PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 11, Pages 3345–3351
S 0002-9939(03)06920-X
Article electronically published on February 14, 2003

THE CLASS EQUATION AND COUNTING IN FACTORIZABLE MONOIDS

S. LIPSCOMB AND J. KONIECZNY

(Communicated by Stephen D. Smith)

ABSTRACT. For orders and conjugacy in finite group theory, Lagrange's Theorem and the class equation have universal application. Here, the class equation (extended to monoids via standard group action by conjugation) is applied to factorizable submonoids of the symmetric inverse monoid. In particular, if M is a monoid induced by a subgroup G of the symmetric group S_n, then the center $Z_G(M)$ (all elements of M that commute with every element of G) is $Z(G) \cup \{0\}$ if and only if G is transitive. In the case where G is both transitive and of order either p or p^2 (for p prime), formulas are provided for the order of M as well as the number and sizes of its conjugacy classes.

1. INTRODUCTION

In this paper, we study monoids of restrictions of permutations under function composition. Indeed, for each subgroup G of the symmetric group S_n of all permutations of $N = \{1, 2, \ldots, n\}$, we define the induced monoid

$$M(G) = \{\alpha \ : \ \alpha \text{ is a restriction of some } \sigma \in G\}$$

whose multiplication is function composition. These monoids are *inverse* (for each $\alpha \in M(G)$, there is a unique $\beta \in M(G)$ satisfying $\alpha = \alpha\beta\alpha$ and $\beta = \beta\alpha\beta$) and *factorizable* (each $\alpha \in M(G)$ factors $\alpha = \varepsilon\sigma$ where ε is an idempotent and $\sigma \in G$ is a unit). In the special case $G = S_n$, the induced monoid $M(S_n)$ is denoted C_n, and it is widely known as the *symmetric inverse monoid*.

Abstract factorizable inverse monoids have been studied by Chen and Hsieh [1]. The definition of the property of being factorizable (given originally for inverse monoids) has been generalized to arbitrary semigroups: A semigroup S is called factorizable if $S = GE$ for some subgroup G of S and some set E of idempotents of S [7]. For example, the semigroup PT_X of all partial transformations on a set X is factorizable if and only if X is finite [7]. A similar result holds for the semigroup T_X of all full transformations on X [7] and the symmetric inverse semigroup I_X of all partial one-to-one transformations on X [1].

In the present paper, for various kinds of subgroups G of S_n, we study the induced submonoids $M(G)$ of C_n. In Section 2 we provide definitions, in Section 3

Received by the editors April 12, 2002 and, in revised form, June 5, 2002.
2000 *Mathematics Subject Classification.* Primary 20M20, 20M15.
Key words and phrases. Factorizable monoids, symmetric inverse semigroups, class equation, conjugacy classes, permutation groups, transformation semigroups.

we consider orders $|M(G)|$, and in Section 4, using the class equation for finite monoids, we investigate conjugacy classes.

2. Basic definitions

Let M be a monoid with the identity 1. Then $u \in M$ is a *unit* when $v \in M$ exists such that $uv = vu = 1$. If such a v exists, it is unique and denoted u^{-1}. The subset $G \subseteq M$ of all units is a subgroup of M, called the *group of units* of M. For example, S_n is the group of units of $M(S_n) = C_n$. The monoid C_n is of particular importance because every finite inverse monoid is isomorphic to a submonoid of C_n for some n [2, Theorem 5.1.7]. The elements of C_n are partial one-to-one transformations on N, they are sometimes called *charts* [6], and the domain and range of the chart α are denoted, respectively, $\mathbf{d}\alpha$ and $\mathbf{r}\alpha$.

An element b of a monoid M is called an *inverse* of $a \in M$ if $a = aba$ and $b = bab$. When each $a \in M$ has exactly one inverse, then M is an *inverse monoid*. For example, C_n is an inverse monoid since the required unique inverse of $\alpha \in C_n$ is α^{-1}.

Every inverse monoid M has a *natural partial order* given by $a \leq b$ whenever an idempotent $e \in M$ exists such that $a = eb$ [2, p. 152]. An inverse monoid M is *factorizable* when each $a \in M$ is "under" a unit $u \in M$, i.e., $a \leq u$ [4]. In other words, an inverse monoid M is factorizable if every element of M can be factored as a product of an idempotent and a unit. For example, C_n is factorizable: For each idempotent $\varepsilon \in C_n$ and each $x \in N$, either $x\varepsilon = x$ or $x\varepsilon$ is not defined, i.e., ε is completely determined by its domain. So for $A \subseteq N$, ε_A will denote the idempotent in C_n with domain A. Next, for a unit $\sigma \in S_n$, the element $\varepsilon_A\sigma \in C_n$ is a restriction of σ to A. Indeed, every $\alpha \in C_n$ is a restriction of some unit $\sigma \in S_n$ to $A = \mathbf{d}\alpha$. It follows that C_n is a factorizable inverse monoid.

We shall use "$G \leq S_n$" to indicate that G is a subgroup of S_n. It is easy to see that the induced monoid $M(G)$ is an inverse submonoid of C_n. And since $M(G)$ consists of all elements of the form $\varepsilon\sigma$ where $\varepsilon \in C_n$ is idempotent and $\sigma \in G$, it is factorizable. In fact, $M(G)$ is the largest (with respect to inclusion) factorizable submonoid of C_n that has G as its group of units.

For $G \leq S_n$ and $A \subseteq N$, the *stabilizer* G_A of A consists of all $\sigma \in G$ such that $x\sigma = x$ for every $x \in A$. If $A = \{x\}$, we write $G_A = G_x$ and call G_x the stabilizer of x. It is clear that G_A is a subgroup of G. A subgroup $G \leq S_n$ is *balanced* if for all subsets $A, B \subseteq N$ of the same cardinality, we have $|G_A| = |G_B|$. For example, S_n and its alternating subgroup A_n are balanced, while the cyclic subgroup $G = \langle(1\ 2)\rangle$ generated by the 2-cycle (12) in S_4 is not balanced. A group $G \leq S_n$ is *transitive* if for all $x, y \in N$, a $\sigma \in G$ exists such that $y = x\sigma$; *semiregular* if $G_x = \{1\}$ for each $x \in N$; and *regular* if it is both semiregular and transitive. Note that every semiregular group G is balanced since $G_A = \{1\}$ for every non-empty $A \subseteq N$.

For abstract monoids M, we say $b \in M$ is *conjugate* to $a \in M$ if $b = u^{-1}au$ for some unit $u \in M$. The subset $[a]$ of all elements of M conjugate to a is the *conjugacy class* of a; and $\{\,[a] : a \in M\}$ is a partition of M.

For each set $A \subseteq N$, let $R_A^M = \{\,\varepsilon_A\sigma : \sigma \in G\,\}$ denote the set of all elements in $M = M(G)$ that have domain A. (The set R_A^M is a Green's $\mathcal{R}$-class of M; see [2, p. 45] for the definition of *Green's relations*.) Note that if $A = \emptyset$, then $R_A^M = \{0\}$, where 0 is the empty (or zero) transformation on N.

3. Order of $M(G)$

The next lemma is crucial in proving the counting theorems of this section.

Lemma 3.1. *Let $G \leq S_n$ and $M = M(G)$. For each $A \subseteq N$,*

$$|R_A^M| = \frac{|G|}{|G_A|}.$$

Proof. Define $f : R_A^M \to G/G_A$ by $f(\varepsilon_A\sigma) = G_A\sigma$. Then f is well-defined and one-to-one since for all $\sigma, \rho \in G$,

$$\varepsilon_A\sigma = \varepsilon_A\rho \Leftrightarrow \varepsilon_A = \varepsilon_A\rho\sigma^{-1} \Leftrightarrow \rho\sigma^{-1} \in G_A \Leftrightarrow \rho \in G_A\sigma \Leftrightarrow G_A\sigma = G_A\rho.$$

Since the function f is clearly onto, it follows that $|R_A^M|$ is the number $|G|/|G_A|$ of right cosets of G_A in G. □

The next three theorems give, respectively, formulas for orders of monoids induced by balanced, semiregular, and transitive abelian groups. Let $k \in \{0, 1, \ldots, n\}$. Then $C(n, k)$ denotes "n choose k" (the number of k-element subsets of N), and for a balanced group $G \leq S_n$, m_k denotes $|G_{\{1,\ldots,k\}}|$. That is, m_k is the size of the stabilizer G_A for any k-element set $A \subseteq N$. Note that $G_\emptyset = G$ and so $m_0 = |G|$.

Theorem 3.2. *Let $G \leq S_n$ be balanced and $M = M(G)$. Then*

$$|M| = |G| \sum_{k=0}^{n} \frac{C(n, k)}{m_k}.$$

Proof. When $A, B \subseteq N$ are distinct, R_A^M and R_B^M are disjoint (the domain of any $\varepsilon_A\sigma \in R_A^M$ is A). So for each $k \in \{0, 1, \ldots, n\}$, there are $C(n, k)$ pairwise disjoint sets R_A^M with $|A| = k$. But since G is balanced, Lemma 3.1 shows that each set R_A^M with $|A| = k$ has $|G|/|G_A| = |G|/m_k$ elements. Thus, M has $C(n, k)(|G|/m_k)$ elements with domains of size k. The result follows. □

To illustrate Theorem 3.2, first suppose $G = S_n$. Then $M = C_n$ and $m_k = (n - k)!$ for every k, showing that

$$|C_n| = n! \sum_{k=0}^{n} \frac{C(n, k)}{(n - k)!}.$$

Second, suppose $G = A_n$. Then $M = A_n^c$, the alternating monoid. (The monoid A_n^c, which is a natural extension of the alternating group, was discovered by the first author [5].) For $G = A_n$, we have $m_k = 1$ (if $k \geq n - 1$) and $m_k = \frac{(n-k)!}{2}$ (if $k \leq n - 2$). Thus

$$|A_n^c| = \frac{n!}{2} \sum_{k=0}^{n-2} \frac{C(n, k)}{\frac{(n-k)!}{2}} + \frac{n!}{2} C(n, n - 1) + \frac{n!}{2} C(n, n) = n! \sum_{k=0}^{n-2} \frac{C(n, k)}{(n - k)!} + \frac{(n + 1)!}{2}.$$

The next theorem is an immediate consequence of Theorem 3.2 because when G is semiregular, it is balanced, $m_0 = |G|$, and $m_k = 1$ for each $k = 1, 2, \ldots, n$.

Theorem 3.3. *Let $G \leq S_n$ be semiregular and $M = M(G)$. Then*

$$|M| = |G|(2^n - 1) + 1.$$

If $G \leq S_n$ is semiregular, then every non-zero $\alpha \in M(G)$ can be expressed *uniquely* as $\alpha = \varepsilon_A \sigma$ where $A = \mathbf{d}\alpha$ and $\sigma \in G$. Indeed, $\alpha = \varepsilon_A \sigma$ for some $\sigma \in G$ by the definition of $M(G)$. Suppose $\varepsilon_A \sigma = \varepsilon_A \delta$ where $\sigma, \delta \in G$. Then $\varepsilon_A \sigma \delta^{-1} = \varepsilon_A$ and so $\sigma\delta^{-1}$ fixes every $x \in A$. It follows that $\sigma\delta^{-1} = 1$ (since $A \neq \emptyset$ and $G_x = \{1\}$ for every $x \in N$), and so $\sigma = \delta$.

Note that the observation above provides another proof of Theorem 3.3: To construct a non-zero $\alpha = \varepsilon_A \sigma \in M(G)$, we have $2^n - 1$ choices for A and $|G|$ choices for σ.

For the next theorem, recall that the *degree* of $G \leq S_n$ is the number of points $x \in N$ such that $x\sigma \neq x$ for some $\sigma \in G$ (the number of points that are moved by G). For example, the degree of A_n is n if $n > 1$.

Theorem 3.4. *Let $G \leq S_n$ be both transitive and abelian, and $M = M(G)$. Then*

$$|M| = |G|(2^{|G|} - 1) + 1.$$

Proof. Since G is transitive and abelian, G is regular [8, Proposition 4.4]. Thus, by Theorem 3.3, $|M| = |G|(2^n - 1) + 1$. Since G is regular, its degree and order are equal [8, Proposition 4.2]. But the degree of G is n since a transitive group moves every point. Thus $n = |G|$ and so $|M| = |G|(2^{|G|} - 1) + 1$. □

Corollary 3.5. *Let $G \leq S_n$ be transitive, $M = M(G)$, and p be a prime. Then:*

1. *If $|G| = p$, then $|M| = p(2^p - 1) + 1$.*
2. *If $|G| = p^2$, then $|M| = p^2(2^{p^2} - 1) + 1$.*

Proof. The proof follows immediately from Theorem 3.4 and the fact that every group of order p or p^2 is abelian. □

4. Conjugacy classes

Let M be any monoid with G its group of units. Then a singleton set $\{x\}$ is a conjugacy class if and only if x commutes with every $u \in G$. It follows that the *center*

$$Z_G(M) = \{\, x \in M : xu = ux \text{ for every } u \in G \,\}$$

of M relative to G, which is a submonoid of M, counts the singleton conjugacy classes (just as the center $Z(G)$ of G counts the singleton conjugacy classes in the group case). Moreover, $Z_G(M)$ is an inverse submonoid of M when M is an inverse monoid, and $Z_G(M) = Z(G)$ when $M = G$ is a group.

As in the group theory case, we use centralizers to count elements in non-singleton conjugacy classes. For $x \in M$, we denote by $C_G(x)$ the *centralizer of x in G*, which is defined as the set of all members of G that commute with x. It is clear that the centralizer $C_G(x)$ is a subgroup of G.

For any finite group G, its *class equation* is

$$|G| = |Z(G)| + \sum_i [G : C_G(a_i)]$$

where one $a_i \in G$ is chosen from each conjugacy class in G containing more than one element [3, (42′), p. 76]. The class equation for finite groups is a special case of the class equation for finite monoids.

Theorem 4.1. *Let M be a finite monoid and let G be its group of units. Then*

$$|M| = |Z_G(M)| + \sum_i [G : C_G(x_i)] \tag{1}$$

where one $x_i \in M$ is chosen from each conjugacy class in M containing more than one element.

Proof. By the definition of $Z_G(M)$, $|Z_G(M)|$ is the number of singleton conjugacy classes. Let $x \in M$ be chosen from a conjugacy class $[x]$ containing more than one element, and let $H = C_G(x)$. It suffices to show that the number $|[x]|$ of conjugates of x is equal to $[G : H]$. To this end, define $f : [x] \to G/H$ by $f(u^{-1}xu) = Hu$. The function f is well-defined and one-to-one since

$$u^{-1}xu = v^{-1}xv \Leftrightarrow xuv^{-1} = uv^{-1}x \Leftrightarrow uv^{-1} \in C_G(x) = H \Leftrightarrow Hu = Hv.$$

Since f is clearly onto, $|[x]| = [G : H]$. □

Note that the class equation (1) is a special case of a more general formula enumerating the elements of a finite set S on which an action of a finite group G is defined [3, (40), p. 76]. In particular, the action underlying Theorem 4.1 is that of G acting on M by conjugation.

Corollary 4.2. *Let M be a finite monoid and let G be its group of units. Then the order of each conjugacy class of M divides the order of G.*

Proof. Let $x \in M$. By the proof of Theorem 4.1, $|[x]|$ is equal to $[G : C_G(x)]$, which divides $|G|$. □

In passing, we observe that for any $u \in G$, we have $x \in G$ if and only if $u^{-1}xu \in G$. It follows that each conjugacy class of M is either a subset of G or of $M - G$. In other words, the set of conjugacy classes of a finite monoid refines the doubleton partition $\{G, M - G\}$ of M.

We shall now investigate the center $Z_G(M)$ of a submonoid M of C_n induced by its group of units G. The next theorem shows that only special elements of a monoid M induced by $G \leq S_n$ can be members of $Z_G(M)$. A subset $A \subseteq N$ is called *invariant under* G if $A\sigma \subseteq A$ for every $\sigma \in G$.

Theorem 4.3. *Let $G \leq S_n$ and $M = M(G)$. Let $\alpha \in Z_G(M)$ with $A = \mathbf{d}\alpha$. Then A is invariant under G and α is a permutation on A.*

Proof. Since $A = \mathbf{d}\alpha$, we have $\alpha = \varepsilon_A\sigma$ for some $\sigma \in G$. Let ρ be any element of G. Since $\alpha \in Z_G(M)$, we have $\varepsilon_A\sigma\rho = \rho\varepsilon_A\sigma$. Let $x \in A$. Then $x(\varepsilon_A\sigma\rho)$ is defined, and so $x(\rho\varepsilon_A\sigma)$ is also defined. But the latter can happen only if $x\rho \in A$. Thus $A\rho \subseteq A$ and so A is invariant under G. In particular, $A\sigma \subseteq A$ and so $\alpha = \varepsilon_A\sigma$ is a permutation on A. □

For any $G \leq S_n$ and $M = M(G)$, we have $Z(G) \cup \{0\} \subseteq Z_G(M)$ where 0 is the zero transformation on N. The next theorem characterizes those groups G for which $Z_G(M) = Z(G) \cup \{0\}$, that is, $Z_G(M)$ is as small as possible.

Theorem 4.4. *Let $G \leq S_n$ and $M = M(G)$. Then $Z_G(M) = Z(G) \cup \{0\}$ if and only if G is transitive.*

Proof. Suppose G is transitive and $\alpha = \varepsilon_A\sigma \in Z_G(M) - (Z(G) \cup \{0\})$. Then A is a non-empty proper subset of N. Choose $x \in A$ and $y \in N - A$. Since G is transitive, there is $\rho \in G$ such that $x\rho = y$. Then $\alpha\rho = \rho\alpha$ implies that $x(\varepsilon_A\sigma\rho) = x(\rho\varepsilon_A\sigma) = y(\varepsilon_A\sigma)$. But this is a contradiction since $x(\varepsilon_A\sigma\rho)$ is defined and $y(\varepsilon_A\sigma)$ is undefined.

Conversely, suppose G is not transitive. Then for a fixed $x \in N$, let $A \subseteq N$ be the G-orbit of x, that is, $A = \{\, x\sigma : \sigma \in G \,\}$. Since G is not transitive, A is a proper subset of N, showing that the idempotent $\varepsilon_A \notin G \cup \{0\}$. In addition, since $A\sigma = A$ for each $\sigma \in G$, we have $\varepsilon_A\sigma = \sigma\varepsilon_A$ for each $\sigma \in G$. Thus $\varepsilon_A \in Z_G(M)$ and so $Z_G(M) \neq Z(G) \cup \{0\}$. □

For applications of the results above, we provide two theorems.

Theorem 4.5. *Let $G \leq S_n$ be transitive of order p, where p is a prime, and let $M = M(G)$. Then M has $p+1$ singleton conjugacy classes and 2^p-2 non-singleton classes, each of size p.*

Proof. Since G is transitive and abelian, Theorem 4.4 yields $Z_G(M) = Z(G)\cup\{0\} = G \cup \{0\}$. Thus M has $|G| + 1 = p + 1$ singleton conjugacy classes. For a non-singleton class $[\alpha]$, Corollary 4.2 shows that $|[\alpha]|$ divides $|G| = p$. Thus, every such class has size p. It follows that the number m of non-singleton classes satisfies $p+1+mp = |M|$. But this equation coupled with $|M| = (2^p-1)p+1$ (Corollary 3.5) shows that $m = 2^p - 2$. □

Theorem 4.6. *Let $G \leq S_n$ be transitive of order p^2, where p is a prime, and let $M = M(G)$. Then M has p^2+1 singleton conjugacy classes and $2^{p^2} + (q-1)2^p - 2q$ non-singleton classes where $q = p$ when G is cyclic and $q = p^2$ otherwise. Moreover, each non-singleton class is either of size p or size p^2:*

1. *If G cyclic, M has $p(2^p - 2)$ classes of size p and $2^{p^2} - 2^p$ of size p^2.*
2. *Otherwise, M has $p(p+1)(2^p - 2)$ classes of size p and $2^{p^2} - (p+1)2^p + 2p$ of size p^2.*

Proof. Since G is transitive, $Z_G(M) = Z(G) \cup \{0\}$ (Theorem 4.4), and since G is abelian, $Z(G) = G$. Thus M has $|G|+1 = p^2+1$ singleton conjugacy classes. For a non-singleton class $[\alpha]$, Corollary 4.2 shows that $|[\alpha]|$ divides $|G| = p^2$. Thus, every such class is either of order p or p^2. In addition, if $|[\alpha]| = p$, then $[G : C_G(\alpha)] = p$ (proof of Theorem 4.1), and so $|C_G(\alpha)| = p$.

Suppose $G = \langle\tau\rangle$ is cyclic. First, we count $\alpha \in M$ such that $|C_G(\alpha)| = p$, that is, $C_G(\alpha) = \langle\tau^p\rangle$, the unique subgroup of G of order p. Thus it suffices to count those $\alpha \in M - Z_G(M)$ that commute with τ^p. Note that τ^p is a product $\tau^p = \rho_1\rho_2\ldots\rho_p$ of p disjoint cycles, each of length p. By the observation after Theorem 3.3, α can be expressed uniquely as $\alpha = \varepsilon_A\sigma$, where $A \subseteq N$ and $\sigma = \tau^k \in G$ for some $k = 1, 2, \ldots, p^2$. We have that α commutes with τ^p, that is, $\varepsilon_A\tau^k\tau^p = \tau^p\varepsilon_A\tau^k$. Multiplying both sides of the last equality by τ^{-k}, we obtain $\varepsilon_A\tau^p = \tau^p\varepsilon_A$. It follows that $\alpha = \varepsilon_A\sigma$ and τ^p commute precisely when A is the set of all points in N moved by some subset of cycles in the cycle decomposition of τ^p.

Now, the number of elements of $M - Z_G(M)$ of the form $\varepsilon_A\sigma$, where A is the set of all points in N moved by some subset of cycles in the cycle decomposition of τ^p, and $\sigma \in G$, is $(2^p - 2)p^2$ (since we have $2^p - 2$ choices for A and p^2 choices for σ). Hence the number of conjugacy classes in M with p members is $\frac{(2^p-2)p^2}{p} = p(2^p-2)$.

Turning to the number of conjugacy classes in M with p^2 members, we let m denote the number of classes of size p^2. Then, recalling the formula for the size of M (Corollary 3.5), we have

$$[p^2+1]\cdot 1 + [p(2^p-2)]\cdot p + m\cdot p^2 = p^2(2^{p^2}-1)+1,$$

which implies $m = 2^{p^2} - 2^p$.

Next, we suppose that G is not cyclic. Again, we count $\alpha \in M$ such that $|C_G(\alpha)| = p$. Since G is not cyclic, every non-identity element of G has order p. It follows that G has exactly $p+1$ subgroups of order p, say $H_1, \ldots, H_{p+1}$, with $H_i \cap H_j = \{1\}$ for $i \neq j$. For $i \in \{1, \ldots, p+1\}$, let τ_i be a generator of H_i. For every $\alpha \in M$, $|C_G(\alpha)| = p$ if and only if $C_G(\alpha) = H_i$ for some $i = 1, \ldots, p+1$. Thus it suffices to count those $\alpha \in M - Z_G(M)$ that commute with τ_i for exactly one $i \in \{1, \ldots, p+1\}$.

Fix τ_i and note that, since G is regular and $n = p^2$, τ_i is a product $\tau_i = \rho_1\rho_2\cdots\rho_p$ of p disjoint cycles, each of length p. By the argument in the cyclic case above, the number of $\alpha \in M - Z_G(M)$ that commute with the fixed τ_i is $(2^p-2)p^2$. Thus the number of $\alpha \in M - Z_G(M)$ that commute with exactly one τ_i is $(p+1)(2^p-1)p^2$ (since we have $p+1$ choices for τ_i). Hence the number of conjugacy classes in M with p members is $\frac{(2^p-2)(p+1)p^2}{p} = p(p+1)(2^p-2)$.

Turning to the number of conjugacy classes in M with p^2 members, we let m denote the number of classes of size p^2. Then, recalling the formula for the size of M (Corollary 3.5), we have

$$[p^2+1]\cdot 1 + [p(p+1)(2^p-2)]\cdot p + m\cdot p^2 = p^2(2^{p^2}-1)+1,$$

which implies $m = 2^{p^2} - (p+1)2^p + 2p$. □

References

[1] S.Y. Chen and S.C. Hsieh, *Factorizable inverse semigroups*, Semigroup Forum **8** (1974), 283–297. MR **51:**13089

[2] J.M. Howie, *Fundamentals of Semigroup Theory*, Oxford University Press, New York, 1995. MR **98e:**20059

[3] N. Jacobson, *Basic Algebra I*, W.H. Freeman Company, New York, 1985. MR **86d:**00001

[4] M.V. Lawson, *Inverse Semigroups*, World Scientific, Singapore, 1998. MR **2000g:**20123

[5] S.L. Lipscomb, *Problems and applications of finite inverse semigroups*, Words, languages and combinatorics (Kyoto, 1990), 337–352, World Sci. Publishing, River Edge, NJ, 1992. MR **93a:**20104

[6] S.L. Lipscomb, *Symmetric Inverse Semigroups*, Mathematical Surveys and Monographs, vol. 46, American Mathematical Society, Providence, RI, 1996. MR **97j:**20065

[7] Y. Tirasupa, *Factorizable transformation semigroups*, Semigroup Forum **18** (1979), 15–19. MR **80j:**20072

[8] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964. MR **32:**1252

Department of Mathematics, Mary Washington College, Fredericksburg, Virginia 22401

E-mail address: slipscom@mwc.edu

Department of Mathematics, Mary Washington College, Fredericksburg, Virginia 22401

E-mail address: jkoniecz@mwc.edu