BULL. AUSTRAL. MATH. SOC. 20M20
VOL. 71 (2005) [69–74]

THE STRUCTURE OF ELEMENTS IN FINITE FULL TRANSFORMATION SEMIGROUPS

GONCA AYIK, HAYRULLAH AYIK, YUSUF ÜNLÜ AND JOHN M. HOWIE

The *index* and *period* of an element a of a finite semigroup are the smallest values of $m \geqslant 1$ and $r \geqslant 1$ such that $a^{m+r} = a^m$. An element with index m and period 1 is called an *m-potent* element. For an element α of a finite full transformation semigroup with index m and period r, a unique factorisation $\alpha = \sigma\beta$ such that $\mathrm{Shift}(\sigma) \cap \mathrm{Shift}(\beta) = \emptyset$ is obtained, where σ is a permutation of order r and β is an m-potent. Some applications of this factorisation are given.

1. INTRODUCTION

The full transformation semigroup $\mathcal{T}_X$ on a set X, the semigroup analogue of the symmetric group $\mathcal{S}_X$, has been much studied over the last fifty years, in both the finite and the infinite cases. (See, for example [**10, 3**].) Here we are concerned solely with the case where $X = X_n = \{1, 2, \ldots, n\}$, and we denote the semigroup $\mathcal{T}_{X_n}$ of all self maps of X_n by T_n. For each $\alpha \in T_n$ we define $\mathrm{Fix}(\alpha)$ as $\{x \in X_n \mid x\alpha = x\}$, and we denote $X_n \setminus \mathrm{Fix}(\alpha)$ by $\mathrm{Shift}(\alpha)$.

Let S be a semigroup and $a \in S$. If there exist $m, r \in \mathbb{Z}^+$ such that $a^{m+r} = a^m$ and $a, a^2, \ldots, a^{m+r-1}$ are pairwise distinct, then a is called an (m, r)*-potent* element of S, and we say that a has *index* m and *period* r. In particular, if $r = 1$, then a is called an *m-potent*, and if $m = r = 1$ then a is called an *idempotent*.

The aim of this paper is to describe a natural factorisation of (m, r)-potent elements in T_n and to give some applications of this factorisation.

For undefined terms in semigroup theory, see [**4**].

2. ORBITS

Let $\alpha \in T_n$. The equivalence relation $\equiv$ on X_n, defined by

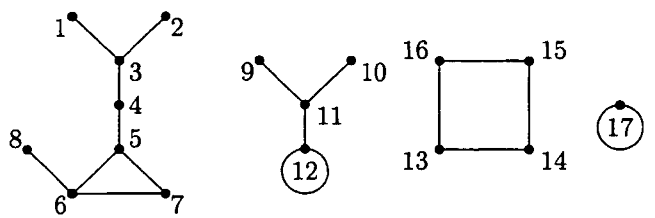
$$x \equiv y \text{ if and only if } (\exists r, s \geqslant 0)\, x\alpha^r = x\alpha^s,$$

Received 23rd August, 2004
The fourth author acknowledges with thanks the grant from TÜBİTAK that enabled him to visit Adana.

partitions X_n into *orbits* $\Omega_1, \Omega_2, \ldots, \Omega_k$. The orbits are the connected components of the function graph, and provide valuable information about the structure of the map α. Typically, an orbit consists of a cycle with some trees attached. If there are no attached trees, we say that the orbit Ω_i is *cyclic*, if the cycle is trivial (consisting of a single fixed point) and $|\Omega_i| \geqslant 2$ we say that Ω_i is *acyclic*; if Ω_i consists of a single fixed point, we say that it is *trivial*. An example will clarify the ideas. Let $n = 17$ and let α be the map

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 3 & 3 & 4 & 5 & 6 & 7 & 5 & 6 & 11 & 11 & 12 & 12 & 14 & 15 & 16 & 13 & 17 \end{pmatrix}.$$

The orbits of α (with the convention that arrows point towards the cycle or fixed point, and that arrows go counterclockwise within the cycles) can be depicted thus:

(1) 

In [**1**], three of the present authors described and made use of a 'linear' notation (a modification of Lipscomb's notation [**6**]) for elements of T_n, in which the map depicted above appears as

[1 3 4 5 6 7 | 5] [13 14 15 16 | 13] [9 11 12 | 12] [2 3 | 3][8 6 | 6] [10 11 | 11].

It would be possible to rewrite this article using that notation, but the way in which it mixes the orbits makes the arguments more difficult and less transparent.

In the general case it is clear that, for each x in X_n, the sequence

$$x, x\alpha, x\alpha^2, \ldots$$

eventually arrives in a cycle (or a fixed point, which of course we may regard as a special case of a cycle) and remains there for all subsequent iterations. Denote the set of all elements contained in cycles by $Z(\alpha)$. (In our example, $Z(\alpha) = \{5, 6, 7, 12, 13, 14, 15, 16, 17\}$.) The index m of α is the length of the longest path into $Z(\alpha)$, and the period r is the least common multiple of the lengths of the cycles. (In our example, we have $m = 3$ and $r = 12$.)

It is clear also that the element α is m-potent if and only if $Z(\alpha)$ consists solely of fixed points and there exists y in X_n such that

$$y\alpha^m \in Z(\alpha), \quad y\alpha^{m-1} \notin Z(\alpha).$$

The largest m that can occur is $n - 1$; this happens, for example, if $x\alpha = x + 1$ for $x = 1, 2, \ldots, n - 1$ and $n\alpha = n$.

3. The factorisation of (m,r)-potents

Let $ST_n = T_n \setminus S_n$, the full singular transformation semigroup of degree n, and let $\alpha \in ST_n$ be m-potent: Thus $\alpha^{m+1} = \alpha^m$, and $\alpha^{q+1} \neq \alpha^q$ for all $q < m$. For each x in X_n, let m_x be the least integer such that $x\alpha^{m_x} \in Z(\alpha)$, and, for $j = 0, 1, \ldots, m$, let $A_j = \{x \in X_n \mid m_x = j\}$. It is evident that $A_0 = Z(\alpha)$, and that the sets $A_0, A_1, \ldots, A_m$ are mutually disjoint. It is clear too that $\bigcup_{j=0}^{m} A_j = X_n$, since, for all x in X_n, the sequence $x, x\alpha, x\alpha^2, \ldots$ must reach $Z(\alpha)$ in at most m steps. Finally, we see that the sets are all non-empty, since there exists y in A_m, and $y\alpha^{m-j} \in A_j$ for $j = 0, 1, \ldots, m-1$. We have proved the following theorem:

Theorem 1. *With the above definitions, $(A_0, A_1, \ldots, A_m)$ is a partition of the set X_n.*

For example, if α is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 3 & 4 & 5 & 5 & 8 & 8 & 10 & 10 & 10 & 11 \end{pmatrix},$$

then

$$A_0 = \{5, 10, 11\}, \quad A_1 = \{4, 8, 9\}, \quad A_2 = \{3, 6, 7\}, \quad A_3 = \{1, 2\}.$$

Let $\alpha \in T_n$ have index m and period r. Suppose that there are k orbits $\Omega_1, \Omega_2, \ldots, \Omega_k$ and that, for each j in $\{1, 2, \ldots, k\}$, the map $\alpha_j = \alpha|_{\Omega_j}$ has index m_j and period r_j. We have already observed that $m = \max\{m_1, m_2, \ldots, m_k\}$ and r is the lowest common multiple of $r_1, r_2, \ldots, r_k$.

Let $j \in \{1, 2, \ldots, k\}$. For each element a in $Z(\alpha_j)$ there is an associated vertex set $T_j(a)$ of a tree, defined by the property that $x \in T_j(a)$ if and only if either $x = a$, or there is a sequence $x, x\alpha, x\alpha^2, \ldots$ such that, for some $u \geqslant 1$,

$$x\alpha^v \in X_n \setminus Z(\alpha_j) \text{ for } 0 \leqslant v < u, \text{ and } x\alpha^u = a.$$

(That is a rather cumbersome explanation of a simple idea: in our first example, we have

$$T_1(5) = \{1, 2, 3, 4, 5\}, \quad T_1(6) = \{8, 6\}, \quad T_1(7) = \{7\}.)$$

Notice that $\bigcup_{a \in Z(\alpha_j)} T_j(a) = \Omega_j$. We then define β_j on the set Ω_j by

$$x\beta_j = \begin{cases} x\alpha_j & \text{if } x \notin Z(\alpha_j) \\ x & \text{otherwise,} \end{cases}$$

and define a permutation σ_j on Ω_j by

$$x\sigma_j = \begin{cases} x\alpha_j & \text{if } x \in Z(\alpha_j) \\ x & \text{otherwise.} \end{cases}$$

Then β_j is an m_j-potent, σ_j is a cycle of length (and order) r_j, and $\sigma_j\beta_j = \alpha_j$. From the definitions it is clear also that $\operatorname{Shift}(\sigma_j) \cap \operatorname{Shift}(\beta_j) = \emptyset$.

Since the orbits are mutually disjoint, we can conclude that $\alpha = \sigma\beta$, where $\sigma = \sigma_1\sigma_2\ldots\sigma_k$, $\beta = \beta_1\beta_2\ldots\beta_k$ and $\operatorname{Shift}(\sigma) \cap \operatorname{Shift}(\beta) = \emptyset$. Then σ is a permutation of order $r = \operatorname{lcm}(r_1, r_2, \ldots, r_k)$ and β is an m-potent, with $m = \max\{m_1, m_2, \ldots, m_k\}$.

We have proved the following result:

Theorem 2. *Let α be an element of T_n of index m and period r. Then there exist a permutation σ of order r and an m-potent element β such that $\alpha = \sigma\beta$ and* $\operatorname{Shift}(\sigma) \cap \operatorname{Shift}(\beta) = \emptyset$.

We have the following converse result:

Theorem 3. *Let σ be a permutation of order r and let β be an m-potent such that* $\operatorname{Shift}(\sigma) \cap \operatorname{Shift}(\beta) = \emptyset$. *Let $\alpha = \sigma\beta$. Then*

(i) *α has index m and period r;*

(ii) *$\operatorname{im}(\alpha^m)$ is the disjoint union of* $\operatorname{Shift}(\sigma)$ *and* $\operatorname{Fix}(\alpha)$.

Proof: (i) Observe first that, for all x in X_n,

$$x \in \operatorname{Shift}(\beta) \Rightarrow x\sigma\beta = x\beta\,, \quad x \in \operatorname{Shift}(\sigma) \Rightarrow x\sigma\beta = x\sigma\,. \tag{2}$$

Consider the orbits of σ and β. If the orbit Ω_j of β is entirely contained in $\operatorname{Fix}(\sigma)$, then $x(\sigma\beta)^q = x\beta^q$ for all x in Ω_j and for all q. The other possibility is that the fixed point of Ω_j is in a non-singleton orbit Λ_j of σ. If $x \in \Omega_j$ is such that $x\beta^{q+1} = x\beta^q$ ($q \geqslant 1$), then $x, x\beta, x\beta^2, \ldots, x\beta^{q-1} \in \operatorname{Fix}(\sigma)$, and so $x(\sigma\beta)^q = x\beta^q$. If $\sigma|_{\Lambda_j}$ is a cycle of length $s > 1$, then $x\beta^q\sigma, x\beta^q\sigma^2, \ldots \in \operatorname{Fix}(\beta)$, and so $x(\sigma\beta)^{q+t} = x\beta^q\sigma^t$ for all t. It follows that $x(\sigma\beta)^{q+s} = x(\sigma\beta)^q$ and that no smaller q and s will suffice.

We carry this out for each orbit Ω_j in turn, and obtain the orbital structure of $\sigma\beta$. The longest path into $Z(\sigma\beta)$ is determined by the corresponding path for β, and the (non-trivial) cycles are the same as those for σ. We deduce that $\sigma\beta$ has index m and period r. (Graphically, the strategy of the above proof is easy to visualise: at each point z in $\operatorname{Shift}(\sigma) \cap \operatorname{Fix}(\beta)$ the tree ending in z is simply 'tacked on' to the cycle.)

(ii) If β is the identity map (in which case $m = 1$), then the result is obvious. We suppose that β is not the identity map. Suppose first that $z \in \operatorname{im}(\alpha^m)$. In the notation of Theorem 1, let $x \in A_j$ for some j in $\{1, 2, \ldots, m\}$, so that $x, x\beta, \ldots, x\beta^{j-1} \in \operatorname{Shift}(\beta)$ and $x\alpha^j = x\beta^j \in \operatorname{Shift}(\sigma) \cup \operatorname{Fix}(\alpha)$. Certainly $x\alpha^m \in \operatorname{Shift}(\sigma) \cup \operatorname{Fix}(\alpha)$.

Conversely, suppose that $z \in \operatorname{Shift}(\sigma) \cup \operatorname{Fix}(\alpha)$. If $z \in \operatorname{Fix}(\alpha)$, then

$$z = z\alpha = \cdots = z\alpha^m \in \operatorname{im}(\alpha^m)\,.$$

If $z \in \operatorname{Shift}(\sigma)$, then $z\sigma^{-m} \in \operatorname{Shift}(\sigma)$, and so, by (2),

$$z = (z\sigma^{-m})\sigma^m = (z\sigma^{-m})\alpha^m \in \operatorname{im}(\alpha^m)\,.$$

It is clear that the union $\mathrm{Shift}(\sigma) \cup \mathrm{Fix}(\alpha)$ is disjoint. □

We are ready now to prove our main result:

Theorem 4. *Let α be an element of T_n. Then α is an (m,r)-potent if and only if there exist a unique permutation σ of order r and a unique m-potent element β such that $\alpha = \sigma\beta$ and $\mathrm{Shift}(\sigma) \cap \mathrm{Shift}(\beta) = \emptyset$.*

Proof: From Theorems 2 and 3 it is enough to show that the factorisation of α given by Theorem 2 is unique. Let $\alpha = \sigma_1\beta_1 = \sigma_2\beta_2$ where σ_j is a permutation of order r_j and β_j is an m_j-potent such that $\mathrm{Shift}(\sigma_j) \cap \mathrm{Shift}(\beta_j) = \emptyset$ for $j = 1, 2$. It follows from Theorem 3 that α has index m_j and period r_j for $j = 1, 2$. Hence $m_1 = m_2$ and $r_1 = r_2$. Moreover, it follows from Theorem 3(ii) that $\mathrm{Shift}(\sigma_1) = \mathrm{im}(\alpha^m) \setminus \mathrm{Fix}(\alpha) = \mathrm{Shift}(\sigma_2)$. Since, for all z in $\mathrm{Shift}(\sigma_j)$,

$$z\alpha = z\sigma_j\beta_j = z\sigma_j\ ,$$

it follows that $\sigma_1 = \sigma_2$, and it then follows immediately that $\beta_1 = \beta_2$. □

It is important to note that the uniqueness of the factorisation depends upon the condition $\mathrm{Shift}(\sigma) \cap \mathrm{Shift}(\beta) = \emptyset$. For example, we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix}.$$

4. Applications

The numbers of some kinds of elements in T_n are known (see, for example [**2, 7, 8, 9**]). By using Theorem 1, we can obtain a formula for the number of m-potents in T_n as well. The number of partitions of n into $m+1$ parts is also the number of equivalences on the set X_n having $m+1$ classes; this is the Stirling number $S(n, m+1)$ of the second kind. (See, for example, [**5**], where the relevance of Stirling numbers to semigroup theory is made clear.) Denote the set of partitions of n into $m+1$ non-zero parts by $P_{m+1}(n)$. Given a partition $k_0, k_1, \dots, k_m$ of n, we can assign sets $A_0, A_1, \dots, A_m$, with $|A_j| = k_j$ for each j, in

$$\binom{n}{k_0, k_1, \dots, k_m}$$

ways. Each element of A_1 must map to elements of A_0 and there are $|A_1|^{|A_0|}$ ways in which this can happen. Similarly, there are $|A_2|^{|A_1|}$ ways in which the elements of A_2 can map into A_1. Continuing in this way, we obtain the following theorem:

Theorem 5. *The number of m-potent elements ($m = 1, 2, \dots, n-1$) in ST_n is*

$$\sum_{(k_0,k_1,\dots,k_m)\in P_{m+1}(n)} \binom{n}{k_0, k_1, \dots, k_m} k_1^{k_0} k_2^{k_1} \dots k_m^{k_{m-1}}\ .$$

Let $\tau(k,r)$ denote the number of permutations of k elements of order r. Since $(0,r)$-potent elements are permutations, we only take into account (m,r)-potent elements with $m \geqslant 1$ in the following theorem.

THEOREM 6. *Let $m \geqslant 1$ and $r \geqslant 1$. Then the number of (m,r)-potent elements in ST_n is*

$$\sum_{(k_0,k_1,\ldots,k_m)\in P_{m+1}(n)} \binom{n}{k_0, k_1, \ldots, k_m} k_1^{k_0} k_2^{k_1} \ldots k_m^{k_{m-1}} \tau(k_0, r) .$$

PROOF: We know that each (m,r)-potent element can be uniquely written as $\sigma\beta$ where σ is a permutation of order r and β is an m-potent element and $\mathrm{Fix}(\sigma) \cup \mathrm{Fix}(\beta) = X_n$.

Let $(A_0, A_1, \ldots, A_m)$ be a partition of X_n with $|A_i| = k_i$ $(i = 0, 1, \ldots, m)$, and let $\kappa = \kappa(A_0, A_1, \ldots, A_m)$ denote the set of all m-potent elements in T_n with corresponding partition $(A_0, A_1, \ldots, A_m)$, as in Theorem 1. For each $\beta \in \kappa$ we have $\mathrm{Fix}(\beta) = A_0$. Since, by Theorem 2, $\mathrm{Shift}(\sigma) \subseteq A_0$, there are $\tau(k_0, r)$ permutations of order r in T_n having $\mathrm{Shift}(\sigma) \subseteq A_0$. Similarly, the result follows from Theorem 4, as required. ∎

REFERENCES

[1] G. Ayık, H. Ayık and J.M. Howie, 'On factorisations and generators in transformation semigroups', *Semigroup Forum* (to appear).

[2] B. Harris and L. Schoenfeld, 'The number of idempotents in symmetric semigroup', *J. Combinatorial Theory* **3** (1967), 122–135.

[3] J.M. Howie, 'The subsemigroup generated by the idempotents of a full transformation semigroup', *J. London Math. Soc.* **41** (1966), 707–716.

[4] J.M. Howie, *Fundamentals of semigroup theory*, London Mathematical Society Monographs **12** (Oxford University Press, New York 1995).

[5] J.M. Howie and R.B. McFadden, 'Idempotent rank in finite full transformation semigroups', *Proc. Royal Soc. Edinburgh Sect. A* **114** (1990), 161–167.

[6] S. Lipscomb, *Symmetric inverse semigroups*, Math. Surveys and Monographs **46** (American Math. Soc., Providence, R.I., 1996).

[7] J. Riordan, 'Forests of labeled trees', *J. Combinatorial Theory* **5** (1968), 90–103.

[8] V.N. Sachkov, *Combinatorial methods in discrete mathematics* (Cambridge University Press, Cambridge, 1996).

[9] F.M. Sioson, 'Counting elements in semigroups', *J. Combinatorial Theory* **12** (1972), 339–345.

[10] N.N. Vorob'ev, 'On symmetric associative systems', (Russian), *Leningrad. Gos. Ped. Inst. Uc. Zap.* **89** (1953), 161–166.

Department of Mathematics
Çukurova University
Adana
Turkey
e-mail: hayik@mail.cukurova.edu.tr

Mathematical Institute
University of St Andrews
North Haugh, St Andrews
Fife KY16 9SS
United Kingdom
e-mail: jmh@st-and.ac.uk