Finite Aperiodic Semigroups with Commuting Idempotents and Generalizations

Peter M. Higgins and Stuart W. Margolis

1 Introduction

Among the most important and intensively studied classes of semigroups are finite semigroups, regular semigroups and inverse semigroups. Finite semigroups arise as syntactic semigroups of regular languages and as transition semigroups of finite automata. This connection has lead to a large and deep literature on classifying regular languages by means of algebraic properties of their corresponding syntactic semigroups. The Eilenberg Variety Theorem [E] establishes a one-one correspondence between so called varieties of formal languages and pseudovarieties of finite semigroups. Recall that a pseudovariety is a collection of finite semigroups closed under homomorphic image, subsemigroups and (finite) direct product. The books by Eilenberg [E], Lallement [L], Pin [P] and Almeida [Al] give many details about this field.

Regular semigroups, that is semigroups S such that for all $s \in S$ there is $t \in S$ such that $sts = s$ have also been intensively studied. Natural examples of regular semigroups include the full transformation semigroup on a set and the semigroup of all matrices over a field. Recently Putcha and Renner have developed a theory of algebraic monoids. In this theory, regular semigroups are naturally associated with reductive algebraic groups. Furthermore, they have developed a notion of "finite monoid of Lie type", a class of finite regular semigroups associated with groups of Lie type. See [Pu] or the survey article [S].

Regular semigroups have also been intensively studied within semigroup theory itself. Among the classes that have received the most treatment is the class of inverse semigroups. These are precisely the regular semigroups whose idempotents commute- that is form a semilattice under multiplication. This property turns out to be equivalent to the fact that every element s in an inverse semigroup S has a unique inverse s^{-1} satisfying $ss^{-1}s = s$ and $s^{-1}ss^{-1} = s^{-1}$. An important example of an inverse semigroup is the semigroup of all partial bijections on a set. This is called the symmetric inverse semigroup and plays the role in inverse semigroup theory that the symmetric group plays in group theory. The Preston-Vagner Theorem is the analogue of the Cayley Theorem and states that every inverse semigroup is faithfully represented by partial bijections. Thus inverse semigroups arise naturally when studying partial automorphisms of a set. They from an important area of study in geometry where they are called pseudogroups of local transformations. See the book [Pe] for background as well as the forthcoming book by Lawson [La].

Historically, these three area of semigroup theory have developed independently of one another (although for some time results from inverse semigroup theory have been used as models of how to look for generalizations to regular semigroup theory). In the early 1990's Ash [A] gave a deep connection between inverse semigroups and finite semigroups by proving his now famous result that states that any finite semigroup S, the idempotents of which commute with each other, is

a homomorphic image of a subsemigroup T of some finite inverse semigroup I, in which case we say that S *divides* I. (The converse is of course clearly also true.) This can be also be stated within the context of pseudovariety theory: the pseudovariety of finite semigroups generated by finite inverse semigroups is precisely the pseudovariety of finite semigroups whose idempotents commute.

Previous to this, Birget [B] (or for a recent proof, see [G]) proved that any (finite) semigroup S whose principal left and right ideals from forests under inclusion (such semigroups are called unambiguous) embeds into a (finite) regular semigroup S_{reg} such that S and S have the same maximal subgroups. In particular, since it is known that every (finite) semigroup is a homomorphic image of a (finite) unambiguous semigroup (via the Rhodes expansion [T]), it follows that every finite semigroup with trivial subgroups (called aperiodic semigroups) divides a regular aperiodic semigroup. Again from the point of view of pseudovarieties, this says that the pseudovariety of aperiodic semigroups is generated by its regular members.

The purpose of this paper is to study the intersection of the previous two results: does every finite aperiodic semigroup with commuting idempotents divide a finite aperiodic inverse semigroup? That is, is the pseudovariety generated by finite aperiodic inverse semigroups equal to the pseudovariety of aperiodic semigroups with commuting idempotents? Surprisingly we show that the answer is no and in a very strong sense.

In section 2 we show that the pseudovariety generated by the finite aperiodic inverse semigroups is strictly contained in $\mathbf{A} \cap \mathbf{IC}$, the pseudovariety of all aperiodic semigroups with commuting idempotents. In section 3 we generalize the method introduced here to prove that the smallest pseudovariety containing $\mathbf{A} \cap \mathbf{IC}$ that is generated by inverse semigroups is $\mathbf{IC}$ itself.

2   The Aperiodic Case

In this section we construct a finite semigroup S with commuting idempotents and prove that it does not divide any finite aperiodic inverse semigroup. Our semigroup S is to be a certain 19-element subsemigroup of I_4, the symmetric inverse semigroup on the set $X = \{1, 2, 3, 4\}$. Let B be the ideal of I_4:

$$B = \{\alpha \in I_4 : |\mathrm{dom}\alpha| \leq 1\}.$$

We see that $|B| = 4^2 + 1 = 17$; indeed it is readily checked that B is a combinatorial Brandt semigroup with 4 non-zero idempotents. We then form S by adjoining to B the two elements a' and b' as follows:

$$a' = \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & - & - \end{array} \right), \qquad b' = \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & - & - \end{array} \right)$$

We see at once that $a'^2 = b'^2 = a'b' = b'a' = 0$, so that $S = B \cup \{a', b'\}$ is a 19-element aperiodic subsemigroup of I_4, and so in particular S has commuting idempotents. We shall make use of the following fact taken from [RW].

Lemma 2.1 Let $\phi : T \to S$ be a surjective homomorphism of finite semigroups and let J' be a $\mathcal{J}$-class of S. Then $J'\phi^{-1} = J_1 \cup J_2 \cup \cdots \cup J_k$ is a union of $\mathcal{J}$-classes of T, and if J_i $(1 \leq i \leq k)$ is $\leq_{\mathcal{J}}$-minimal among $J_1, \cdots, J_k$, then $J_i\phi = J'$. Furthermore, if J' is regular, then the index i is uniquely determined, that is J_i is $\leq_{\mathcal{J}}$-minimum among $J_1, \cdots, J_k$, and J_i is itself regular.

Proposition 2.2 The finite semigroup S is aperiodic with commuting idempotents but does not divide any finite aperiodic inverse semigroup I.

Proof: Suppose that there existed a surjective homomorphism $\phi : T \rightarrow S$, where T was a subsemigroup of a finite aperiodic inverse semigroup I.

Let J be the unique minimum (regular) $\mathcal{J}$-class of T such that $J\phi = J'$, the 4×4 $\mathcal{J}-$class of S. Let Z be the ideal of T, $0\phi^{-1}$. Then from the minimality property of J it follows that $C = J \cup Z$ is a subsemigroup of T such that $C\phi = B$. Consider the Rees quotient C/Z. Since Z is a kernel class of the mapping ϕ, it follows that ϕ induces a surjective homomorphism $\bar{\phi} : C/Z \rightarrow B$. Hence B is a homomorphic image of the finite aperiodic Brandt semigroup C/Z; however, since such semigroups are congruence-free, it follows that $\bar{\phi} : C/Z \rightarrow B$ is an isomorphism. Therefore we can conclude that J is also a 4×4 regular combinatorial $\mathcal{J}$-class of T.

We shall denote by $(i,j)'$ the member of B which maps i onto j, ($i, j \in \{1, 2, 3, 4\}$), and denote the unique inverse image in J of $(i,j)'$ under ϕ by (i,j). Choose and fix members a and b of T such that $a\phi = a'$ and $b\phi = b'$. We complete the demonstration by verifying that the monogenic subsemigroup $A = \langle ba^{-1} \rangle$ contains a non-trivial subgroup. In order to do this it is sufficient to show that the right multiplicative action of ba^{-1} on the point $(1,1)$ of T is that of a non-trivial cycle.

We continue the proof of the proposition by analyzing the actions of a and b on the members of J. Suppose that in S, $(i,j)'a' = (k,l)'$. This gives:

$$((i,j)a)\phi = (i,j)\phi a\phi = (i,j)'a' = (k,l)' = (k,l)\phi. \tag{1}$$

Now $(i,j)a \leq_{\mathcal{J}} (i,j)$ and since $((i,j)a)\phi \in J'$, the minimality condition on J ensures that this inequality of $\mathcal{J}$-classes cannot be strict. Hence $(i,j)a \in J$, and since ϕ is one-to-one on J we conclude from (1) that $(i,j)a = (k,l)$. Conversely, if $(i,j)a = (k,l)$ it follow from the fact that ϕ is a homomorphism that $(i,j)'a' = (k,l)'$. The same argument applies equally well to b, or to the reverse products. In conclusion, if we let c stand for either of a or b we have:

$$(i,j)c = (k,l) \text{ iff } (i,j)'c' = (k,l)', \text{ and } c(i,j) = (k,l) \text{ iff } c'(i,j)' = (k,l)'.$$

That is to say, a and b act on J as a' and b' act on J'. Moreover, since $(j,i)'$ is inverse to $(i,j)'$ in J', it follows that in the inverse semigroup I, $(i,j)^{-1} = (j,i)$.

To complete the proof it is sufficient to verify that in the inverse semigroup I:

$$(1,1)ba^{-1} = (1,2), \quad \text{and} \quad (1,2)ba^{-1} = (1,1).$$

Now, since $(1,1)'b' = (1,4)'$ it follows that $(1,1)b = (1,4)$; similarly $a(4,1) = (2,1)$. Hence we obtain:

$$(1,1)ba^{-1} = (1,4)a^{-1} = (((1,4)a^{-1})^{-1})^{-1} = (a(4,1))^{-1} = (2,1)^{-1} = (1,2).$$

The following similar calculation completes the proof:

$$(1,2)ba^{-1} = (1,3)a^{-1} = (((1,3)a^{-1})^{-1}))^{-1} = (a(3,1))^{-1} = (1,1)^{-1} = (1,1).$$

3   The General Case

Let $b_1, b_2, \cdots, b_k$ be injective mappings on the set $X_n = \{1, 2, \cdots, n\}$, and let U be the semigroup generated by the injections b_i, $(1 \leq i \leq k)$. We build the following subsemigroup $S(U)$ of the symmetric inverse semigroup I_{2n}, the base set of which we shall take to be $X_{2n} = \{1, 2, \cdots, n, 1', 2', \cdots, n'\}$. For a subset $D = \{i_1, i_2, \cdots, i_t\}$ of X_n denote by D' the set $\{i'_1, i'_2, \cdots, i'_t\}$. For each i $(1 \leq i \leq k)$ let b'_i be the map with $\mathrm{dom}b'_i = \mathrm{dom}b_i$, and $\mathrm{ran}b'_i = (\mathrm{ran}b_i)'$ which acts as follows:

$$j \cdot b'_i = (j \cdot b_i)'.$$

Similarly, let a' be the map with domain X_n and range X'_n for which $j \cdot a' = j'$.

Finally let $S(U)$ be the semigroup generated by the mappings b'_i, $(1 \leq i \leq k)$, together with a' and B, the combinatorial Brandt semigroup consisting of all the mappings of I_{2n} of rank no more than 1.

For example, the semigroup S of the previous section is a special case of this construction: there $n = 2$ and the elements 3 and 4 correspond to $1'$ and $2'$ respectively; moreover $k = 1$, and the unique injection $b_1 = b$ of $\{1, 2\}$ is the transposition $(1\ 2)$, and so our U is a two-element group.

As before, $S(U)$ is the disjoint union of B, the combinatorial Brandt semigroup of all mappings in I_{2n} of rank at most 1, (which has $(2n)^2 + 1$ elements and $2n$ non-zero idempotents), and the set $\{b'_1, b'_2, \cdots, b'_k, a'\}$, as this latter set generates only a zero semigroup, as ranges and domains are disjoint. Thus $|S(U)| = 4n^2 + k + 2$, (in the previous section we saw $n = 2$ and $k = 1$ to yield our 19-element semigroup S). It follows that $S(U)$ is aperiodic with commuting idempotents. We shall follow the argument of Proposition 2.2 to prove the main result, Theorem 2.2. We shall however require one basic fact concerning Brandt semigroups.

Lemma 3.1 The only congruence ρ on a Brandt semigroup S that is not contained in $\mathcal{H}$ is the universal congruence ω.

Proof: Suppose that $\rho \not\subseteq \mathcal{H}$. Certainly if $(a, 0) \in \rho$ with $a \neq 0$ then the fact that S is 0-simple gives immediately that $\rho = \omega$. On the other hand, suppose that a and b are not 0, and that $(a, b) \in \rho$ but that $(a, b) \notin \mathcal{H}$. Suppose that $(a, b) \notin \mathcal{L}$. Taking the unique idempotent $e \in \mathrm{E}(L_b)$ we obtain $b = be\ \rho\ ae = 0$, whence $\rho = \omega$ by the previous argument. The dual argument yields the same conclusion in the alternative case where $(a, b) \notin \mathcal{R}$. $\square$

Theorem 3.2 If $S(U)$ is a divisor of some finite inverse semigroup I, then U divides I also.

Proof: Suppose that $\phi : T \rightarrow S(U)$ is a surjective homomorphism from a semigroup T which is a subsemigroup of some finite inverse semigroup I. Let J' denote the major $\mathcal{J}$-class of B and, again invoking Lemma 2.1, let J be the unique minimum (regular) $\mathcal{J}$-class of T such that $J\phi = J'$. We proceed as in the proof of Proposition 2.2 to conclude that B is a homomorphic image of C/Z, a completely 0-simple inverse semigroup, that is a Brandt semigroup over some group H. That the major $\mathcal{J}$-class J' of C/Z is also a $2n \times 2n$ array (and not some strictly larger one) is a consequence of Lemma 3.1.

We denote by $(i, j)'$ the member of B which maps i onto j, $(i, j \in \{1, 2, \cdots, n, 1', 2', \cdots, n'\})$. From Lemma 3.1 it follows that $(i, j)'\phi^{-1} \cap J$ is a single $\mathcal{H}$-class $H_{(i,j)}$ contained in J, and not a union of several such $\mathcal{H}$-classes. (We shall often write $H_{i,j}$.) Hence ϕ induces a bijection between

the $\mathcal{H}$-classes within J and those of J', which are of course singletons $(i,j)'$. Since ϕ preserves $\mathcal{L}$ and $\mathcal{R}$-classes it follows that J consists of $2n$ $\mathcal{R}$-classes and $2n$ $\mathcal{L}$-classes respectively indexed as follows:

$$R_i = H_{i,1} \cup H_{i,2} \cup \cdots \cup H_{i,2n};$$

$$L_i = H_{1,i} \cup H_{2,i} \cup \cdots \cup H_{2n,i}, \ (1 \le i \le 2n).$$

Choose and fix members a and B_i $(1 \le i \le k)$ of T such that $a\phi = a'$ and $B_i\phi = b_i'$. Let $c \in \{a, B_1, B_2, \cdots, B_k\}$, and take B_i' to stand for b_i'. After the fashion of the proof of Proposition 2.2, suppose that in $S(U)$ we have $(i,j)'c' = (k,l)'$. Then since $(k,l)' \le_{\mathcal{R}} (i,j)'$ and J' is regular it follows that $(i,j)\mathcal{R}(k,l)$, so that $k = i$. This gives:

$$(H_{i,j}c)\phi = H_{i,j}\phi c\phi = (i,j)'c' = (i,l)' = H_{i,l}\phi. \tag{2}$$

Again, the fact that $(H_{i,j}c)\phi \in J'$ together with the minimality condition on J ensures that $H_{i,j}c \subseteq J$. Now for any member $x \in H_{i,j}$, $xc \le_{\mathcal{R}} x$, and $x\mathcal{J}xc$, whence it follows that $x\mathcal{R}xc$ as no two distinct $\mathcal{R}$-classes within the regular $\mathcal{J}$-class J are comparable. It follows from Green's Lemma that right multiplication by c defines a bijection of $H_{i,j}$ onto the $\mathcal{H}$-class $H_{i,j}c$, and since the action induced by ϕ on the $\mathcal{H}$-classes of J' is one-to-one, it follows that $H_{i,j}c = H_{i,l}$. Conversely, if $H_{i,j}c = H_{i,l}$, it follows from the fact that ϕ is a homomorphism that $(i,j)'c' = (i,l)'$. Combining this analysis with its dual we see that c acts on the $\mathcal{H}$-classes of J as c' acts on the members of J' in that the actions are both defined or not defined together, and if defined they take the form:

$$H_{i,j}c = H_{i,l} \text{ iff } (i,j)'c' = (i,l)' \text{ and } cH_{i,j} = H_{l,j} \text{ iff } c'(i,j)' = (l,j)'.$$

Furthermore, since $(j,i)'$ is inverse to $(i,j)'$ in J', it follows that in the inverse semigroup I, the set of inverses of $H_{i,j}$, which we write as $H_{i,j}^{-1}$, is equal to $H_{j,i}$.

Now let $b \in \{b_1, b_2, \cdots, b_k\}$, and write B for the chosen member of $b'\phi^{-1}$. If $j \in \text{dom}\,b$, then $H_{i,j}B = H_{(i,j)b'} = H_{i,(j \cdot b)'}$. Thus we obtain:

$$H_{i,j}Ba^{-1} = H_{i,(j\cdot b)'}a^{-1} = (((H_{i,(j\cdot b)'}a^{-1})^{-1})^{-1} = (aH_{(j\cdot b)',i})^{-1} = (H_{j\cdot b,i})^{-1} = H_{i,j\cdot b}.$$

It follows that:

$$L_j Ba^{-1} = L_{j\cdot b} \text{ if } j \in \text{dom}\,b \text{ and } L_j Ba^{-1} \cap J = \emptyset \text{ otherwise.} \tag{3}$$

We finish the proof by showing that the semigroup U is a homomorphic image of the subsemigroup A of I generated by $\{B_1 a^{-1}, B_2 a^{-1}, \cdots, B_k a^{-1}\}$. We claim that the mapping whereby $Ba^{-1} \mapsto b$ induces a homomorphism of A onto U. To justify this we are required to check that if two products $x = B_{i_1} a^{-1} B_{i_2} a^{-1} \cdots B_{i_p} a^{-1}$, and $y = B_{j_1} a^{-1} B_{j_2} a^{-1} \cdots B_{j_q} a^{-1}$, represent equal members of A, then their respective images $\bar{x}$ and $\bar{y}$ in U are also equal.

To this end, take any $j \in \{1, 2, \cdots, n\}$, and suppose that $j \cdot \bar{x}$ is defined. Then we obtain from p-fold and q-fold use of (3):

$$L_{j \cdot \bar{x}} = L_j x = L_j y = L_{j \cdot \bar{y}},$$

whence $j \cdot \bar{x} = j \cdot \bar{y}$ for all $j \in \mathrm{dom}x$; by the same argument, $j \cdot \bar{y} = j \cdot \bar{x}$ for all $j \in \mathrm{dom}y$, which yields the required conclusion $\bar{x} = \bar{y}$. $\square$

Corollary 3.3 Let $\mathbf{V}$ be a pseudovariety of semigroups generated by a collection of inverse semigroups. Then

$$\mathbf{A} \cap \mathbf{IC} \subseteq \mathbf{V} \Rightarrow \mathbf{V} = \mathbf{IC}.$$

Proof: Let U be any semigroup of one-to-one mappings on some finite set. Construct the finite semigroup $S(U)$ as above. Since $S(U)$ is aperiodic with commuting idempotents, $S(U) \in \mathbf{V}$. Since $\mathbf{V}$ is generated by inverse semigroups it also follows that $S(U)$ divides some finite inverse semigroup I such that $I \in \mathbf{V}$. Then by Theorem 3.1 U divides I as well, whence $U \in \mathbf{V}$. Therefore $\mathbf{V}$ contains all such semigroups U, whence, by Ash's Theorem $\mathbf{IC} \subseteq \mathbf{V}$; the reverse inclusion is certainly true, so that the corollary is proved.

Corollary 3.4 Let $\mathbf{G}$ be a proper pseudovariety of groups, let $\mathbf{V}(\mathbf{G})$ be the pseudovariety of all semigroups the subgroups of which lie in $\mathbf{G}$. Then there exists a finite aperiodic semigroup with commuting idempotents that does not divide any inverse semigroup in $\mathbf{V}(\mathbf{G})$.

Proof: Take G to be a finite group not in $\mathbf{G}$. Then $S(G) \in \mathbf{A} \cap \mathbf{IC}$. However, if $S(G)$ divides a finite inverse semigroup I, then so does G, and so any such I is not a member of $\mathbf{V}(\mathbf{G})$.

Remark Theorem 3.2 in fact allows us to replace the pseudovariety $\mathbf{A}$ by a smaller pseudovariety and thereby gain a stronger statement than Corollary 3.3. The pseudovariety $\mathcal{V}$ in question is contained in that generated by all ideal extensions of aperiodic Brandt semigroups by zero semigroups. Now the pseudovariety generated by the class of aperiodic Brandt semigroups is known to be given by:

$$[x^2 = x^3, xyx = xyxyx, x^2y^2 = y^2x^2]. \tag{4}$$

The generators of $\mathcal{V}$ are our semigroups $S(U)$ which have the additional property that the complement of the major $\mathcal{J}$-class forms a zero subsemigroup. It follows from this observation together with the fact that $S(U)^2$ satisfies the equations (4), that $\mathcal{V}$ is contained in the pseudovariety given by:

$$\mathcal{W} = [x^2 = x^3, xyzwxy = xyzwxyzwxy, x^2y^2 = y^2x^2].$$

Therefore we may replace $\mathcal{A}$ by the pseudovariety $\mathcal{W}$ in the statement of Corollary 3.3.

References

[A] Ash, C.J., 'Finite semigroups with commuting idempotents', J. Austral. Math. Soc. (Series A), **43**, 1987.

[B] Birget, J.C., 'The Synthesis Theorem for finite regular semigroups, and its generalization,' J. Pure Appl. Algebra 55 (1988), 1-79.

[G] Grillet, P.A., *Semigroups, An introduction to the Structure Theory*, Marcel Dekker, New York, (1995).

[RW] Rhodes, J., and P. Weil, 'Decomposition techniques for finite semigroups using categories,' Inter. J. Pure and Applied Algebra, **62** (1989), 269-284.