

EMBEDDINGS INTO FINITE IDEMPOTENT-GENERATED SEMIGROUPS: SOME ARITHMETICAL RESULTS

by EMILIA GIRALDES AND JOHN M. HOWIE*

(Received 7th August 1989)

A *semiband* is defined as a semigroup generated by idempotents. It is known that every finite semigroup is embeddable in a finite semiband. For a class \mathbf{C} of semigroups and an integer $n \geq 2$, the number $\sigma_{\mathbf{C}}(n)$ is defined as the smallest k with the property that every semigroup of order n in the class \mathbf{C} is embeddable in a semiband of order not exceeding k . It is shown that for the class \mathbf{Gp} of groups $\sigma_{\mathbf{Gp}}(n) = nq(\rho_{\mathbf{Gp}}(n))$, where

$$q(m) = \min\{(r+1)(s+1) : rs \geq m\}$$

and

$$\rho_{\mathbf{C}}(n) = \max\{\text{rank}(S) : S \in \mathbf{C}, |S| = n\}.$$

Estimates are known (and are quoted) for the function q . Estimates are considered for the function $\rho_{\mathbf{C}}$ for various \mathbf{C} .

It is shown also that if $\mathbf{C0S}$, \mathbf{CS} denote respectively the classes of completely 0-simple and completely simple semigroups, then

$$\sigma_{\mathbf{C0S}}(n) = \sigma_{\mathbf{Gp}}(n-1) + 1, \sigma_{\mathbf{CS}}(n) = \sigma_{\mathbf{Gp}}(n).$$

1980 *Mathematics subject classification* (1985 Revision): 20M10

It has been known for some time [6] that every finite semigroup can be embedded in a finite semigroup generated by idempotents—i.e. in a finite *semiband*, to use the terminology of Benzaken and Mayr [1] and Pastijn [12]. The question of how efficiently (in an arithmetical sense) this can be done was raised and partly answered in [8]. The purpose of this note is to extend and develop some of the ideas in that paper.

The first stage, of course, is to make the question more precise. We borrow from [8] the definition that if $n \geq 2$ is an integer and \mathbf{C} is a class of semigroups then the integer k ($\geq n$) is a \mathbf{C} -semiband-cover of n if every semigroup of order n in the class \mathbf{C} can be embedded in a semiband of order not greater than k . Then $\sigma_{\mathbf{C}}(n)$ is defined as the smallest \mathbf{C} -semiband cover of n .

In this paper we shall be interested in the classes \mathbf{Sg} (semigroups), \mathbf{Gp} (groups), \mathbf{Nilp} (nilpotent groups), \mathbf{Ab} (abelian groups), \mathbf{EAb} (elementary abelian groups), \mathbf{CS} (completely simple semigroups), $\mathbf{0Gp}$ (0-groups) and $\mathbf{C0S}$ (completely 0-simple semigroups).

*This work was done partly during a visit to the Universidade Nova de Lisboa by the second author. Financial assistance from the British Council, the Universidade Nova and the Instituto Nacional de Investigação Científica is gratefully acknowledged.

1. Preliminaries

If S is a finite semigroup then as usual we define $r(S)$, the *rank* of S , by

$$r(S) = \min \{|A| : A \subseteq S, \langle A \rangle = S\}.$$

The rank of the trivial semigroup with just one element is defined to be 0. We shall be interested also in the smallest possible number of non-idempotents in a generating set of S : if E is the set of idempotents of S then

$$g(S) = \min \{|A \setminus E| : A \subseteq S, \langle A \rangle = S\}.$$

The numbers $r(S)$ and $g(S)$ may well be different: for example, if S is a semiband then $g(S) = 0$, while $r(S)$ may be quite large. (See, for example, [5], [9].) However, we do have:

Lemma 1. *If S has a single idempotent, then $g(S) = r(S)$.*

Proof. From the definition it is clear that $g(S) \leq r(S)$ for every finite semigroup. To show this opposite inequality, let S be a semigroup with a single idempotent element e . If $r(S) = 0$ (so that $S = \{e\}$) or if $r(S) = 1$ (so that $S = \langle a \rangle$, $a^2 \neq a$) then the result is trivial. Suppose that $r(S) \geq 2$ and let $A = \{g_1, \dots, g_k\}$ be a generating set for S , with $k \geq r(S) \geq 2$. At most one of g_1, \dots, g_k is idempotent. If (say) $g_1 = e$ then g_1 is superfluous within the generating set A , since some power of g_2 (being idempotent) must equal e . Thus $\{g_2, \dots, g_k\}$ generates S in this case and so $|A \setminus E| = k - 1 \geq r(S)$.

In particular, $g(S) = r(S)$ if S is a group

If \mathbf{C} is a class of semigroups we may define

$$\rho_{\mathbf{C}}(n) = \max \{r(S) : S \in \mathbf{C}, |S| = n\}$$

and

$$\gamma_{\mathbf{C}}(n) = \max \{g(S) : S \in \mathbf{C}, |S| = n\}.$$

It is a consequence of Lemma 1 that for every class \mathbf{C} of groups

$$\gamma_{\mathbf{C}}(n) = \rho_{\mathbf{C}}(n). \tag{1}$$

In the study of the function $\sigma_{\mathbf{C}}(n)$ (for various classes \mathbf{C} of semigroups) in [8] both $\rho_{\mathbf{C}}(n)$ and the arithmetical function

$$q(n) = \min \{(r + 1)(s + 1) : rs \geq n\} \tag{2}$$

were found to play an important part, but it was not fully realised how intimately the

behaviour of $\sigma_{\mathbf{C}}(n)$ is bound up with the behaviour of these two functions and of the function $\gamma_{\mathbf{C}}(n)$. In [2], by a method suggested in a letter from Professor Norman R. Reilly, it was shown that for every class of semigroups

$$\sigma_{\mathbf{C}}(n) \leq (n+1)q(\gamma_{\mathbf{C}}(n)). \quad (3)$$

If \mathbf{C} is a class of *monoids* this upper bound can be improved:

$$\sigma_{\mathbf{C}}(n) \leq nq(\gamma_{\mathbf{C}}(n)). \quad (4)$$

2. Groups

In the case where \mathbf{C} is a class of *groups* we can in fact specify the function $\sigma_{\mathbf{C}}$ completely in terms of the functions q and $\rho_{\mathbf{C}}$:

Theorem 1. *If \mathbf{C} is a class of groups then for all $n \geq 2$*

$$\sigma_{\mathbf{C}}(n) = nq(\rho_{\mathbf{C}}(n)).$$

Proof. We begin with a lemma.

Lemma 2. *If G is a subgroup of a finite group H then*

$$|G|q(r(G)) \leq |H|q(r(H)).$$

Proof. The result is immediate if $G=H$. Suppose that $G < H$. By the definition (2) of the function q ,

$$q(r(H)) = (u+1)(v+1),$$

where $uv \geq r(H)$. So

$$\begin{aligned} \frac{|H|}{|G|} q(r(H)) &= \frac{|H|}{|G|} (u+1)(v+1) \\ &= (u'+1)(v+1), \end{aligned} \quad (5)$$

where

$$u' = \frac{|H|}{|G|} (u+1) - 1.$$

Now

$$\begin{aligned}
 u'v &= \frac{|H|}{|G|} uv + \left(\frac{|H|}{|G|} - 1 \right) v \\
 &\geq \frac{|H|}{|G|} uv, \text{ since } \frac{|H|}{|G|} \geq 2. \\
 &\geq \frac{|H|}{|G|} r(H).
 \end{aligned}$$

Now, from [8, p. 327], we have that

$$|H|r(H) \geq |G|r(G);$$

hence $u'v \geq r(G)$ and so from (5)

$$\frac{|H|}{|G|} q(r(H)) \geq q(r(G)),$$

as required.

To prove the theorem, consider a finite group G and suppose that it is embedded in a finite semiband B . By the argument in [8, p. 330] we may assume that B is simple or 0-simple and that G is contained in a single \mathcal{H} -class of B . Thus $B = M[H; I, \Lambda; P]$ or $M^\circ[H; I, \Lambda; P]$ with $G \leq H$. Again by the argument in [8, p. 330] we have

$$(|I| - 1)(|\Lambda| - 1) \geq r(H);$$

hence

$$|B| \geq |H||I||\Lambda| \geq |H|q(r(H)) \geq |G|q(r(G)).$$

If we now choose G to be a group in \mathbf{C} of order n and of greatest possible rank $\rho_{\mathbf{C}}(n)$ we get

$$|B| \geq nq(\rho_{\mathbf{C}}(n)),$$

giving

$$\sigma_{\mathbf{C}}(n) \geq nq(\rho_{\mathbf{C}}(n))$$

as required.

This is not the end of the story, of course, for the functions q and $\rho_{\mathbf{C}}$ are not

elementary, and there is obviously some interest in estimating them in terms of more familiar functions. The study of q was begun in [8], where it was shown that

$$m + 2\sqrt{m+1} \leq q(m) \leq m + 3\sqrt{m+1}$$

for all $m \geq 1$. The lower bound is best possible, being attained (for example) whenever m is a square. The upper bound was much less satisfactory, and has been substantially improved in [10], where it is shown that

$$q(m) \leq m + 2\sqrt{m + 2m^{1/4}}$$

for all but 4 values (namely $m = 73, 601, 1261$ and 4063) of m .

As for the function ρ_C , we can find bounds in terms of the arithmetical functions λ, μ defined as follows. If

$$n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} \tag{6}$$

where p_1, \dots, p_k are distinct primes and $r_1, \dots, r_k \geq 1$, let

$$\lambda(n) = r_1 + \dots + r_k, \quad \mu(n) = \max\{r_1, \dots, r_k\}.$$

Then we have:

Theorem 2. *Let C be a class of groups and let $n \geq 2$. Then $\rho_C(n) \leq \lambda(n)$. If C contains the class **EAb** of elementary abelian groups, then $\rho_C(n) \geq \mu(n)$.*

Proof. Both of these inequalities are fairly easy exercises in group theory and are probably well-known. A precise reference is, however, somewhat elusive. Suppose that G is a group of order n given by (6), and let $\{g_1, \dots, g_r\}$ be a generating set for G , where $r = r(G)$. In the sequence

$$\{1\} \subset G_1 \subset G_2 \subset \dots \subset G_r = G,$$

where $G_i = \langle g_1, \dots, g_i \rangle$, all inclusions are proper, and so

$$n = \frac{|G_r|}{|G_{r-1}|} \dots \frac{|G_2|}{|G_1|} \cdot |G_1|$$

is a product of r non-trivial factors. Hence $r \leq r_1 + r_2 + \dots + r_k = \lambda(r)$.

Suppose now that $C \supset \mathbf{EAb}$. Then among the groups of order n in C is the abelian group

$$A = A_1 \times \dots \times A_k.$$

where A_j is the direct product of r_j cyclic groups of order p_j . Thus $r(A_j) = r_j$ and the required inequality now follows from the following lemma, easily proved by methods to be found in [11]:

Lemma 3. *Let A, B be finite groups such that $|A|, |B|$ are coprime. Then $r(A \times B) = \max\{r(A), r(B)\}$.*

Examples.

$$\mu(6) = 1, \rho_{\text{Gp}}(6) = \lambda(6) = 2;$$

$$\mu(8) = \lambda(8) = \rho_{\text{Gp}}(8) = 3;$$

$$\mu(15) = \rho_{\text{Gp}}(15) = 1, \lambda(15) = 2;$$

$$\mu(105) = 1, \rho_{\text{Gp}}(105) = 2, \lambda(105) = 3.$$

Next, we have:

Theorem 3. *Let C be a class of groups such that*

$$\mathbf{EAb} \subseteq C \subseteq \mathbf{Nilp}.$$

Then $\rho_C(n) = \mu(n)$ for all $n \geq 2$.

Proof. Let $G \in C$ be of order n , given by (6). Then G , being nilpotent, is a direct product of its Sylow subgroups:

$$G = P_1 \times P_2 \times \cdots \times P_k,$$

where P_j is a p_j -group of order $p_j^{r_j}$. By Theorem 2 we have

$$r(P_j) \leq \lambda(p_j^{r_j}) = r_j$$

and by Lemma 3 it follows that

$$r(G) \leq \max\{r_j; 1 \leq j \leq k\} = \mu(n).$$

Thus $\rho_C(n) \leq \mu(n)$ and the result now follows from Theorem 2.

The result does not extend to soluble groups. S_3 , the symmetric group on 3 symbols, provides an example.

From Theorems 1 and 3 we now have:

Corollary. *If C is a class of groups such that $\mathbf{EAb} \subseteq C \subseteq \mathbf{Nilp}$, then $\sigma_C(n) = nq(\mu(n))$.*

3. Completely 0-simple semigroups

Theorem 2 gives a useful upper bound for $\rho_C(n)$ when C is a class of groups. For the class \mathbf{Sg} of all semigroups it is not possible to assert anything stronger than the trivial remark that

$$\rho_{\mathbf{Sg}}(n) \leq n,$$

for it is perfectly possible for a semigroup of order n to have rank n . As remarked in [4], however, if S is such a semigroup then S must consist entirely of idempotents and so $g(S) = 0$. Accordingly we can say that

$$\gamma_{\mathbf{Sg}}(n) \leq n - 1.$$

This bound cannot be improved, since, for example, a null semigroup $S = \{0, x_1, \dots, x_{n-1}\}$ of order n has $g(S) = n - 1$. Semigroups for which $r(S) = n - 1$ have been extensively studied in [4] and [3].

As a consequence, the upper bound given by (3) is less effective when applied to a class C not contained in \mathbf{Gp} . However, in view of the fairly good information we have obtained for $\sigma_{\mathbf{Gp}}$, it is reasonable to seek results expressing σ_C (for suitably restricted class C) in terms of $\sigma_{\mathbf{Gp}}$. The main theorem of this section is:

Theorem 4. *Let \mathbf{COS} be the class of completely 0-simple semigroups. Then for all $n \geq 3$*

$$\sigma_{\mathbf{COS}}(n) = \sigma_{\mathbf{Gp}}(n - 1) + 1.$$

Proof. We show first that

$$\sigma_{\mathbf{COS}}(n) \geq \sigma_{\mathbf{Gp}}(n - 1) + 1,$$

and we do this by means of a lemma.

Lemma 1. *Let \mathbf{OGp} be the class of 0-groups. Then, for all $n \geq 2$,*

$$\sigma_{\mathbf{OGp}}(n) = \sigma_{\mathbf{Gp}}(n - 1) + 1.$$

Proof. Let G° be a 0-group of order n . Then G is a group of order $n - 1$ and is embeddable in a semiband B of order $\sigma_{\mathbf{Gp}}(n - 1)$. Hence G° is embedded in B° , of order at most $\sigma_{\mathbf{Gp}}(n - 1) + 1$. Hence

$$\sigma_{\mathbf{OGp}}(n) \leq \sigma_{\mathbf{Gp}}(n - 1) + 1.$$

To prove the opposite inequality, suppose that a 0-group G° is embedded in a semiband B . The elements of G must lie within a single \mathcal{H} -class H of B and must be

expressible as products of idempotents from within the \mathcal{J} -class J of B containing H . The order of J must be at least $(n-1)q(r(G))$, and so must be at least $(n-1)q(\rho_{Gp}(n-1))$ if we choose G to have maximum possible rank among the groups of order $n-1$. By Theorem 1 we thus have that

$$|J| \geq \sigma_{Gp}(n-1).$$

Now if e is the identity of G then $e > 0$ in B and so $0 \notin J$. Hence

$$|B| \geq \sigma_{Gp}(n-1) + 1,$$

as required.

Since $0Gp \subseteq C0S$ it now follows that

$$\sigma_{C0S}(n) \geq \sigma_{0Gp}(n) = \sigma_{Gp}(n-1) + 1.$$

To show the reverse inequality, consider a completely 0-simple semigroup

$$S = M^\circ[G; I, \Lambda; P] \tag{1}$$

of order n , where $|G|=m$, $|I|=r$, $|\Lambda|=s$ and $mrs=n-1$. It is convenient to consider first the case where $m=1$ and so $G=\{1\}$, the trivial group. Let

$$T = M^\circ[\{1\}; I \cup \{x\}, \Lambda \cup \{\xi\}; Q]$$

where $q_{\lambda i} = p_{\lambda i}$ for $\lambda \in \Lambda, i \in I$ and where

$$q_{\lambda x} = q_{\xi i} = q_{\xi x} = 1 \quad (\lambda \in \Lambda, i \in I).$$

Certainly T contains S . Moreover T is a semiband, since for all μ in $\Lambda \cup \{\xi\}$, j in $I \cup \{x\}$ the element $(j, 1, \mu)$ is a product

$$(j, 1, \xi)(x, 1, \mu)$$

of idempotents.

As for the order of T , it is clear that

$$\begin{aligned} |T| - 1 &= (r+1)(s+1) = rs + (r+s) + 1 \\ &= (n-1) + (r+s) + 1 \leq (n-1) + n + 1 = 2n, \end{aligned}$$

since $\max\{r+s : rs=n-1\} = n$. Certainly

$$|T| < \sigma_{G_p}(n-1) + 1.$$

Suppose now that the completely 0-simple semigroup given by (1) has the property that $m > 1$. We may suppose that the sandwich matrix P is normal in the sense of Tamura (see [13], [8]), which certainly implies that for all $i \in I$ there exists $\lambda \in \Lambda$ such that $p_{\lambda i} = 1$ (the identity of G) and for all $\lambda \in \Lambda$ there exists $i \in I$ such that $p_{\lambda i} = 1$. There is in fact no loss of generality in naming I and Λ so that $I \cap \Lambda = \{1\}$ and so that $p_{11} = 1$.

We now construct a completely 0-simple semigroup

$$T = M^\circ[G; J, M; Q].$$

We suppose without loss of generality that $s \geq r$, and we take $J \supset I$ with $|J| = r + u$, $M = \Lambda \cup \{\xi\}$ (so that $|M| = s + 1$). The matrix $Q = (q_{\mu j})$ includes the matrix P in the sense that $q_{\lambda i} = p_{\lambda i}$ for $\lambda \in \Lambda, i \in I$. The extra entries of Q are defined as follows:

$$\begin{aligned} q_{\xi i} &= 1 & (i \in I); \\ q_{1j} &= 1 & (j \in J \setminus I); \end{aligned}$$

the entries $q_{\mu j} (\mu \in M \setminus \{1\}, j \in J \setminus I)$ form a set of generators for G .

$$Q = \begin{bmatrix} & & & 1 \dots 1 \\ & & & \dots \\ & P & & * \\ \dots & & & \dots \\ 1 \dots 1 & & & * \end{bmatrix}.$$

For this to be possible for an arbitrary group of order m we require that

$$su \geq \rho_{G_p}(m); \tag{1}$$

so we may take

$$(s + 1)(u + 1) = q(\rho_{G_p}(m)). \tag{2}$$

The semigroup T is of order

$$m(s + 1)(r + u) + 1. \tag{3}$$

It is clear that $S \leq T$. The next stage in the argument is to prove:

Lemma 2. *T is a semiband.*

Proof. By Theorem 1 in [7] (and in the notation of that theorem) we must show that T is connected and that $V_{x,y} = G$ for some x, y in $J \cup M$. First, for every j in J and μ in M we have a path

$$j \rightarrow \xi \rightarrow k \rightarrow \mu$$

(with $k \in J \setminus I$) since $q_{\xi j}, q_{\xi k}, q_{\mu k}$ are all non-zero. Thus T is connected.

To show the other property it is convenient to draw a temporary notational distinction between 1 as an element of Λ and 1 as an element of I . Writing 1_Λ and 1_I , we note that for each λ in Λ we can by the normal property choose i in I so that $q_{\lambda i} = 1$. Hence for each k in $J \setminus I$ and each λ in Λ we have a path

$$1_I \rightarrow \xi \rightarrow i \rightarrow \lambda \rightarrow k \rightarrow 1_\Lambda$$

with value

$$q_{\xi 1}^{-1} q_{\xi i} q_{\lambda i}^{-1} q_{\lambda k} q_{1 k}^{-1} = 1 \cdot 1 \cdot 1 \cdot q_{\lambda k} \cdot 1 = q_{\lambda k}.$$

The simple path

$$1_I \rightarrow \xi \rightarrow k \rightarrow 1_\Lambda$$

has value $q_{\xi k}$.

It follows that $V_{1,1}$ contains $q_{\mu k}$ for all μ in $M \setminus \{1\}$ and all k in $J \setminus I$. Hence $V_{1,1} = G$ and so T is a semiband.

From (2) and (3) the order of T is

$$m(s+1)[(r-1)+(u+1)] + 1 = m(r-1)(s+1) + mq(\rho_{G_p}(m)) + 1.$$

If $m = n - 1$ this reduces to

$$(n-1)q(\rho_{G_p}(n-1)) + 1 = \sigma_{G_p}(n-1) + 1,$$

the value we have already obtained for a 0-group.

If $m = (n-1)/2$ or $(n-1)/3$ then $(r-1)(s+1) = 0$ and we get a semiband T of order

$$mq(\rho_{G_p}(m)) + 1.$$

Since $\rho_{G_p}(m) \leq \rho_{G_p}(n-1)$ this is certainly less than $\sigma_{G_p}(n-1) + 1$.

Suppose now that $1 < m \leq (n-1)/4$. Then

$$\begin{aligned} |T| - 1 &= m(r-1)(s+1) + mq(\rho_{G_p}(m)) \\ &< mrs + mq(\rho_{G_p}(m)) \text{ (since } (r-1)(s+1) < rs) \\ &= (n-1) + mq(\rho_{G_p}(m)) \\ &\leq (n-1)[1 + \frac{1}{4}q(\rho_{G_p}(m))] \end{aligned}$$

$$\leq (n-1)q(\rho_{G_p}(n-1)).$$

This completes the proof.

Corollary. $\sigma_{CS}(n) = \sigma_{G_p}(n)$.

Proof. Since $G_p \subseteq CS$ we certainly have $\sigma_{CS}(n) \geq \sigma_{G_p}(n)$.

Conversely, let $S = M[G; I, \Lambda; P]$ be a completely simple semigroup of order n . Then $S^\circ = M^\circ[G; I, \Lambda; P]$ is a completely 0-simple semigroup of order $n+1$, and the matrix P has no zero entries. By the method of the theorem we embed S° in a semiband $T = M^\circ[G; J, M; Q]$ of order not greater than $\sigma_{G_p}(n) + 1$, and Q has no zero entries. Then $T \setminus \{0\}$ is a semiband of order not exceeding $\sigma_{G_p}(n)$ containing S .

REFERENCES

1. C. BENZAKEN and H. C. MAYR, Notion de demi-bande: demi-bandes de type deux, *Semigroup Forum* **10** (1975), 115–125.
2. EMILIA JOAQUINA GIRALDES SOARES, *Semigrupos de característica superior* (Dissertação de Doutoramento em Matemática, Universidade de Lisboa, 1984).
3. EMILIA GIRALDES, Semigroups of high rank. II. Doubly noble semigroups, *Proc. Edinburgh Math. Soc.* **28** (1985), 409–417.
4. EMILIA GIRALDES and JOHN M. HOWIE, Semigroups of high rank, *Proc. Edinburgh Math. Soc.* **28** (1985), 13–34.
5. GRACINDA M. S. GOMES and JOHN M. HOWIE, On the ranks of certain semigroups of transformations, *Math. Proc. Cambridge Philos. Soc.* **101** (1987), 395–403.
6. JOHN M. HOWIE, The subsemigroup generated by the idempotents of a full transformation semigroup, *J. London Math. Soc.* **41** (1966), 707–716.
7. JOHN M. HOWIE, Idempotents in completely 0-simple semigroups, *Glasgow Math. J.* **19** (1978), 109–113.
8. JOHN M. HOWIE, Embedding semigroups in semibands: some arithmetical results, *Quart. J. Math. Oxford* (2) **32** (1981), 323–337.
9. JOHN M. HOWIE and ROBERT B. MCFADDEN, Idempotent rank in finite full transformation semigroups, *Proc. Roy. Soc. Edinburgh A* **114** (1990), 161–167.
10. JOHN M. HOWIE and J. L. SELFRIDGE, A semigroup embedding problem and an arithmetical function, *Math. Proc. Cambridge Philos. Soc.*, to appear.
11. IAN D. MACDONALD, *The theory of groups* (Oxford, 1968).
12. FRANCIS PASTIJN, Embedding semigroups in semibands, *Semigroup Forum* **14** (1977), 247–263.
13. T. TAMURA, Decompositions of a completely 0-simple semigroup, *Osaka J. Math.* **12** (1960), 269–275.

UNIVERSIDADE NOVA DE LISBOA

UNIVERSITY OF ST ANDREWS