Math. Proc. Camb. Phil. Soc. (1978), **84**, 11
Printed in Great Britain

The word problem for semigroups satisfying $x^3 = x$

By J. A. GERHARD
University of Manitoba, Winnipeg

(*Received* 7 *January* 1977, *revised* 25 *November* 1977)

In the paper (4) of Green and Rees it was established that the finiteness of finitely generated semigroups satisfying $x^r = x$ is equivalent to the finiteness of finitely generated groups satisfying $x^{r-1} = 1$ (Burnside's Problem). A group satisfying $x^2 = 1$ is abelian and if it is generated by n elements, it has at most 2^n elements. The free finitely generated semigroups satisfying $x^3 = x$ are thus established to be finite, and in fact the connexion with the corresponding problem for groups can be used to give an upper bound on the size of these semigroups. This is a long way from an algorithm for a solution of the word problem however, and providing such an algorithm is the purpose of the present paper. The case $x = x^3$ is of interest since the corresponding result for $x = x^2$ was done by Green and Rees (4) and independently by McLean (6).

Section I is an introductory section to establish the notation and provide background for the rest of the paper. The solution of the word problem is an inductive one and section II provides a detailed description of the inductive assumptions. In addition, invariants are introduced which are used to establish which words are distinct. In section III, a notion of minimality is introduced so that every word is a product of minimal ones. In section IV, the algorithm is described by showing which products of minimal words yield the same element of the free semigroup satisfying $x = x^3$. Finally, in section V, we describe the solution for the two variable case and count the number of distinct words in three variables. The counting could be carried out for four or more variables in a similar way.

I. *Notation and preliminary results*

Throughout this paper, X is a fixed countable set and $F(X)$ is the free semigroup generated by X. The elements of $F(X)$ are called *words*. It will sometimes be convenient to be able to consider the 'empty' word and this is done by letting $F'(X)$ be the free monoid on X. The identity element of $F'(X)$ is denoted by ϕ. Thus $F'(X) = F(X) \cup \{\phi\}$.

An *equation* is a pair (f, g) of elements of $F(X)$. As usual an equation is written $(f = g)$. The equation $(f = g)$ *holds* in S (or S *satisfies* $(f = g)$) if, for every homomorphism $\varphi: F(X) \to S$, $\varphi(f) = \varphi(g)$.

Let $x \in X$. This paper deals with semigroups in which $(x = x^3)$ holds. (Note that this is equivalent to assuming that $f = f^3$ holds for every $f \in F(X)$.) Let $F_3(X)$ be the free semigroup satisfying $x = x^3$ and generated by X. Let $\kappa: F(X) \to F_3(X)$ be obtained by extending the identity mapping on X. The equation $(f = g)$ holds in every semigroup satisfying $(x = x^3)$ if and only if $\kappa(f) = \kappa(g)$. If $\kappa(f) = \kappa(g)$, we write $f \approx g$. To solve the word problem for the free semigroup satisfying $x = x^3$ is to give an algorithm to decide

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

when $f \approx g$ holds for $f, g \in F(X)$. The relation $\approx$ is a congruence relation and the congruence class of $F(X)$ defined by f is denoted by $[f]$.

Much of the following notation occurs in (3) and the reader is referred to that paper if more details are required. Some of the notation is also given in (5). Let

$$f = x_1 \dots x_n \in F(X),$$

where the x_i $(i = 1, \dots, n)$ are (not necessarily distinct) elements of X.

$$L(f) = n, \text{ the } \textit{length} \text{ of } f.$$

$$E(f) = \{x_1, \dots, x_n\}, \text{ the } \textit{set of variables} \text{ of } f.$$

By assumption, $E(f) = \phi$ and $f = \phi$ are equivalent and so our double usage of ϕ should cause no confusion.

$$\bar{I}(f) = x_1 \dots x_j,$$

where $E(x_1 \dots x_j) = E(f)$ and $E(x_1 \dots x_{j-1}) \neq E(f)$. Thus $\bar{I}(f)$ is the shortest initial segment of f which contains all the variables of f.

For the j defined above, let

$$\bar{f}(0) = x_j$$

$$f(0) = \begin{cases} x_1 \dots x_{j-1} & \text{if } j > 1, \\ \phi & \text{if } j = 1. \end{cases}$$

Thus $\bar{I}(f) = f(0)\bar{f}(0)$. By induction for all $k \geqslant 1$, let

$$\bar{f}(0^k) = \begin{cases} \overline{f(0^{k-1})}\,(0) & \text{if } f(0^{k-1}) \neq \phi, \\ \phi & \text{if } f(0^{k-1}) = \phi; \end{cases}$$

$$f(0^k) = \begin{cases} f(0^{k-1})\,(0) & \text{if } f(0^{k-1}) \neq \phi, \\ \phi & \text{if } f(0^{k-1}) = \phi. \end{cases}$$

If $|E(f)| - k \geqslant 1$, then $f(0^k)\bar{f}(0^k)$ is the shortest initial segment of f which contains the first $|E(f)| - k + 1$ variables that occur in f, $\bar{f}(0^k) \notin E(f(0^k))$, and $|E(f(0^k))| = |E(f)| - k$.

If $f = x_1 x_2 \dots x_n$, the *dual* of f is f^* defined by $f^* = x_n \dots x_2 x_1$. The dual of a definition or result about words is just the original statement made for the duals of these words. Duality is often used to shorten results, and sometimes without explicit mention. Again more detail is available in (3).

$\{a_1, \dots, a_n\}$ is a fixed set of n distinct elements of X.

$\mathbf{a} = a_1 a_2 \dots a_n$.

Thus $E(\mathbf{a}) = \{a_1, \dots, a_n\}$ and $|E(\mathbf{a})| = n$.

$$S_n = \{f \mid E(f) \subseteq E(\mathbf{a})\}.$$

A *subword* of f is a word v such that $f = pvq$ for some $p, q \in F'(X)$. The subword is *proper* if $p \neq \phi$ or $q \neq \phi$. A *maximal* subword of f with respect to some property P is a subword v of f which has property P and is such that if v is a proper subword of u and u

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

is a subword of f then u does not have property P. For example, v is a maximal subword of f in n variables if $|E(v)| = n$ and $f = pvq$, and if $p = p_1 x$ for some $x \in X$ then $|E(xv)| = n+1$, and if $q = yq_1$ for some $y \in X$ then $|E(vy)| = n+1$.

The next three lemmas can be found in Green and Rees(4).

LEMMA 1·1. *If* $f \approx g$ *then* $E(f) = E(g)$.

LEMMA 1·2. *Let* $E(f) = E(\mathbf{a})$. *Then* $fS_n f/\approx$ *is a group. The identity element is* $[ff]$ *and for each* $u \in S_n$, $(fuf)^2 \approx ff$.

LEMMA 1·3. *If* $f \approx g$ *then* $\bar{f}(0) = \bar{g}(0), f(0) \approx g(0)$ *and their duals hold.*

The following corollary of Lemma 1·3 follows immediately by induction.

COROLLARY 1·4. *If* $f \approx g$, *then, for all* $k \geqslant 1, \bar{f}(0^k) = \bar{g}(0^k), f(0^k) \approx g(0^k)$ *and their duals hold.*

A proof of Lemma 1·2 appears in Brown(1) where he also establishes the following:

LEMMA 1·5 (Brown(1)). *Let* $u \in S_n$ *and* $E(f) = E(\mathbf{a})$. *Then* $f \approx fufuf$.

Since in $fS_n f/\approx$ every element is its own inverse, it follows that the group is commutative. This makes the following corollaries easy to check.

COROLLARY 1·6. *Let* $u \in S_n$ *and* $E(f) = E(\mathbf{a})$. *Then* $ffuf \approx fuff$.

COROLLARY 1·7. *Let* $u, v \in S_n$ *and* $E(f) = E(\mathbf{a})$. *Then* $fufvf \approx fvfuf$.

LEMMA 1·8 (Green and Rees(4)). *Let* $E(f) = E(g) = E(f') = E(g') = E(\mathbf{a})$. *Then there is a one–one correspondence between* $fS_n g/\approx$ *and* $f'S_n g'/\approx$.

In fact the correspondence can be given by mapping fug to $f'fugg'$ for each $u \in S_n$. As stated in Green and Rees the groups are isomorphic but this is not needed here.

As a consequence of Lemmas 1·1, 1·3 and 1·8, we can solve the word problem by studying the group

$$G_n = \mathbf{a}S_n\mathbf{a}/\approx.$$

II. *Invariants*

The solution of the word problem given here is an inductive one. We assume, for a given n, that the solution of the word problem for words in less than n variables has been obtained. The induction is started by noting that, for words in the single variable x, $x^k \approx x$ if k is odd and $x^k \approx x^2$ if k is even.

We actually require a somewhat more detailed assumption. Of course certain words in n or more variables can be shown to be congruent on the basis of the solution for words in less than n variables and in this way we may be able to write words in n or more variables in a particular form. In fact what we are going to show is that every word in n or more variables can be written in such a way that if u and v are two maximal subwords in less than n variables of any words, and if $u \approx v$, then $u = v$.

To do this, assume by induction that every word can be written in such a way that

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

whenever two maximal subwords in fewer than $n-1$ variables appear that are congruent, they are in fact equal. (For $n = 2$, the assumption simply means that each word is written as itself.) Using the solution of the word problem in $n-1$ variables, we can select for each congruence class a fixed representative from among the words with this property. (For $n = 2$ select x and x^2.) The final step is to show that we can replace every maximal subword in $n-1$ variables by its fixed representative. If two such maximal subwords f and g overlap (so that replacing f by f_1, say, affects g) then they overlap in a subword w which is maximal in fewer than $n-1$ variables. This subword occurs at the beginning or end of f and g. If it appears at the beginning of f, say, then $w = f(0^k)$ for some $k \geqslant 1$. Since $f \approx f_1$ it follows by Corollary 1·4 that $f(0^k) \approx f_1(0^k)$ and so by assumption $f(0^k) = f_1(0^k)$. Thus replacing f by f_1 does not affect the overlapping part. It follows that each maximal subword in $n-1$ variables can be replaced by its fixed representative.

Throughout the rest of the paper, n is fixed and as we have shown we can assume that every word is written so that if u and v are maximal subwords in less than n variables of any words with $u \approx v$ then $u = v$. It should be clear that our choices can be made so that **a** is represented by itself. This is not essential but will make results easier to visualize. It also means if the word $\mathbf{a}f\mathbf{a}g\mathbf{a}$ is rewritten as above it will appear as $\mathbf{a}f_1\mathbf{a}g_1\,\mathbf{a}$ for some f_1, g_1.

DEFINITION 2·1. *A word w is an* invariant *if $f \approx g$ implies that the number of occurrences of w in f is congruent modulo 2 to the number of occurrences of w in g.*

Whether a given word is an invariant or not depends on n since f and g are, by assumption rewritten as described above. In order to prove that certain words are invariants we need the following well-known result (see (2), p. 156) which states that $f \approx g$ if and only if there is a proof.

LEMMA 2·2. *Let $f, g \in F(X)$. Then $f \approx g$ if and only if there exist $h_i \in F(X)$, $0 \leqslant i \leqslant m$, and $p_i, q_i, r_i \in F'(X)$, $0 \leqslant i \leqslant m-1$, such that $h_0 = f$, $h_m = g$ and for $0 \leqslant i \leqslant m-1$,*

$$\{h_i, h_{i+1}\} = \{p_i q_i r_i,\ p_i q_i^3 r_i\}.$$

THEOREM 2·3. *Let $|E(u)| < n$ and $x \in X - E(u)$. Then xux is an invariant.*

Proof. By Lemma 2·2 it is enough to show that the number of occurrences of xux in pqr is congruent modulo 2 to the number of occurrences of xux in pq^3r.

If $|E(q)| < n$ this is obvious since when rewritten using the solution of the word problem in less than n variables, pqr and pq^3r are represented by the same word.

The only situation in which an occurrence of xux in pqr is not simply matched with itself or with three copies of itself in the obvious way is when

$$pqr = p_1 p_2 q r_1 r_2, \quad xux = p_2 q r_1, \quad \text{and} \quad p_2 \neq \phi \neq r_1.$$

But then q is a subword of u and so $|E(q)| < n$.

If there is an occurrence of xux in pq^3r which is not matched with one in pqr in the way described above, it occurs because $q = q_1 q_2$ and $xux = q_2 q_1$ or possibly $q_2 q_1 q_2$ in case $q_2 = x$. In either case, there is a pair of such occurrences of xux in pq^3r.

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

THEOREM 2·4. *The word* $\mathbf{a}$ *is an invariant.*

Proof. The proof is similar to the proof of the previous theorem. If $\mathbf{a} = p_2 q r_1$ with $p_2 \neq \phi \neq r_1$ then $|E(q)| < n$ and so again pqr and pq^3r are represented by the same word.

III. *Minimality*

DEFINITION 3·1. *Let* $f \in S_n$. *Then* $\mathbf{a}f\mathbf{a}$ *is* minimal *if and only if* $\mathbf{a}f\mathbf{a} \approx \pi(\mathbf{a}f_i\mathbf{a} | i \in I)$ *implies that* $L(\mathbf{a}f\mathbf{a}) \leqslant L(\mathbf{a}f_i\mathbf{a})$ *for some* $i \in I$.

The minimal words are therefore those words in $\mathbf{a}S_n\mathbf{a}$ which cannot be written (modulo $\approx$) as a product of shorter words from $\mathbf{a}S_n\mathbf{a}$. The following is obvious.

PROPOSITION 3·2. *Every element of* G_n *can be represented as a product of minimal words.*

THEOREM 3·3. *Let* $E(f) \subseteq E(\mathbf{a}) \neq E(f)$. *Then* $\mathbf{a}f\mathbf{a}$ *is minimal.* (*In particular* $\mathbf{a}^2$ *is minimal.*)

Proof. It is clear that if $f = \phi$ and $\mathbf{a}^2 \approx \pi\mathbf{a}f_k\mathbf{a}$ then $L(\mathbf{a}^2) \leqslant L(\mathbf{a}f_k\mathbf{a})$ for any k. For the case $f \neq \phi$ let $a_i \notin E(f)$. By Theorem 2·4, $a_i \dots a_n f a_1 \dots a_i$ is an invariant. If

$$\mathbf{a}f\mathbf{a} \approx \pi\mathbf{a}f_k\mathbf{a},$$

the invariant must occur in the product. Since $a_i \notin E(a_{i+1} \dots a_n f a_1 \dots a_{i-1})$, and $f \neq \phi$, it follows that $a_i \dots a_n f a_1 \dots a_i$ occurs as a subword of $a_i \dots a_n f_k a_1 \dots a_i$ for some k and therefore $L(\mathbf{a}f\mathbf{a}) \leqslant L(\mathbf{a}f_k\mathbf{a})$.

LEMMA 3·4. *Let* $E(g) = E(xgy) = E(\mathbf{a})$. *Then* $\mathbf{a}xgy\mathbf{a}$ *is not minimal.*

Proof. By Lemma 1·5, $g \approx gagag$. Therefore

$$\begin{aligned}\mathbf{a}xgy\mathbf{a} &\approx \mathbf{a}x(gagag)y\mathbf{a}\\ &\approx \mathbf{a}xg\mathbf{a}^2g\mathbf{a}^2gy\mathbf{a}\end{aligned}$$

(by Corollary 1·6 and the fact that $\mathbf{a} \approx \mathbf{a}^3$). It follows that $\mathbf{a}xgy\mathbf{a}$ is not minimal since it has been written as a product of shorter words.

LEMMA 3·5. *Let* $f = a_i \dots a_n f_1$, $g = a_i \dots a_n g_1$, $\bar{I}(f) = \bar{I}(g)$ *and* $E(f) = E(g) = E(\mathbf{a})$. *Then* $\mathbf{a}f\mathbf{a}g\mathbf{a} \approx \mathbf{a}f_1\mathbf{a}g_1\mathbf{a}$.

Proof. Let $f = \bar{I}(f)\bar{f}$ and $g = \bar{I}(g)\bar{g}$. Then $\mathbf{a}f_1\mathbf{a}g_1\mathbf{a} = a_1 \dots a_{i-1} f a_1 \dots a_{i-1} g\mathbf{a}$

$$\begin{aligned}&\approx a_1 \dots a_{i-1}\bar{I}(f)[\bar{f}a_1 \dots a_{i-1}]\bar{I}(g)[\bar{g}\mathbf{a}](\bar{I}(g)\bar{g}\mathbf{a})^2\\ &\approx a_1 \dots a_{i-1}\bar{I}(f)[\bar{g}\mathbf{a}]\bar{I}(g)[\bar{f}a_1 \dots a_{i-1}](\bar{I}(g)\bar{g}\mathbf{a})^2\end{aligned}$$

(interchanging the square bracketed terms using Corollary 1·7)

$$\begin{aligned}&= \mathbf{a}g_1\mathbf{a}f\mathbf{a}g_1\mathbf{a}g\mathbf{a}\\ &\approx \mathbf{a}f\mathbf{a}g\mathbf{a}\end{aligned}$$

(using Lemma 1·5 and its Corollaries).

COROLLARY 3·6. *Let* $f = a_i \dots a_n f_1$, $E(f) = E(\mathbf{a})$ *and* $\bar{I}(f) \neq f$. *Then* $\mathbf{a}f\mathbf{a}$ *is not minimal.*

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

Proof. Let $g = \bar{I}(f) = a_i \dots a_n g_1$ in the Lemma. Then $\mathbf{a}f\mathbf{a}ga \approx \mathbf{a}f_1\mathbf{a}g_1\mathbf{a}$. It follows that $\mathbf{a}f\mathbf{a} \approx \mathbf{a}g\,\mathbf{a}^2f_1\,\mathbf{a}^2g_1\,\mathbf{a}$ using Lemma 1·5 and its Corollaries. Therefore $\mathbf{a}f\mathbf{a}$ has been expressed as a product of shorter words.

COROLLARY 3·7. *Let* $E(f) = E(\mathbf{a})$ *and* $f = a_i \dots a_n \bar{f} a_1 \dots a_j$. *Then* $\mathbf{a}f\mathbf{a}$ *is not minimal.*

Proof.

$$\mathbf{a}f\mathbf{a}a_i \dots a_n\bar{f}\mathbf{a}$$
$$\approx \mathbf{a}f\mathbf{a}a_i \dots a_n\bar{f}(a_1 \dots a_j)^2\mathbf{a}$$
$$\approx \mathbf{a}\bar{f}a_1 \dots a_j\,\mathbf{a}\bar{f}(a_1 \dots a_j)^2\mathbf{a}$$

(using the Lemma).

Consequently by Lemma 1·5 and its Corollaries, $\mathbf{a}f\mathbf{a} \approx \mathbf{a}\bar{f}a_1 \dots a_j\,\mathbf{a}^2\bar{f}\mathbf{a}^2a_i \dots a_n\bar{f}\mathbf{a}$, and so $\mathbf{a}f\mathbf{a}$ is expressed as a product of shorter words.

LEMMA 3·8. *Let* $E(f) = E(\mathbf{a})$ *and* $f = a_i \dots a_n h$. *Then* $\mathbf{a}f\mathbf{a}$ *is minimal if and only if* $f = \mathbf{a}$ *or* $\bar{I}(f) = f$ *and* $f \neq ga_1 \dots a_j$ *for all* $j \geqslant 1$.

Proof. Let $f = \mathbf{a}$ and assume $\mathbf{a}^3 \approx \pi\mathbf{a}f_k\mathbf{a}$. Now $\mathbf{a}$ is an invariant (by Theorem 2·5) which occurs three times in $\mathbf{a}^3$. It follows that $\mathbf{a}$ occurs an odd number of times in the product and therefore as a subword of f_k for some k. It follows that $L(\mathbf{a}^3) \leqslant L(\mathbf{a}f_k\mathbf{a})$ for that k, establishing that $\mathbf{a}^3$ is minimal.

If $f \neq \mathbf{a}$, let $\bar{I}(f) = f, f = \bar{f}a_j$ and assume that $\mathbf{a}f\mathbf{a} \approx \pi\mathbf{a}f_k\mathbf{a}$. Since $a_j \notin E(\bar{f})$, it follows that $a_j \dots a_n f$ is an invariant by Theorem 2·4. Therefore $a_j \dots a_n f$ occurs in the product. Since $a_j \notin \bar{f}$ and $f \neq ga_1 \dots a_j$ it follows that f is a subword of f_k for some k, and therefore $L(\mathbf{a}f\mathbf{a}) \leqslant L(\mathbf{a}f_k\mathbf{a})$ for that k, proving minimality.

Conversely if $\mathbf{a}f\mathbf{a}$ is minimal then $\bar{I}(f) = f$ by Corollary 3·6 and $f \neq ga_1 \dots a_j$ by Corollary 3·7.

THEOREM 3·9. *Let* $E(f) = E(\mathbf{a})$. *Then* $\mathbf{a}f\mathbf{a}$ *is minimal if and only if* $f = \mathbf{a}$ *or*

(i) $f = xgy$ *implies* $E(g) \neq E(\mathbf{a})$ *and*

(ii) $f = a_i \dots a_n h$ *implies* $\bar{I}(f) = f$ *and* $f \neq ga_1 \dots a_j$ *for all* $j \geqslant 1$ *and*

(ii)* *dual of* (ii).

Proof. Assume $f \neq \mathbf{a}$. Conditions (i), (ii) and (ii)* are necessary by Lemmas 3·4 and 3·8. If one or both of (ii) or (ii)* are applicable they are sufficient by Lemma 3·8 or its dual. Assume therefore that (i) applies but (ii) and (ii)* do not. Let $f = xgy$ and assume $a_i \notin E(g)$. Then $x = a_i$ or $y = a_i$ or both. If $x = y = a_i$, f is invariant (by 2·3). Since (ii) and (ii)* are not applicable, $f \neq a_i \dots a_n h$ and $f \neq ha_1 \dots a_i$. If $\mathbf{a}f\mathbf{a} \approx \pi\mathbf{a}f_k\mathbf{a}$ then f occurs as a subword of the product since it is invariant. It occurs, in fact, as a subword of f_k for some k because of the above properties. Consequently $\mathbf{a}f\mathbf{a}$ is minimal.

If $x = a_i$ and $y \neq a_i$, then $fa_1 \dots a_i$ is invariant. By the same analysis as above, if $\mathbf{a}f\mathbf{a} \approx \pi\mathbf{a}f_k\mathbf{a}$, then $fa_1 \dots a_i$ is a subword of the product, and since $f \neq a_i \dots a_n h$, f is a subword of f_k for some k. It follows that $\mathbf{a}f\mathbf{a}$ is minimal in this case as well. The remaining case is dual.

LEMMA 3·10. *Let* $\mathbf{a}f\mathbf{a}$ *be minimal.*

(i) $\mathbf{a}f\mathbf{a}$ *contains an invariant* J *of which* f *is a subword.*

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

(ii) *If* J *occurs in* $\pi \mathbf{a} f_k \mathbf{a}$ *then* f *occurs as a subword of* f_k *for some* k *and* J *occurs as a subword of* $\mathbf{a} f_k \mathbf{a}$.

Proof. Examine the proofs of Theorem 3·3, Lemma 3·8 and Theorem 3·9.

IV. *The word problem*

We first use the results of section III to describe a normal form for elements of G_n. The proofs of the various results in section III which led to a characterization of minimality enable us to represent every element of G_n as a product of minimal elements. Since G_n is a commutative group with identity $[\mathbf{a}^2]$ in which every element is its own inverse, we can represent every element of G_n as a product $\pi \mathbf{a} f_k \mathbf{a}$, where $\mathbf{a} f_k \mathbf{a}$ is minimal for every k, each minimal element occurs at most once in the product, and $f_k = \phi$ for some k only if the product represents $\mathbf{a}^2$.

DEFINITION 4·1. *An element* $[f] \in G_n$ *is written in* normal form *if* $f = \mathbf{a}^2$ *or*

$$f = \pi(\mathbf{a} f_j \mathbf{a} \mid j = 1, \ldots, m)$$

where $\mathbf{a} f_j \mathbf{a}$ *is minimal and* $f_j \neq \phi$ *for* $j = 1, \ldots, m$ *and* $f_j \neq f_k$ *if* $j \neq k$.

THEOREM 4·2. *Let* $f = \pi(\mathbf{a} f_j \mathbf{a} \mid j = 1, \ldots, r)$ *and* $g = \pi(\mathbf{a} g_k \mathbf{a} \mid k = 1, \ldots, s)$ *represent elements of* G_n *in normal form. Then* $[f] = [g]$ *if and only if* $r = s$ *and* $(f_1, \ldots, f_r)$ *is a permutation of* $(g_1, \ldots, g_s)$.

Proof. The sufficiency of the conditions is of course trivial. To show their necessity assume $f \approx g$. By Lemma 3·10 (i), there is for each f_j a g_k so that f_j is a subword of g_k and for each g_k an f_j so that g_k is a subword of f_j. In particular, this means that if f_j is not a proper subword of g_k for any k, it is equal to g_k for exactly one k.

Assume by induction that if f_i is a proper subword of g_k, then g_k has already been shown to be equal to exactly one f_j. The invariant of which f_i is a subword may occur in $\mathbf{a} g_k \mathbf{a}$ for one of these g_k, but if it does, this occurrence has already been paired with an occurrence in f. So the invariant must occur in $\mathbf{a} g_k \mathbf{a}$ so that f_i is a subword of g_k and not a proper subword. Thus $f_i = g_k$ and so by induction every f_i equals exactly one g_k and vice versa.

Remark 1. Theorem 4·2 shows that G_n is the free group satisfying $x^2 = 1$ on a suitable set of free generators. What is done in section III is to identify the generators.

Remark 2. The form of the algorithm we have given is easy to apply once words are written in normal form. However, it is possible to avoid normal forms as follows. Call a set S of invariants *complete* if for words f and g, $f \approx g$ if and only if for all $s \in S$ the number of occurrences of s in f is congruent modulo 2 to the number of occurrences of s in g. The proof of Theorem 4·2 shows that the invariants associated with the minimal words form a complete set of invariants for words in n variables written as described at the beginning of section II. We can therefore simply compare the number of occurrences of these invariants (modulo 2) in two words to decide if the words represent the same element of G_n.

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

V. *The two and three variable cases*

Table 1. *The three variable case*

Condition on f	Analysis	Number of words
(1) $f = \phi$	$abcabc$	1
(2) $E(f) = \{a\}$	$abcaabc$	1
(3) $E(f) = \{b\}$	$abcbabc$ $abcbbabc$	2
(4) $E(f) = \{c\}$	$abccabc$	1
(5) $E(f) = \{a, b\}$	fab can be any word in two variables a, b which ends in ab. There are 128/4 of these. The possibilities for f include ϕ, a, b, bb already listed	28
(6) $E(f) = \{a, c\}$	cfa can be any word in two variables a, c which starts in c and ends in a. There are 32 of these including $f = \phi$, a, c, already listed	29
(7) $E(f) = \{b, c\}$ $E(f) = \{a, b, c\}$	Dual to 5 $f = xhy$, where $x, y \in \{a, b, c\}$ and $E(h) \neq \{a, b, c\}$	28
(8) $ah(b, c)\ a$	Impossible by 3·9(ii)*	0
(9) $ah(a, c)\ b$	$cah(a, c)$ can be any word in two variables a, c. $h(a, c)$ cannot end in a by (3·9) (ii)*. There are $128/4.2$ possibilities. These include $f = ab$, aab, listed above	14
(10) $ah(b, c)\ b$	$h(b, c)\ b$ can be any word in two variables. It cannot start with bc. There are $(3 \times 128)/(4 \times 2)$ of these	48
(11) $ah(a, b)\ c$	$ah(a, b)$ can be any word in two variables. It cannot end with ab unless $f = abc$	49
(12) $ah(b, c)\ c$	Dual to 11, $f = abc$ already counted	48
(13) $bh(a, c)\ a$	$h(a, c)\ aa$ can be any word in two variables. It cannot start with c	16
(14) $bh(b, c)\ a$	Impossible	0
(15) $bh(a, c)\ b$	$h(a, c)$ can be any word in two variables. It cannot start with c or end with a	32
(16) $bh(a, b)\ c$	Dual to 10	48
(17) $bh(a, c)\ c$	Dual to 9	14
(18) $ch(a, b)\ a$	Impossible	0
(19) $ch(b, c)\ a$	Impossible	0
(20) $ch(a, b)\ b$	Dual to 14	0
(21) $ch(a, c)\ b$	Dual to 13	16
(22) $ch(a, b)\ c$	Dual to 8	0

The number of minimal words distinct from the identity is therefore 374. It follows that $q_3 = 2^{374}$ and therefore that $p_3 = 3^2 128^2 2^{374}$.

Let p_n be the number of distinct elements of $F_3(X)$ in which all the variables of a fixed set of n distinct variables occur. It is shown in (4) that

$$p_n = n^2 p_{n-1}^2 q_n,$$

where $q_n = |G_n|$. As is also pointed out in (4) the numbers p_n can be used to obtain $|F_3(m)|$, where $F_3(m)$ is the free semigroup satisfying $x = x^3$ on m free generators. In fact,

$$|F_3(m)| = \sum_{k=1}^{m} \binom{m}{k} p_k.$$

Of course $|F_3(1)| = p_1 = 2$.

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press

By examining Theorems 3·3 and 3·9 it can be seen that the minimal words in the two variables a, b are *abab*, *abaab*, *abbab*, *ababab*. Since *abab* acts as the identity, $|G_2| = 2^3$. It follows that $p_2 = 2^2 . 2^2 . 2^3 = 128$ and therefore

$$|F_3(2)| = 2p_1 + p_2 = 132.$$

In the three variable case, it is not practical to write down the minimal elements of G_3. We can, however, count them by classifying them in a certain way. This, and the counting for each class is done in Table 1. The minimal elements of G_3 are assumed to be represented by a word of the form *abcfabc* and various conditions on f are given.

This research was supported by the National Research Council of Canada.

REFERENCES

(1) Brown, T. C. On the finiteness of semigroups in which $x^r = x$. *Proc. Cambridge Philos. Soc.* **60** (1964), 1028–1029.
(2) Cohn, P. M. *Universal algebra* (New York, Harper and Row, 1965).
(3) Gerhard, J. A. The lattice of equational classes of idempotent semigroups, *J. Algebra* **15** (1970), 195–224.
(4) Green, J. A. & Rees, D. On semigroups in which $x^r = x$. *Proc. Cambridge Philos. Soc.* **48** (1952), 35-40.
(5) Howie, J. M. *An introduction to semigroup theory* (London, Academic Press, 1976).
(6) McLean, D. Idempotent semigroups. *Amer. Math. Monthly* **61** (1954), 110–113.

https://doi.org/10.1017/S0305004100054827 Published online by Cambridge University Press