Proceedings of the Edinburgh Mathematical Society (1999) **42**, 551–557 ©

ON PRODUCTS OF ALL ELEMENTS OF A FINITE SEMIGROUP

by P. Z. HERMANN,* E. F. ROBERTSON and N. RUŠKUC

(Received 22nd October 1997)

Let S be a finite semigroup. Consider the set $p(S)$ of all elements of S which can be represented as a product of all the elements of S in some order. It is shown that $p(S)$ is contained in the minimal ideal M of S and intersects each maximal subgroup H of M in essentially the same way. The main result shows that $p(S)$ intersects H in a union of cosets of H'.

1991 *Mathematics subject classification:* 20D60, 20M12.

1. Introduction

Let A be a set with an associative binary operation denoted by multiplication, and let $X \subseteq A$ be a finite subset of A. If $|X| = n$, with $X = \{x_1, \ldots, x_n\}$, we define

$$p(X) = \{x_{\pi(1)} \ldots x_{\pi(n)} : \pi \in \mathrm{Sym}(n)\},$$

where $\mathrm{Sym}(n)$ denotes the set of all permutations of degree n. With this notation Wilson's Theorem from elementary number theory states that

$$p(\mathbb{Z}_p \backslash \{0\}) = \{-1\},$$

where p is a prime.

The set $\mathbb{Z}_p \backslash \{0\}$ can be viewed as the multiplicative group of the field $\mathrm{GF}(p)$, and also as the set of all non-zero elements of the ring $\mathbb{Z}_p$. A number of results have been proved generalising Wilson's Theorem in the above form. In particular, if $\mathbb{Z}_p \backslash \{0\}$ is replaced by an arbitrary finite group then we have the following

Theorem 1.1 ([2]). *Let G be a finite group. Then $p(G)$ is a complete coset of the derived subgroup G' of G, i.e. for some $a \in G$ we have $p(G) = G'a$.*

Also, if $\mathbb{Z}_p$ is replaced by an arbitrary ring R, the set $p(R \backslash \{0\})$ is described in [3].

* The first author wishes to acknowledge support from the TEMPUS grant JEP06044-94/1 which enabled him to visit the University of St Andrews where this work was carried out. Research partially supported by Hungarian Research Foundation OTKA, No. T022925.

There it is proved that $p(R\backslash\{0\}) = \{0\}$, except when R is the full matrix ring over a finite field, or one of six exceptions.

In this paper we use Theorem 1.1 to prove a more general result concerning the set $p(S)$ for an arbitrary finite semigroup S.

2. Statement of the Main Result

Let S be a finite semigroup. It is clear that $p(S)$ is a subset of the minimal ideal M of S. By [**4**, Proposition 3.1.3] M is a simple semigroup. Moreover M, being finite, contains minimal left ideals and minimal right ideals, and so is completely simple. Therefore, by Rees' Theorem [**4**, Theorems 3.2.3, 3.3.1], M can be represented as a Rees matrix semigroup $\mathcal{M}[H; I, J; P] = I \times H \times J$. Here H is a group, I and J are index sets, P is a $J \times I$ matrix with entries in H, and multiplication is given by

$$(i_1, h_1, j_1)(i_2, h_2, j_2) = (i_1, h_1 p_{j_1 i_2} h_2, j_2).$$

It is well known that P can be chosen in normal form, that is $p_{1i} = p_{j1} = 1$; see [**4**, Theorem 3.4.2].

From this representation it is easy to see that M is the disjoint union of $|I||J|$ groups

$$(i, H, j) = \{(i, h, j) : h \in H\}.$$

Each of these groups is a maximal subgroup of M and is isomorphic to H.

Since S is finite, it has a unique maximal group homomorphic image G by [**4**, Exercise 2.6.12]. In the following lemma we list some properties linking S, M and G; these will help in understanding the statement of the main theorem, and will also be used in its proof.

Lemma 2.1. *Let S be a finite semigroup, let G be the maximal group homomorphic image of S, let $\nu : S \to G$ be the natural epimorphism, let M be the minimal ideal of S, and let H be a maximal subgroup of M.*

(i) *The restrictions $\nu\restriction_H$ and $\nu\restriction_M$ are both onto.*

(ii) *G is the maximal group homomorphic image of M.*

(iii) *If M is represented as a Rees matrix semigroup $\mathcal{M}[H; I, J; P]$, with P in normal form, then the kernel of the restriction $\nu\restriction_H$ is the normal subgroup of H generated by the set $\{p_{ji} : i \in I, j \in J\}$.*

Proof. (i) This follows from [**1**, Theorem 2].

(ii) By (i) G is a homomorphic image of M. To show that every group homomorphic image of M is also a homomorphic image of S we let $\phi : M \to G$ be an epimorphism, and choose an arbitrary idempotent $e \in M$. Define a mapping $\psi : S \to G$

https://doi.org/10.1017/S0013091500020514 Published online by Cambridge University Press

by $x\psi = (exe)\phi$. For $x \in M$ we have

$$x\psi = (exe)\phi = (e\phi)(x\phi)(e\phi) = x\phi,$$

and so ψ is onto. To show that ψ is a homomorphism, let $x, y \in S$ be arbitrary. Since $ex, ye \in M$ we have

$$\begin{aligned}(xy)\psi &= (exye)\phi = (ex)\phi(ye)\phi = (ex)\phi(e\phi)(e\phi)(ye)\phi \\ &= (exe)\phi(eye)\phi = (x\psi)(y\psi),\end{aligned}$$

as required.

(iii) This follows from (ii) and [4, Theorem 3.5.9]. □

Now we can state and prove our main theorem.

Main Theorem. *Let S be a finite semigroup, let G be the maximal group homomorphic image of S, let $\nu : S \to G$ be the natural epimorphism, and let M be the minimal ideal of S.*

(i) *There exists a coset $G'a$ in G such that*

$$p(S) = (G'a)\nu^{-1} \cap M = (G'a)\nu\restriction_M^{-1}. \tag{1}$$

(ii) *$p(S)$ intersects every maximal subgroup of M.*

(iii) *Let H be an arbitrary maximal subgroup of M, and let $T = \ker(\nu\restriction_H)$. Then $p(S) \cap H$ is a full coset of the normal subgroup $H'T$ of H, i.e.*

$$p(S) \cap H = H'Th = (G'\nu\restriction_H^{-1})h. \tag{2}$$

Remark 2.2. If $S = H = G$ is a group, then the Main Theorem reduces to Theorem 1.1. More generally, if $M = \mathcal{M}[H; I, J; P]$ with $P = [1]_{J\times I}$ (i.e. if the idempotents of M are closed under multiplication) the set $p(S) \cap H$ is a full coset of H' in H.

Remark 2.3. If S is a semigroup with zero then clearly $p(S) = \{0\}$. In this case, given the results of [3], it would be of more interest to describe the set $p(S\backslash\{0\})$. Note that $p(S\backslash\{0\}) \subseteq M$, where M is any 0-minimal ideal of S. Consequently, if S has more than one 0-minimal ideal then $p(S) = \{0\}$. So let us assume that M is a unique 0-minimal ideal of S. It is known that M is either a semigroup with zero multiplication, or else it is isomorphic to a Rees matrix semigroup $\mathcal{M}^0[H; I, J; P]$ over a group with zero; see [4, Proposition 3.1.3 and Theorem 3.2.3]. If M has zero multiplication and $|M| > 3$ then we must have $p(S\backslash\{0\}) = \{0\}$. If M has zero multiplication and $|M| = 2$, then $p(S\backslash\{0\})$ is either equal to $\{0\}$ or to $M\backslash\{0\}$ or to M, and all these possibilities occur. The remaining case is when M is a Rees matrix semigroup over a group with zero. For

https://doi.org/10.1017/S0013091500020514 Published online by Cambridge University Press

example, if S is a full matrix semigroup over a finite field, then $p(S\backslash\{0\}) = M$ by [3] and [4, Exercise 2.6.19]. By way of contrast, if S is the five element Brandt semigroup

$$\langle a, b \mid aba = a, bab = b, a^2 = 0, b^2 = 0\rangle,$$

then $S = M$ and $p(S) = \{0, ab, ba\}$; so $p(S)$ intersects some, but not all, $\mathcal{H}$-classes of M.

3. Proof of the Main Theorem

First we note that part (ii) of the theorem is an immediate consequence of part (i) and Lemma 2.1 (i).

Next we prove direct inclusion for parts (i) and (iii), namely

$$p(S) \subseteq (G'a)\nu^{-1} = (G'a)\nu\restriction_M^{-1}, \tag{3}$$

$$p(S) \cap H \subseteq H'Th = (G'\nu\restriction_H^{-1})h. \tag{4}$$

As we mentioned before, $p(S)$ is clearly contained in M. If $|S| = n$, with $S = \{s_1, \ldots, s_n\}$, then we have

$$(p(S))\nu = \{s_{\pi(1)} \ldots s_{\pi(n)} : \pi \in \mathrm{Sym}(n)\}\nu = \{(s_{\pi(1)}\nu) \ldots (s_{\pi(n)}\nu) : \pi \in \mathrm{Sym}(n)\}.$$

All the products in this set are permutations of each other, and hence they are all equal modulo G'. Therefore $p(S)\nu \subseteq G'a$ for some $a \in G$, and so $p(S) \subseteq (G'a)\nu^{-1}$. By Lemma 2.1 it follows that $H'\nu = G'$ and $a = h\nu$ for some $h \in H$. Now we have

$$p(S) \cap H \subseteq (G'a)\nu^{-1} \cap H = (G'a)\nu\restriction_H^{-1} = ((H'h)\nu\restriction_H)\nu\restriction_H^{-1}$$

$$= H'Th = (H'\nu\restriction_H)\nu\restriction_H^{-1}h = (G'\nu\restriction_H^{-1})h.$$

Now we can see that the proof of the theorem will be finished once we complete the proof of part (iii). Indeed, we have seen that

$$p(S) \subseteq (G'a)\nu\restriction_M^{-1} = \bigcup_H (G'a)\nu\restriction_H^{-1}$$

where the union is taken over all maximal subgroups of M. Thus $p(S)$ is contained in a set of size $|H'T||I||J|$. On the other hand, (iii) implies that $p(S) \cap H$ is a set of size $|H'T|$, and so the above inclusion cannot be proper.

In the remainder of this section we concentrate on the proof of (iii). Without loss of generality we identify H with the group $(1, H, 1)$ in the Rees matrix representation $\mathcal{M}[H; I, J; P]$ of M, and we recall that P can be chosen in normal form. By Lemma 2.1 (iii) T is the normal subgroup of H generated by the set $\{p_{ji} : i \in I, j \in J\}$.

Assume first that $|J| = 1$, in which case P is a row of ones, and therefore T is trivial.

https://doi.org/10.1017/S0013091500020514 Published online by Cambridge University Press

Decompose S into the disjoint union $S = (1, H, 1) \cup (S \backslash (1, H, 1))$, so that

$$p(S) \supseteq p((1, H, 1))p(S \backslash (1, H, 1)). \tag{5}$$

Since $p((1, H, 1)) \subseteq (1, H, 1)$ and $|J| = 1$, the right hand side of (5) is contained in $(1, H, 1)$. Therefore, for an arbitrary $x \in p(S \backslash (1, H, 1))$, we have

$$|p(S) \cap H| \geq |p((1, H, 1))p(S \backslash (1, H, 1)) \cap H| = |p((1, H, 1))p(S \backslash (1, H, 1))|$$

$$\geq |p(1, H, 1)x| = |p((1, H, 1))| = |p(H)| = |H'| = |H'T|$$

by [4, Lemmas 2.2.1 and 2.2.2] and Theorem 1.1. From the last inequality and (4), we conclude that $p(S) \cap H = H'Th$ in this case. The case where $|I| = 1$ is dealt with by a dual argument.

Now we consider the general situation with $|I| > 1$ and $|J| > 1$, and we let

$$I^* = I \backslash \{1\}, J^* = J \backslash \{1\}.$$

We decompose S into the disjoint union

$$S = (1, H, 1) \cup (S \backslash ((I, H, 1) \cup (1, H, J))) \cup ((I^*, H, 1) \cup (1, H, J^*)),$$

so that

$$p(S) \supseteq p((1, H, 1))p(S \backslash ((I, H, 1) \cup (1, H, J)))p((I^*, H, 1) \cup (1, H, J^*)).$$

Since $|I| > 1$ and $|J| > 1$, the set $S \backslash ((I, H, 1) \cup (1, H, J))$ contains elements from M, and hence

$$p(S \backslash ((I, H, 1) \cup (1, H, J))) \subseteq M.$$

Let us choose an arbitrary

$$(i_0, h_0, j_0) \in p(S \backslash ((I, H, 1) \cup (1, H, J))).$$

By Theorem 1.1 we have $p((1, H, 1)) = (1, H'h_1, 1)$ for some $h_1 \in H$, and so

$$p(S) \supseteq (1, H'h_1, 1)(i_0, h_0, j_0)p((I^*, H, 1) \cup (1, H, J^*)). \tag{6}$$

We next show that the right hand side of (6) contains the coset $H'Th_0h_1^{|I|+|J|-1}$ of $H'T$. Recall that T is generated by the conjugates of the elements p_{ji}. It is easy to see that every element of T can be written as a product of these conjugates of length less than $|T|$. It then follows that every element of $H'Th_0h_1^{|I|+|J|-1}$ can be written as

https://doi.org/10.1017/S0013091500020514 Published online by Cambridge University Press

$$h'\left(\prod_{i\in I^*}\prod_{j\in J^*} p_{ji}^{\alpha_{ji}}\right)h_0 h_1^{|I|+|J|-1}, \tag{7}$$

where $h' \in H'$ and α_{ji} are non-negative integers such that

$$\sum_{i\in I^*}\sum_{j\in J^*}\alpha_{ji} < |H|. \tag{8}$$

(Here, and throughout this section, we adopt the following convention regarding sums and products. Whenever we have an expression $\sum_{x\in X} f(x)$ or $\prod_{x\in X} f(x)$, we take an arbitrary ordering for X, which we consider fixed from then on, and take all summations and products over X with respect to that fixed ordering.)

From (8) it follows that there exist disjoint subsets H_{ji} ($j \in J^*, i \in I^*$) of H such that

$$|H_{ji}| = \alpha_{ji}.$$

For brevity of notation in what follows, for each $i \in I^*$ and each $j \in J^*$ we define

$$H_i^* = H\setminus\bigcup_{j\in J^*} H_{ji},\ H_j^* = H\setminus\bigcup_{i\in I^*} H_{ji}.$$

Now the product

$$\left[\prod_{j\in J^*}\prod_{h\in H_j^*}(1,h,j)\right]\left[\prod_{i\in I^*}\prod_{j\in J^*}\prod_{h\in H_{ji}}(1,h,j)(i,h,1)\right]\left[\prod_{i\in I^*}\prod_{h\in H_i^*}(i,h,1)\right]$$

$$=\left(1,\left[\prod_{j\in J^*}\prod_{h\in H_j^*}h\right]\left[\prod_{i\in I^*}\prod_{j\in J^*}\prod_{h\in H_{ji}}hp_{ji}h\right]\left[\prod_{i\in I^*}\prod_{h\in H_i^*}h\right],1\right)$$

belongs to $p((I^*,H,1)\cup(1,H,J^*))$, and hence the right hand side of (6) contains the set

$$\begin{aligned}&\left(1,H'h_1h_0\left[\prod_{j\in J^*}\prod_{h\in H_j^*}h\right]\left[\prod_{i\in I^*}\prod_{j\in J^*}\prod_{h\in H_{ji}}hp_{ji}h\right]\left[\prod_{i\in I^*}\prod_{h\in H_i^*}h\right],1\right)\\ &=\left(1,H'h_1h_0\left(\prod_{h\in H}h\right)^{|I^*|+|J^*|}\prod_{i\in I^*}\prod_{j\in J^*}p_{ji}^{\alpha_{ji}},1\right).\end{aligned} \tag{9}$$

The product $\prod_{h\in H} h$ is a particular element of $p(H)$, and hence is equal to h_1 modulo H', so that the set (9) is equal to the set

https://doi.org/10.1017/S0013091500020514 Published online by Cambridge University Press

$$\left(1, H'\left(\prod_{i\in I'}\prod_{j\in J'} p_{ji}^{\alpha_{ji}}\right)h_0 h_1^{|I|+|J|-1}, 1\right),$$

which, in turn, contains the element (7), exactly as required.

We have proved that $p(S)\cap H$ contains a subset of size $|H'T|$. On the other hand, by (4), we already know that $p(S)\cap H$ is contained in such a set, namely in $H'Th$, so that we must have $p(S)\cap H = H'Th$. This completes the proof of the theorem.

REFERENCES

1. C. M. Campbell, E. F. Robertson, N. Ruškuc and R. M. Thomas, Semigroup and group presentations, *Bull. London Math. Soc.* **27** (1995), 46–50.

2. J. Dénes and P. Z. Hermann, On the product of all elements in a finite group, *Ann. Discrete Math.* **15** (1982), 105–109.

3. P. Z. Hermann, On the product of all nonzero elements of a finite ring, *Glasgow Math. J.* **30** (1988), 325–330.

4. J. M. Howie, *Fundamentals of Semigroup Theory* (Clarendon Press, Oxford, 1995).

P. Z. Hermann
Department of Algebra and Number Theory
Eötvös Loránd University
Múzeum krt. 6-8
Budapest
H-1088 Hungary
E-mail address: hp@cs.elte.hu

E. F. Robertson and N. Ruškuc
Mathematical Institute
University of St Andrews
St Andrews KY16 9SS
Scotland
E-mail addresses: efr@st-and.ac.uk,
nrl@st-and.ac.uk