded in a semigroup generated by two elements.*

It is of some interest to determine which subsemigroups of F can play the role of K in the above construction. First of all, such a subsemigroup must possess a free set of generators. For example, the subsemigroup of F generated by ab, aba, bab already has the relation $(aba)(bab)=(ab)^3$ between its generators. However, this condition is not sufficient as we see if we attempt to carry through the construction used in Theorem II for the case when S is the semigroup generated by g_1, g_2, g_3 with the defining relation $g_1g_2=g_2g_1$ and K is generated by the free set of generators ab, ab^2, ab^3. From the relation $(ab)(ab^2)=(ab^2)(ab)$ in F we can deduce the further relation $(ab)(ab^3) = (ab^2)^2$ which is a relation in K. We cannot deduce this relation inside K however, since it corresponds to the relation $g_1g_3=g_2^2$ in S and this does not follow from the original defining relation of S. However, an examination of the proof of Theorem II shows that, in addition to the freeness of K, we use only that property of K stated in Lemma 2.1. It is also true that this property of K is necessary.

COROLLARY TO THEOREM II. *Necessary and sufficient conditions that a subsemigroup of F can play the role of K in the proof of Theorem* II *are* (i) *it possesses a free set of generators*, (ii) *it possesses that property of K stated in Lemma* 2.1.

PROOF. It can easily be verified that we use only these properties of K to prove Theorem II and so the sufficiency of the conditions is shown. To show the necessity of the conditions we observe first of all that K must be free since any relation between the generators of K would imply that a similar relation holds between the generators of S.

Now let K be such that there are words u, v in F, u in K, v not in K, and uv a word in K. Thus K does not satisfy condition (ii) above. Let S have the single defining relation $r^2=r$, where r is the word in S corresponding to u in the one-one correspondence between the words of S and the words of K. The relations in S implied by this defining relation are all of the form $w_1r^iw_2r^iw_3\cdots=w_1r^mw_2r^nw_3\cdots$ where the w's are words in S, with possibly the first and last absent. But the relation $u^2=u$ in K, considered as a relation in F, implies the further relation $u(uv)=uv$ in K and this does not correspond to any of the relations in S. Hence K, with the relation $u^2=u$ added, is not isomorphic to S. This completes the proof.

3. The embedding of projective planes.[6] Let π_0 be the partial plane consisting of the four points P, Q, A_0, B_0 and the two lines l, m where P, Q lie on l and P, A_0 on m. We construct a sequence of partial planes π_1, π_2, π_3, $\cdots$ as follows: π_i is obtained from π_{i-1} by adding points A_i, B_i, C_i, D_i, E_i, F_i, G_i and lines $PB_{i-1}B_iE_i$; $QA_{i-1}E_iF_i$; $A_{i-1}B_{i-1}D_i$, D_i being on l; $QB_{i-1}C_i$, C_i being on m; $B_iC_iD_iF_i$; $C_iE_iG_i$, G_i being on l; $A_iD_iE_i$, A_i being on m. Denote by π' the union of all the π_i. This partial plane is a subset of the free projective plane π^4 generated by the four points P, Q, A_0, B_0.

Let π be the projective plane we wish to embed. π can be generated by one of its lines n, all points X_1, X_2, X_3, $\cdots$ on n, and two points U, V not on n. We now form the partial plane π'' consisting of all points and lines in π' and π with the line l identified with the line n and G_i identified with X_i for all i. We can do this without any other forced identifications between the points and lines of π' and the points and lines of π. By adding lines F_1F_2U; F_3F_4U; F_5F_6V; F_7F_8V we form a partial extension π''' of π''. Now π''' is generated by P, Q, A_0, B_0 and so, by taking the free extension of π''' to a complete projective plane,[7] we have obtained the required embedding.

THEOREM III *Any countable projective plane can be embedded in a projective plane generated by four points.*

It should be noted that the same interpretation can be given to this construction as in the preceding sections. That is, we have

[6] See [4] for definitions of the terms used in this section.

[7] See [4, p. 234].

added relations to a subplane of π^4 to make it isomorphic to the plane we wish to embed. In the free plane generated by P, Q, A_0, B_0 the subplane used is generated by G_1, G_2, G_3, $\cdots$ and the two points which are the intersections of, respectively, the lines F_1F_2, F_3F_4 and the lines F_5F_6, F_7F_8.

4. **The general problem.** Let $\mathfrak{A}$ be a class of algebras. For convenience we shall assume that $\mathfrak{A}$ is defined by a finite number of finitary operations, in a given $\mathfrak{A}$-algebra each n-ary operation being defined for all ordered sequences of n elements, and that each axiom of $\mathfrak{A}$ states that every $\mathfrak{A}$-algebra satisfies a certain identical relation. We shall denote by (E_1) and (E_2) those properties of $\mathfrak{A}$ defined in the introduction.

THEOREM IV. *If a class* $\mathfrak{A}$ *has property* (E_1), *it has also property* (E_2) *and* $n \leqq m$.

PROOF. If $\mathfrak{A}$ has property (E_1), there is an $\mathfrak{A}$-algebra A, generated by m elements $g_1, g_2, g_3, \cdots, g_m$, containing a subalgebra H which is a free $\mathfrak{A}$-algebra on a countable number of generators. Denote by $w_i(g_1, g_2, g_3, \cdots)$, $i = 1, 2, 3, \cdots$, the generators of this subalgebra. Let F be the free $\mathfrak{A}$-algebra on m generators, $a_1, a_2, a_3, \cdots, a_m$, and let K be the subalgebra of F generated by $w_i(a_1, a_2, a_3, \cdots)$. In the homomorphism of F onto A determined by $a_i \to g_i$, K is mapped onto H. Since H is free, there is a homomorphism $w_i(g_1, g_2, g_3, \cdots) \to w_i(a_1, a_2, a_3, \cdots)$ of H onto K and the product both ways of these two homomorphisms is the identity mapping. Hence H and K are isomorphic. Alternatively, we can see that there cannot be any relations between the generators of K since these relations would necessarily be preserved in the homomorphism of F onto A, implying relations between the generators of H.

Since the free abelian group on m generators has, as subgroups, only free abelian groups on m or fewer generators, we cannot expect an embedding theorem for abelian groups of the type considered here. This, of course, can also be deduced from the basis theorem for abelian groups.

In all the cases considered here, $m = n$. This is true, also, for groups and linear nonassociative algebras.[8] It would be interesting to know

[8] It is shown in [6] that a nonassociative linear algebra of countable dimension can be embedded in a nonassociative linear algebra generated by one element. Since the ring of $n \times n$ matrices over a field can be generated by two matrices, any associative linear algebra of finite dimension can be embedded in an associative linear algebra generated by two elements. However, the discussion in this section does not apply to linear algebras or projective geometries, although by enlarging our definition of an algebra we could probably obtain corresponding results.

whether it is possible to have $m > n$, or whether, if there is an embedding theorem at all, necessarily $m = n$.

ADDED IN PROOF. It will be seen that we have not, in fact, proved the necessity of condition (ii) in the corollary to Theorem II, but only the necessity of a weaker condition. We do not know at present whether condition (ii) is necessary.

We take this opportunity to point out that the proof of Theorem II uses methods closely related to those in Marshall Hall, Jr., *The word problem for semigroups with two generators*, J. Symbolic Logic vol. 14 (1949) pp. 115–118.

BIBLIOGRAPHY

1. Reinhold Baer, *The homomorphism theorems for loops*, Amer. J. Math. vol. 67 (1945) pp. 450–460.

2. Grace E. Bates, *Free loops and nets and their generalizations*, Amer. J. Math. vol. 69 (1947) pp. 499–550.

3. Trevor Evans, *On multiplicative systems defined by generators and relations. I. Normal form theorems*, Proc. Cambridge Philos. Soc. vol. 47 (1951) pp. 637–649.

4. Marshall Hall, *Projective planes*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 229–277.

5. Graham Higman, B. H. Neumann, and Hanna Neumann, *Embedding theorems for groups*, J. London Math. Soc. vol. 24 (1949) pp. 247–254.

6. A. I. Zukov, *Reduced systems of defining relations in non-associative algebras*, Mat. Sbornik. N.S. vol. 27 (1950) pp. 267–280.

THE UNIVERSITY OF WISCONSIN AND
EMORY UNIVERSITY