EMBEDDING IN A FINITE 2-GENERATOR SEMIGROUP

PETER M. HIGGINS

Department of Mathematical Sciences, University of Essex,
Wivenhoe Park, Colchester, Essex CO4 3SQ, UK
e-mail: peteh@essex.ac.uk

Abstract. We augment the body of existing results on embedding finite semigroups of a certain type into 2-generator finite semigroups of the same type. The approach adopted applies to finite semigroups the idempotents of which form a band and also to finite orthodox semigroups.

2010 *Mathematics Subject Classification.* 20M19, 20M20.

1. Introduction. In this paper, we will be concerned with the possibility of embedding a finite semigroup S into a finite 2-generated semigroup T that shares properties with S. In particular, we show that any finite orthodox semigroup S may be embedded in a finite orthodox semigroup T generated by two group elements and that any finite orthodox monoid S^1 may be embedded as a semigroup into a finite 2-generated orthodox monoid T whose subband of idempotents satisfies the same semigroup identities. Prior to that we prove that if S^1 is a finite monoid whose idempotents $E(S^1)$ form a subsemigroup, then S^1 may be embedded in a 2-generated finite monoid T whose idempotents also form a subsemigroup and belong to the same variety of bands. For background on semigroups, we refer to standard texts such as [**4**] or [**5**].

Any semigroup S may be embedded in the full transformation semigroup $T = T_{S^1}$ (we shall sometimes write $S \leq T$ to denote that S is a subsemigroup of T). Since this natural 'Cayley' embedding preserves finiteness, it follows at once that any finite semigroup S embeds in the (regular) 3-generator semigroup T_n, where $n = |S^1|$. We denote the corresponding semigroups of partial transformations on a set X by PT_X and if $|X| = n$ we write this as PT_n.

In 1952, Trevor Evans proved in [**2**] that any countable semigroup embeds in a 2-generator semigroup although that fact is implicit in the paper [**11**] of Sierpinski published (in French) in 1935 where it was shown that any countably infinite collection of mappings in T_X embeds in a 2-generator subsemigroup of T_X. The first explicit proof that a finite semigroup may be embedded in a 2-generated finite semigroup dates from 1960 and is due to B.H. Neumann [**10**] who employed a wreath product construction. The short proof of this fact recorded here however is indicative of the approach of the present paper.

THEOREM 1.1. *Any finite semigroup S may be embedded in a finite semigroup $T = \langle \alpha, \beta \rangle$ where α is an idempotent and β is a nilpotent.*

Proof. Without loss we assume that $S = S^1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ with $S \leq T_X$ for some finite set X and where we take $\alpha_0 = \iota$, the identity mapping, in this instance

with domain X. Our semigroup $T \leq PT_Z$ where $Z = X \times \{0, 1, 2, \ldots, n\}$. We also put $\alpha_n = \iota$. The designated generators α and β are defined as follows:

$$(x, i) \cdot \alpha = (x \cdot \alpha_i, 0) \, (0 \leq i \leq n),$$
$$(x, i) \cdot \beta = (x, i + 1) \, (0 \leq i \leq n - 1).$$

In particular $\beta^{n+1} = 0$, the empty mapping and α is idempotent:

$$(x, i) \cdot \alpha^2 = (x \cdot \alpha_i, 0) \cdot \alpha = (x \cdot \alpha_i \alpha_0, 0) = (x \cdot \alpha_i, 0) = (x, i) \cdot \alpha.$$

Hence T is generated by an idempotent α together with a nilpotent β. Now put $\lambda = \beta^n \alpha \in T$. Then dom $\lambda = X \times \{0\}$ and

$$(x, 0) \cdot \lambda = (x, 0) \cdot \beta^n \alpha = (x, n) \cdot \alpha = (x \cdot \alpha_n, 0) = (x, 0),$$

so that $\lambda = \iota|_{X \times \{0\}}$. Put $\gamma_i = \lambda \beta^i \alpha \, (0 \leq i \leq n - 1)$; then dom $\gamma_i = X \times \{0\}$ and

$$(x, 0) \cdot \gamma_i = (x, 0) \cdot \lambda \beta^i \alpha = (x, 0) \cdot \beta^i \alpha = (x, i) \cdot \alpha = (x \cdot \alpha_i, 0).$$

It follows that the mapping where $\alpha_i \mapsto \gamma_i$ is a monomorphism of S into T, as required. $\square$

It is not possible, however, to embed an arbitrary finite semigroup into a finite semigroup generated by two idempotents as it is easy to prove that any semigroup (finite or not) generated by two idempotents has at most six idempotents and also does not contain a three-element chain. A complete description of semigroups generated by two idempotents has been provided by Benzaken and Mayr [1].

In [7] Margolis showed that a finite semigroup S may be embedded in a 2-generated semigroup T that is a Rees matrix semigroup $M(S)$ over S with a cyclic group adjoined as group of units. This allowed the conclusion that if all the subgroups of S were abelian (nilpotent, solvable, etc.), then you can embed S into a 2-generator semigroup T with T satisfying the same restriction on subgroups as S. The construction idea was used in [6] to show that a compact metric semigroup may be embedded in a 2-generator compact monoid. Moreover, it is implicit in [7] that any (finite) n-generated semigroup S may be embedded in a (finite) semigroup T generated by $n + 1$ idempotents, from which it follows that any finite semigroup S may be embedded in a finite semigroup generated by three idempotents.

Although not the principle result in their paper, in [8] McAlister, Stephen and Vernitski obtained a direct embedding of T_n into a 2-generator subsemigroup of T_{n+1}. Although they then move on to the question of inverse semigroups (discussed below), their construction implies the following result.

THEOREM 1.2. *Any finite semigroup may be embedded in a 2-generated semigroup that is finite and regular.*

It is enough to prove the result for $T_n (n \geq 3)$ and in [8] McAlister et al. embed T_n in a semigroup $S = \langle \alpha, \beta \rangle \leq T = T_{n+1}$. We write the idempotent of defect 1 in which $i \mapsto j \, (i \neq j)$ as $\binom{i}{j}$. Using this notation, the generator β is the $(n + 1)$-cycle $\beta = (1 \, 2 \, \cdots \, n \, n + 1)$ while $\alpha = (1 \, 2)\binom{n}{n+1}$, a product of a transposition and an idempotent of defect 1. That S contains a copy of T_n then follows from a series of easily verified facts:
• the map $\varepsilon = \alpha^2 = \binom{n}{n+1}$ is an idempotent of defect 1;

- for any $\gamma \in \varepsilon T \varepsilon$, consider the restriction $\gamma|_{\{1,2,\ldots,n-1,n+1\}}$: this defines an isomorphism of $\varepsilon T \varepsilon$ onto T_n with base set $\{1, 2, \ldots, n-1, n+1\}$;
- T_n is generated by the set consisting of the n-cycle $(1\, 2\, \cdots\, n-1\, n+1)$, the transposition $(1\, 2)$ and the idempotent of defect 1, $\binom{n-1}{n+1}$;
- taking inverse images of these three mappings under the isomorphism results in a set of three generators of $\varepsilon T \varepsilon$, which are respectively $\kappa = (1\, 2\, \cdots\, n-1\, n+1)\binom{n}{1}$, α, and the idempotent of defect 2, $\phi = \binom{n}{n+1}\binom{n-1}{n+1}$.
- finally, we note that $\varepsilon = \alpha^2$, $\kappa = \beta \varepsilon$, and $\phi = \beta \varepsilon \beta^{-1} \varepsilon$, and so $T_n \cong \varepsilon T \varepsilon \leq S$.

This concludes the proof in [8] that any finite semigroup may be embedded in a finite semigroup that is generated by a pair of group elements. (Note there are two minor corrections: the paper says that $(n-1) \cdot \kappa = n$ when it should say that $(n-1) \cdot \kappa = n+1$ and β is listed as one of the three generators of $\varepsilon T \varepsilon$ when it should say α.)

Proof of Theorem 1.3. To complete the proof we need only observe that the semigroup S is indeed regular. First note that

$$\varepsilon T \varepsilon \leq S \Rightarrow \varepsilon^2 T \varepsilon^2 \subseteq \varepsilon S \varepsilon \Rightarrow \varepsilon T \varepsilon \subseteq \varepsilon S \varepsilon \subseteq \varepsilon T \varepsilon,$$

so that

$$\varepsilon T \varepsilon = \varepsilon S \varepsilon = \alpha(\alpha S \alpha)\alpha \subseteq \alpha S \alpha = \alpha^3 S \alpha^3 \subseteq \varepsilon S \varepsilon,$$

giving equality throughout and in particular that $\alpha S \alpha \cong T_n$ is a regular subsemigroup of S.

Now take any $\gamma \in S$. Either $\gamma \in \langle \beta \rangle$, and so γ is a (regular) group element or, since $\alpha = \alpha^3$, we may write $\gamma = \beta^t \sigma \beta^s$ for some $\sigma \in \alpha S \alpha$ and $0 \leq t, s \leq n$. Taking any inverse $\sigma' \in V(\sigma)$ we may now check that $\beta^{-s} \sigma' \beta^{-t} \in V(\gamma)$. Therefore, the semigroup S is indeed regular. $\qquad\square$

Equally, the construction in [7] also preserves regularity and so Theorem 1.3 is also implicit in the Margolis paper. In [3, Theorem 4.1], Hall gives a result of C.J. Ash, which shows that any countable inverse semigroup may be embedded in an inverse semigroup with two generators and any finite inverse semigroup may be embedded in a finite inverse semigroup that is generated as an inverse semigroup by two generators. (In [8] it is shown that any finite inverse semigroup may be embedded in a finite inverse semigroup that is generated as a semigroup by two generators.) The construction we introduce here is inspired by the model of Ash. We have one principal generator that contains copies of all the mappings in S, the semigroup to be embedded, while the second generator is a cycle. The domain and range of the principal generator then consists of many copies of the base interval, which are distributed among the cycle of intervals in such a way that unwanted products, which might spoil the embedding, are avoided in the mappings that are to be simulated.

2. Mian-chowla property. The base set of the 2-generator transformation semigroup T will consist of a cycle of a large number of copies of the underlying interval on which act the members of the semigroup S, which is to be embedded in T. However, the action of our principal mapping α that simulates all the members of S will be confined to a relatively small number of sparsely spaced intervals. This will ensure that unwanted products do not arise in the construction.

To this end, let $S = \{\alpha_1, \ldots, \alpha_n\}$ be a finite semigroup with S defined by partial transformations on a finite base set X. Since we are interested in embedding S into a 2-generator semigroup T sharing some of the same properties as S, we may assume that $n \geq 3$. Moreover, without loss we may assume that S does not contain the empty mapping.

In order to make our construction free of unwanted non-zero products, we make use of the following sequence of numbers, first introduced in [**9**].

DEFINITION 2.1. The Mian–Chowla (MC) sequence is the sequence of non-negative integers $m_0, m_1, \ldots$ recursively defined as follows. Set $m_0 = 0$; for $i \geq 1$ define m_i to be the least integer exceeding m_{i-1} such that each difference between distinct integers in the sequence $m_0, m_1, \ldots, m_i$ is unique.

REMARK 2.2. The recursive step of the MC sequence is well-defined as by choosing a sufficiently large integer we may find some m such that each difference $m - m_j$ has not appeared previously among the differences of pairs taken from the sequence: indeed it is clear that $m_i \leq 2m_{i-1} + 1$ so that $m_i \leq 2^i - 1$. The MC sequence begins:

$$0, 1, 3, 7, 12, 20, 30, 44, 65, 80, 96, 122, 147, 181, 203, 251, 289, \ldots$$

The recursive rule of definition of the MC sequence is often formulated in the equivalent form that m_i is the least integer such that the list of all pairwise sums, $m_j + m_k$ for $j, k \leq i$, has no repeats. Note that under this alternative formulation, $j = k$ is not forbidden.

In Section 3, we shall work with this particular sequence in our construction: m_i will denote the member of the MC sequence indexed by i. However, the results will apply to *any* strictly increasing sequence of integers with the MC property, meaning that no number appears as a difference between distinct members more than once. There are of course any number of such sequences: for example the sequence k^n, $n = 0, 1, 2, \ldots$, for any base $k \geq 2$ possesses the MC property. Moreover, the MC property is inherited by subsequences. In Section 4, we shall also call upon the following specific fact.

LEMMA 2.3. *For $i, j, k, l \leq n$, if $i \geq j$ and $k \geq l$ then $(2^i + 2^j) - (2^k + 2^l) = 2^n + 2^0$ implies that $i = n$, $l = 0$ and $j = k$.*

Proof. If $i \leq n - 1$ then $2^i + 2^j \leq 2 \cdot 2^{n-1} = 2^n$ and the equation cannot hold. Hence $i = n$, giving $2^j - (2^k + 2^l) = 1$. Hence $j \geq 2$ and since both sides of the equation are odd, it follows that $l = 0$, and so $j = k$. $\qquad\square$

REMARK 2.4. Unfortunately, the MC sequence lacks the corresponding property as for example:

$$44 + 65 = 109 = 96 + 12 + 1 + 0 \Leftrightarrow m_7 + m_8 = m_{10} + m_4 + m_1 + m_0$$
$$\Leftrightarrow (m_7 + m_8) - (m_4 + m_1) = m_{10} + m_0.$$

Suppose that $M = m_0, m_1, \ldots, m_n$ is a (strictly increasing) MC sequence of non-negative integers and put $m = 1 + m_n$. For any set $A \subseteq M$ and $r \in \mathbb{Z}$, let us write $A + r = \{(a + r)(\mathrm{mod}\ m), a \in A\}$. Suppose that $|A| \geq 3$ and $A + r \subseteq M$ with $r \not\equiv 0$ (mod m). Without loss we may assume that $1 \leq r \leq m - 1$. By hypothesis, for each $m_i \in A$, $(m_i + r)(\mathrm{mod}\ m) = m_j$ for some $0 \leq j \leq n$. It follows that either $m_j - m_i = r$ or if $(m_i + r)(\mathrm{mod}\ m) = m_i + r - m$, then $m_j - m_i = r - m$. Let m_a, m_b, m_c be three

pairwise distinct members of A. Consider, modulo m, each of $m_a + r, m_b + r$ and $m_c + r$. It now follows that for at least two of m_a, m_b, m_c, let us say m_a and m_b, there exist $m_j, m_k \in M$ such that $m_j - m_a = m_k - m_b$, contrary to the MC condition. Hence we conclude:

LEMMA 2.5. *Let $M = m_0, m_1, \ldots, m_n$ be a finite strictly increasing sequence of non-negative integers with the MC property and put $m = 1 + m_n$. Suppose that $A \subseteq M$ is such that $(A + r) \ (mod \ m) \subseteq M$ for some $r \not\equiv 0 \ (mod \ m)$. Then $|A| \leq 2$.*

3. Embedding in a semigroup generated by a nilpotent and a cycle. In this section, we construct a general embedding of a finite semigroup S into a 2-generated finite semigroup T, which preserves the property that the idempotents form a subsemigroup.

We will make use here of the easily proved result that in the presence of the band identity $x = x^2$, any *heterotypical identity* ϕ (one in which a variable appears on one side only) implies the identity $x = xyx$. It follows that any band satisfying ϕ is a rectangular band.

Let S be a finite semigroup $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. We shall take S to be a subsemigroup of PT_X, where X is a finite base set. We may also assume that the domain of each α_i is not empty. In the following construction we could replace the set of mappings $\{\alpha_i\}$ by any generating set of S but for simplicity of notation we work with S as the generating set for S.

Let $\{m_i\}_{i \geq 0}$ denote the MC sequence and let $Z = X \times \{0, 1, 2, \ldots, m_{2n-1}\}$. Taking addition modulo $m = 1 + m_{2n-1}$, we take one generator of our containing 2-generator semigroup T to be β where:

$$(x, i) \cdot \beta = (x, i + 1) \ (0 \leq i \leq m_{2n-1}). \tag{1}$$

Since β is a cycle, the notation β^r is meaningful for all integers r. We next specify the domain and range of our second generator α: dom α is contained in the union of the n copies of X, $Y_i = X \times \{m_i\}$ ($n \leq i \leq 2n - 1$) while the range $Z\alpha$ is a subset of a second union of another n copies of X: $X \times \{m_i\}$ ($0 \leq i \leq n - 1$). We define the action of α on the *interval* $Y_{n+j} = X \times \{m_{n+j}\}$ as we shall call it as:

$$(x, m_{n+j}) \cdot \alpha = (x \cdot \alpha_j, m_j) \ (0 \leq j \leq n - 1). \tag{2}$$

DEFINITION 3.1. Let $T = \langle \alpha, \beta \rangle$, with α, β defined as in (1) and (2).

LEMMA 3.2. *The generators α and β of T satisfy $\alpha^2 = 0$ and $\beta^m = \iota$, where $m = 1 + m_{2n-1}$. For each $\gamma \in T$ and $0 \leq i \leq n - 1$ there exists some $0 \leq j \leq n - 1$ such that $(X \times \{i\})\gamma \subseteq X \times \{j\}$; moreover if $(x, i) \cdot \gamma, (x', i') \cdot \gamma \in X \times \{j\}$ then $i = i'$.*

Proof. The first two facts follow respectively from (2) for α and from (1) for β. The claims in the second sentence follow for $\gamma = \alpha, \beta$ as each mapping is one-to-one on second components whence, by induction on the length of the product, the same follows for an arbitrary product γ of these two generators. $\square$

LEMMA 3.3. *Let $\gamma \leq_{\mathcal{J}} \alpha\beta^r\alpha$. Then, dom $\gamma \subseteq X \times \{i\}$ for some i such that $0 \leq i \leq m - 1$.*

Proof. First suppose that $\gamma = \rho\lambda\sigma$ with dom $\lambda \subseteq X \times \{j\}$ say and that $(x, i) \in$ dom $\rho\lambda$ so that $(x, i) \cdot \rho \in X \times \{j\}$. It follows from Lemma 3.2 applied to ρ that

dom $\rho\lambda \subseteq X \times \{i\}$ and then since dom $\rho\lambda\sigma \subseteq$ dom $\rho\lambda$, we obtain dom $\gamma \subseteq X \times \{i\}$. Therefore, it is enough to prove the claim for a mapping γ of the form $\gamma = \alpha\beta^r\alpha$. Since dom $\gamma \subseteq$ dom α, it follows that each member of dom γ has the form (x, m_{n+j}) for some $0 \le j \le n - 1$. We then obtain:

$$(x, m_{n+j}) \cdot \alpha\beta^r\alpha = (x \cdot \alpha_j, m_j) \cdot \beta^r\alpha = (x \cdot \alpha_j, (m_j + r)\,(\mathrm{mod}\ m)) \cdot \alpha. \tag{3}$$

Again by definition of α we infer that $m_j + r \equiv m_{n+l} \,(\mathrm{mod}\ m)$ for some $0 \le l \le n - 1$. Now suppose that $(x', m_{n+j'}) \in$ dom γ; by (3) we deduce that $m_{j'} + r \equiv m_{n+l'} \,(\mathrm{mod}\ m)$ say, so that $m_{n+l'} - m_{j'} \equiv m_{n+l} - m_j \equiv r \,(\mathrm{mod}\ m)$. Since $0 \le m_j, m_{j'} < m_{n+l}, m_{n+l'} \le m - 1$, it follows that these congruences imply the corresponding equalities and that $r \not\equiv 0 \,(\mathrm{mod}\ m)$. By the MC property however we conclude that $j = j'$ and $l = l'$. In particular, dom $\gamma \subseteq X \times \{m_{n+j}\}$, giving the required conclusion. $\qquad\square$

LEMMA 3.4. *Define the mapping* $\lambda_0 = (\beta^{m_n}\alpha)^2$. *Then,* $\lambda_0 = \iota|_{X \times \{0\}}$.

Proof. From the definition of λ_0 we obtain

$$(x, 0) \cdot \lambda_0 = (x, 0) \cdot (\beta^{m_n}\alpha)^2 = (x, m_n) \cdot \alpha\beta^{m_n}\alpha = (x \cdot \alpha_0, m_0) \cdot \beta^{m_n}\alpha$$
$$= (x, 0) \cdot \beta^{m_n}\alpha = \cdots = (x, 0).$$

The result now follows from this together with Lemma 3.3. $\qquad\square$

LEMMA 3.5. *The semigroup* $T = \langle \alpha, \beta \rangle$ *contains each of the mappings* $\lambda_{i,j,k} = \lambda(\alpha_i, j, k)$ *where* dom $\lambda_{i,j,k} \subseteq X \times \{j\}$, ran $\lambda_{i,j,k} \subseteq X \times \{k\}$ *and* $(x, j) \cdot \lambda_{i,j,k} = (x \cdot \alpha_i, k)$ $(0 \le i \le n - 1,\ 0 \le j, k \le m - 1)$.

Proof. We verify that $\lambda(\alpha_i, j, k) = \beta^{-j}\lambda_0\beta^{m_{n+i}}\alpha\beta^{k-m_i}$. Consider (x, t) with $t \not\equiv j\,(\mathrm{mod}\ m)$. Then, $(x, t) \cdot \beta^{-j} = (x, t - j) \notin X \times \{0\}$ so that by Lemma 3.4, $(x, t - j) \notin$ dom λ_0. It follows that dom $\beta^{-j}\lambda_0\beta^{m_{n+i}}\alpha\beta^{k-m_i} \subseteq X \times \{j\}$. Next take $(x, j) \in X \times \{j\}$:

$$(x, j) \cdot \beta^{-j}\lambda_0\beta^{m_{n+i}}\alpha\beta^{k-m_i} = (x, 0) \cdot \lambda_0\beta^{m_{n+i}}\alpha\beta^{k-m_i} = (x, 0) \cdot \beta^{m_{n+i}}\alpha\beta^{k-m_i}$$
$$= (x, m_{n+i}) \cdot \alpha\beta^{k-m_i} = (x \cdot \alpha_i, m_i) \cdot \beta^{k-m_i} = (x \cdot \alpha_i, k).$$

Therefore, $\lambda(\alpha_i, j, k) \in T$. $\qquad\square$

THEOREM 3.6 (Structure of T).

    (i) *The monoid T has two $\mathcal{H}$-classes and these are also $\mathcal{D}$-classes: $H_\beta = \{\beta^r : 0 \le r \le m - 1\}$ of cardinal m, which is the group of units of T and $H_\alpha = \{\beta^r\alpha\beta^s : 0 \le r, s \le m - 1\}$ of cardinal m^2 and $H_\alpha <_{\mathcal{J}} H_\beta$. All members $\gamma = \beta^r\alpha\beta^s$ of H_α are not regular; dom $\gamma \subseteq \{X \times (m_{n+i} - r)\,(\mathrm{mod}\ m)\,(0 \le i \le n - 1)\}$ with dom γ meeting each specified interval and ran $\gamma \subseteq \{X \times (m_i + s)\,(\mathrm{mod}\ m)\,(0 \le i \le n - 1)\}$ with ran γ similarly meeting each specified interval.*

    (ii) *$T_1 = \{\lambda(\alpha_i, j, k) : 0 \le i \le n - 1,\ 0 \le j, k \le m - 1\} \cup \{0\}$ is isomorphic to the Rees matrix semigroup $M = \mathcal{M}^0[S, m, m, I_m]$, where I_m is the $m \times m$ identity matrix. Moreover, T_1 is isomorphic to $(S \times B)/I$, where B is the $m \times m$ combinatorial Brandt semigroup and I is the ideal $S \times \{0\}$ of $S \times B$. For each $j \in \mathbb{Z}_m$, the set $T_{1,j} = \{\lambda(\alpha_i, j, j) : 0 \le i \le n - 1\}$ is a subsemigroup of T isomorphic to S.*

    (iii) *For any $\gamma \in T$, with dom $\gamma \cap (X \times \{j\}) \ne \emptyset$, $\gamma|_{X \times \{j\}} = \lambda_{i,j,k}$ for some $0 \le i \le n - 1$, $0 \le k \le m - 1$.*

(iv) $T = T_1 \cup H_\alpha \cup H_\beta$, and the union is a disjoint union. Moreover T_1 is an ideal of T and if S is regular then so is T_1.

(v) The set of idempotents $E(T) = \bigcup_{i=1}^{m} E_i \cup \{0, \iota\}$, where $E_i = \{\lambda(e, i, i) : e \in E(S), 0 \leq i \leq m - 1\}$. Moreover, all products of non-identity idempotents equal 0 except those within some E_i. In particular if $E(S)$ is a band then so is $E(T)$.

Proof.

(i) The powers of β are exactly the members of T with range (and domain) Z, and by Lemma 3.2 $\langle \beta \rangle$ is a cyclic group, the group of units of T, whence it follows that $D_\beta = H_\beta = \langle \beta \rangle$ and by definition $|H_\beta| = m$.

The set $A = \{\beta^r \alpha \beta^s : r, s \geq 0\} \subseteq H_\alpha$. By Lemma 3.3, any $\delta \leq_{\mathcal{J}} \gamma$, where $\gamma \in T \setminus (A \cup H_\beta)$ has domain within some single interval of Z. If $\gamma \in D_\alpha)$ we would have $\alpha \leq_{\mathcal{J}} \gamma$, whence dom α is contained in a single interval of Z, which contradicts the definition of α. It follows that $D_\alpha \subseteq A \subseteq H_\alpha \subseteq D_\alpha$, giving equality throughout and $H_\alpha <_{\mathcal{J}} H_\beta$.

Next take $\gamma = \beta^r \alpha \beta^s$ so that

$$\text{dom } \gamma = \text{dom } \beta^r \alpha \beta^s = \{(x, (j - r) \,(\text{mod } m) : (x, j) \in \text{dom } \alpha\}.$$

Since dom $\alpha \subseteq \{(X, m_{n+i}) : (0 \leq i \leq n - 1)\}$ and dom α meets each of these intervals, it follows that dom $\gamma \subseteq \{(X, (m_{n+i} - r) \,(\text{mod } m) \,(0 \leq i \leq n - 1)\}$ as stated and that dom γ meets each of these intervals. Since α maps the members of its domain in the interval (X, m_{n+i}) into the interval (X, m_i), the claim for ran γ now follows in the same way.

Suppose that $\gamma = \beta^{r_1} \alpha \beta^{s_1}$, $\delta = \beta^{r_2} \alpha \beta^{s_2}$ and that $\gamma = \delta$. We wish to show that $\beta^{r_1} = \beta^{r_2}$ and $\beta^{s_1} = \beta^{s_2}$. By cancelling powers of β in the equation of any counter example to this claim we would obtain a counter example where $\gamma = \beta^r \alpha \beta^s$ and where $\delta = \alpha$, $(0 \leq r, s \leq m - 1)$ so let us assume this case. However, since $|S| \geq 3$ we have by Lemma 2.5 and our statement on domains that dom $\gamma = $ dom α implies that $r = 0$ and similarly we have ran $\gamma = $ ran α implies $s = 0$, as required. We conclude that all products $\beta^r \alpha \beta^s$ $(0 \leq r, s \leq m - 1)$ are pairwise distinct and $|H_\alpha| = m^2$ as claimed.

If any member of D_α were regular, the same would be true of α. However, by Lemmas 3.2 and 3.3, for any $\gamma \in T$ we have $\alpha \gamma \alpha \notin D_\alpha$, so in particular $\alpha = \alpha \gamma \alpha$ is impossible in T and hence D_α is not a regular $\mathcal{D}$-class.

(ii) From Lemma 3.5 and the definitions of α and β we have the following formulae:

$$\lambda(\alpha_{i_1}, j_1, k)\lambda(\alpha_{i_2}, k, k_2) = \lambda(\alpha_{i_1} \alpha_{i_2}, j_1, k_2), \tag{4}$$

$$\lambda(\alpha_{i_1}, j_1, k_1)\lambda(\alpha_{i_2}, j_2, k_2) = 0 \text{ if } k_1 \neq j_2, \tag{5}$$

$$\beta\lambda(\alpha_i, j, k) = \lambda(\alpha_i, j - 1, k), \quad \lambda(\alpha_i, j, k)\beta = \lambda(\alpha_i, j, k + 1), \tag{6}$$

$$\alpha\lambda(\alpha_i, m_j, k) = \lambda(\alpha_j \alpha_i, m_{n+j}, k)\,(0 \leq j \leq n - 1), \tag{7}$$

$$\alpha\lambda(\alpha_i, j, k) = 0 \text{ if } j \notin \{m_t : 0 \leq t \leq n - 1\}, \tag{8}$$

$$\lambda(\alpha_i, j, m_{n+k})\alpha = \lambda(\alpha_i\alpha_k, j, m_k), \tag{9}$$

$$\lambda(\alpha_i, j, k)\alpha = 0 \text{ if } k \notin \{m_{n+t} : 0 \leq t \leq n-1\}. \tag{10}$$

From (4) and (5) we see that products in T_1 are indeed those of the Rees matrix semigroup M, which is then isomorphic to $(S \times B)/I$. The diagonal $\mathcal{H}$-classes of M are each copies of our monoid S.

(iii) The claim is clearly true for $\gamma = \alpha, \beta$ as

$$\alpha|_{X \times \{m_{n+i}\}} = \lambda(\alpha_i, m_{n+i}, m_i) \text{ and } \beta|_{X \times \{i\}} = \lambda(\alpha_0, i, i+1).$$

The result now follows by induction on the length of γ (taken as a product in the generators α and β): let $\gamma = \rho\mu$ say, where $\mu \in \{\alpha, \beta\}$. Then, $(\rho\mu)|_{(X \times \{j\})} = \rho|_{X \times \{j\}}\mu$ but by induction we may write this product as $\lambda(\alpha_i, j, k_1)\mu$ say. By formulae (6), (9), and (10) this in turn may be written as $\lambda(\alpha_l, j, k)|_{X \times \{j\}} = \lambda(\alpha_l, j, k)$ for some $0 \leq l \leq n-1$ and $0 \leq k \leq m-1$, as required.

(iv) Since the domains of members of T_1 are each contained within a single interval and those of $H_\alpha \cup H_\beta$ are not, we have by this and part (i) that the three sets are pairwise disjoint. It remains to verify that if $\gamma \in T \setminus (H_\alpha \cup H_\beta)$ then $\gamma \in T_1$. However, by Lemma 3.3 we have dom $\gamma \subseteq X \times \{j\}$ say and so by part (iii) we have either $\gamma = 0$ or $\gamma = \gamma|_{X \times \{j\}} = \lambda_{i,j,k}$ for some i, k. In other words, $\gamma \in T_1$. From equations (6)–(10) it follows that T_1 is an ideal of T. Finally for any non-zero $\lambda = \lambda(\alpha_i, j, k) \in T_1$ we have $\lambda(\alpha_i', k, j) \in T_1$ is an inverse of λ in T_1 for any choice of $\alpha_i' \in V(\alpha_i)$.

(v) By (i), ι is the unique idempotent in $H_\alpha \cup H_\beta$. Hence any other non-zero idempotent ε belongs to T_1 and in particular dom $\varepsilon \subseteq X \times \{i\}$ say. Since ε is a non-zero idempotent, it follows that $\emptyset \neq Z\varepsilon \subseteq X \times \{i\}$. Hence by (iv) we obtain $\varepsilon = \lambda(e, i, i)$ for some $e \in S$, and clearly $e = e^2$ so that $\varepsilon \in E_i$, as claimed. The claims regarding products of idempotents now follows. This completes the proof of the theorem. □

COROLLARY 3.7. *Let S be a finite monoid such that $E(S)$ is a subsemigroup of S. Then, S may be embedded in a finite monoid T such that $E(T)$ is a submonoid of T and T is generated as a semigroup by a set of two generators $\{\alpha, \beta\}$ where β is a group element and α is nilpotent of index 2. Moreover if $|E(S)| \geq 2$, then $E(T)$ satisfies the same semigroup identities as $E(S)$.*

REMARK 3.8. If $|E(S)| \leq 1$ then, since S is a monoid and every member of S has an idempotent power, it follows that S is a finite group. We may then embed S in the finite symmetric group $T = G_S$, which is two-generated and then $E(S)$ and $E(T)$ are both trivial and so satisfy every semigroup identity.

Proof. Take $T = \langle \alpha, \beta \rangle$ as in Theorem 3.6. It remains only to verify that if $\phi : p = q$ is a semigroup identity satisfied by $E(S)$ then ϕ is satisfied by $E(T)$, the converse implication being clear as $E(S)$ is embedded in $E(T)$. If one side of ϕ, the word p say, had a variable y that did not appear in q, then substituting all other variables in ϕ by ι gives the identity $y = 1$, whence it follows that the monoid $E(S)$ is trivial, contrary to hypothesis. Hence, each variable x of ϕ appears in both p and q.

By Theorem 3.6(v), all products of non-identity idempotents within $E(T)$ equal 0 unless they take place within some $E_i = \{\lambda(e, i, i) : e \in E(S), 0 \leq i \leq m - 1\}$. Hence if, under some substitution from $E(T)$, one side of ϕ, p say, is not 0, then all variables of ϕ have been substituted by either ι or by members of some subsemigroup E_i of $E(T)$. By replacing ι with the identity of E_i as required, we express the products p and q as products of members of E_i while retaining the same values. However, since $E_i \cong E(S)$, it follows that $p = q$ is satisfied in E_i as well and so the products p and q in E_i are equal. It follows that $E(T)$ also satisfies the identity ϕ.   □

REMARK 3.9. In the case of a finite semigroup S that is not a monoid we may work with S^1. If $E(S)$ forms a band then so does $E(S^1)$ and the previous construction then yields a finite 2-generated monoid T containing S^1 (and so containing S) such that $E(T)$ is also a band.

4. Orthodox semigroups.   We next use the construction of Section 3 to provide another proof of Theorem 1.3 and to show that if the original semigroup S is orthodox, the same is true for the 2-generated containing semigroup T. We will however, now put $m_i = 2^i$, $i = 0, 1, 2 \ldots, 2n - 1$ so our modulus used for our cycle β becomes $m = 1 + 2^{2n-1}$. Let $S = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ now denote a finite regular monoid with $\alpha_0 = \iota$ and $S \leq PT_X$ for some finite base set X as before. We may also assume that the domain of each mapping α_i is not empty.

For each $\alpha_i \in S$ choose and fix an inverse $\alpha_i' \in V(\alpha_i)$ (there is no assumption that the mapping $(')$ on S is one-to-one). The cycle β is just as before and its action is given by (1). Similarly, the action (2) remains applicable to our second generator α. However, we augment the domain of α to include all the intervals $X \times \{m_i\}$ ($0 \leq i \leq n - 1$), the union of which contained the range set of α but previously lay outside of the domain of α. Define:

$$(x, m_i) \cdot \alpha = (x \cdot \alpha_i', m_{n+i}) \ (0 \leq i \leq n - 1). \tag{11}$$

REMARK 4.1. It will be convenient to also denote α_i' by α_{i+n}, in which case the definition of the action of α is encapsulated by:

$$(x, m_t) \cdot \alpha = (x \cdot \alpha_{t \pm n}, m_{t \pm n}) \ (0 \leq t \leq 2n - 1), \tag{12}$$

where the signs associated with the $\pm$ signs in (12) are not independent but are equal to each other: the sign on the subscripts is $+$ or $-$ according as $0 \leq t \leq n - 1$ or $n \leq t \leq 2n - 1$. Although α is no longer a nilpotent (see Lemma 4.3) it is still the case that any $\gamma \in T$ acts in a one-to-one fashion on the second entries of the pairs $(x, i) \in$ dom γ (as shown in the proof of Lemma 3.2) and γ maps intervals into intervals as this holds for each of the generators α and β. We next prove the counterpart of Lemma 3.3.

LEMMA 4.2.

   (i) *The mappings α and β of T satisfy $\beta = \beta^m$ and $\alpha = \alpha^3$.*
   (ii) *Let $\gamma = \beta^r \alpha^\varepsilon \beta^s$ for $\varepsilon \geq 1$. Then,*
      dom $\gamma \subseteq \{X \times \{(m_t - r) \, (mod \, m), \ (0 \leq t \leq 2n - 1)\}$ and dom γ has non-empty intersection with each of these intervals. Similarly, ran $\gamma \subseteq$

$\{X \times (m_t + s) \ (mod \ m) \ (0 \le t \le 2n - 1)\}$ *with ran γ meeting each of these intervals.*

(iii) *Let $\gamma \le_{\mathcal{J}} \alpha \beta^r \alpha$ where $r \not\equiv 0 \ (mod \ m)$. Then, dom $\gamma \subseteq X \times \{i\}$ for some $0 \le i \le m - 1$.*

Proof.

(i) That $\beta = \beta^m$ is true as before. For any $(x, m_{n+i}) \in$ dom α we have by (12) that

$$(x, m_{n+i}) \cdot \alpha^3 = (x \cdot \alpha_i, m_i) \cdot \alpha^2 = (x \cdot \alpha_i \alpha_i', m_{n+i}) \cdot \alpha$$
$$= (x \cdot \alpha_i \alpha_i' \alpha_i, m_i) = (x \cdot \alpha_i, m_i) = (x, m_{n+i}) \cdot \alpha,$$

and in the same way we obtain $(x, m_i) \cdot \alpha^3 = (x, m_i) \cdot \alpha$, thus showing that $\alpha = \alpha^3$. Note also that by finiteness it follows that $\alpha|_{\text{ran } \alpha}$ is a permutation and so dom $\alpha =$ dom α^2 and ran $\alpha =$ ran α^2.

(ii) Let us write (for the purposes of this part only)

$$D_\gamma = \{i : (X \times \{i\}) \cap \text{dom } \gamma \ne \emptyset\} \text{ and } R_\gamma = \{i : (X \times \{i\}) \cap \text{ran } \gamma \ne \emptyset\}.$$

Observe that for any $\varepsilon \ge 1$, $D_{\alpha^\varepsilon} = R_{\alpha^\varepsilon} = \{m_t : 0 \le t \le 2n - 1\}$. Also note that for any $\gamma \in T$ we have $D_{\beta^r \gamma \beta^s} = (D_\gamma - r) \ (mod \ m)$ and $R_{\beta^r \gamma \beta^s} = (R_\gamma + s)$ (mod m). Applying these facts to $\gamma = \alpha^\varepsilon$ then proves the claims of (ii).

(iii) As in the proof of Lemma 3.3, it is enough to consider the case represented by $\gamma = \alpha \beta^r \alpha$. Since dom $\gamma \subseteq$ dom α, it follows that each member of dom γ has the form (x, m_t) for some $0 \le t \le 2n - 1$ and so

$$(x, m_t) \cdot \alpha \beta^r \alpha = (x \cdot \alpha_{t \pm n}, m_{t \pm n}) \cdot \beta^r \alpha = (x \cdot \alpha_{t \pm n}, m_{t \pm n} + r \ (mod \ m)) \cdot \alpha \tag{13}$$

This implies that $m_{t \pm n} + r \equiv m_k \ (mod \ m)$ for some $0 \le k \le 2n - 1$. Now suppose that $(x', m_{t'}) \in$ dom γ; by (13) we deduce that $m_{t' \pm n} + r \equiv m_{k'} \ (mod \ m)$ for some $0 \le k' \le 2n - 1$, which yields:

$$m_{t \pm n} - m_k \equiv m_{t' \pm n} - m_{k'} \equiv -r \ (mod \ m), \tag{14}$$

where the signs taken in the $\pm$ symbols occurring in (14) are not necessarily equal to each other. If the first congruence in (14) is equality then since $r \not\equiv 0 \ (mod \ m)$, we have that $m_{t \pm n} \ne m_k$ and $m_{t' \pm n} \ne m_{k'}$ and so by the MC property $m_{t \pm n} = m_{t' \pm n}$ (and $m_k = m_{k'}$). It follows either that $t = t'$ or

$$((t - n = t' + n) \text{ or } (t + n = t' - n)) \Rightarrow |t - t'| = 2n.$$

However, since $0 \le t, t' \le 2n - 1$, the latter is not possible and so $t = t'$. Otherwise the congruence in (14) is not equality whence:

$$(m_{t \pm n} + m_{k'}) - (m_{t' \pm n} + m_k) = \pm(1 + m_{2n-1}). \tag{15}$$

By multiplying throughout by -1 and interchanging t and t' if necessary, we may take the $+$ sign in (15). Since $r \not\equiv 0 \ (mod \ m)$ we have that $m_{t \pm n} \ne m_k$ and $m_{t' \pm n} \ne m_{k'}$. However, by Lemma 2.3, one term in the first bracket equals m_{2n-1}, one term in the second bracket equals 1 and the other two terms cancel each other.

Hence either $m_{t \pm n} = 2^{2n-1}$, $m_{t' \pm n} = 1$ and $m_k = m'_k$, or $m'_k = 2^{2n-1}$, $m_k = 1$ and $m_{t \pm n} = m_{t' \pm n}$. However, $m_k = m_{k'}$ implies (by (14)) that $m_{t \pm n} = m_{t' \pm n}$ and so $t = t'$ is the conclusion. Similarly the latter possibility once again gives $t = t'$. Therefore, dom $\gamma \subseteq X \times \{m_t\}$. □

Lemmas 3.4 and 3.5 are valid for our extended construction, the proofs being unchanged from the originals. Moreover, the description of the mapping $\lambda_{i,j,k}$ of Theorem 3.6(ii) continues to hold in our monoid T currently under consideration, as do the formulae (4)–(6). The full set of corresponding formulae for T (additions and subtractions taken mod m) are as follows:

$$\beta\lambda(\alpha_i, j, k) = \lambda(\alpha_i, j-1, k), \quad \lambda(\alpha_i, j, k)\beta = \lambda(\alpha_i, j, k+1), \tag{16}$$

$$\alpha\lambda(\alpha_i, m_j, k) = \lambda(\alpha_j\alpha_i, m_{j \pm n}, k) \, (+ \text{ if } 0 \le j \le n-1, \, - \text{ if } n \le j \le 2n-1), \tag{17}$$

$$\alpha\lambda(\alpha_i, j, k) = 0 \text{ if } j \notin \{m_t : 0 \le t \le 2n-1\}, \tag{18}$$

$$\lambda(\alpha_i, k, m_j)\alpha = \lambda(\alpha_i\alpha_{j \pm n}, k, m_{j \pm n}) \, (+ \text{ if } 0 \le j \le n-1, \, - \text{ if } n \le j \le 2n-1), \tag{19}$$

$$\lambda(\alpha_i, j, k)\alpha = 0 \text{ if } k \notin \{m_t : 0 \le t \le 2n-1\}, \tag{20}$$

PROPOSITION 4.3. *Let* $T = \langle \alpha, \beta \rangle$.

(i) *For any* $\gamma \in T$, *with dom* $\gamma \cap (X \times \{j\}) \ne \emptyset$, $\gamma|_{X \times \{j\}} = \lambda_{i,j,k}$ *for some* $0 \le i \le n-1$, $0 \le k \le m-1$;

(ii) T *is regular.*

Proof.

(i) The claim is clearly true for $\gamma = \alpha, \beta$ as

$$\alpha|_{X \times \{m_i\}} = \lambda(\alpha_{i \pm n}, m_i, m_{i \pm n}) \text{ and } \beta|_{X \times \{i\}} = \lambda(\alpha_0, i, i+1).$$

The result now follows as in Theorem 3.6 (iii) by induction on the length of γ (taken as a product in the generators α and β), together with formulae (16)–(20).

(ii) Take an arbitrary product $p = \beta^{r_1}\alpha\beta^{r_2}\alpha \cdots \beta^{r_{t-1}}\alpha\beta^{r_t} \in T$ with $(1 \le t, 0 \le r_i \le m-1)$. If $p = beta^{r_1}$ then p is a group element and so p is regular. Since $\alpha = \alpha^3$ it follows that all mappings of the form $\beta^r\alpha^\varepsilon\beta^s$ $(\varepsilon = 1, 2)$ are contained in the regular $\mathcal{D}$-class D_α of T. This deals with the case where $t \le 2$ and the case $(t = 3$ and $r_2 = 0)$. The remaining cases are where $t \ge 3$ and p has one of the two forms $p = \beta^{r_1}\alpha\beta^{r_2}\alpha\beta^{r_3} \cdots$ or $p = \beta^{r_1}\alpha^2\beta^{r_2}\alpha\beta^{r_3} \cdots$ with $r_2 \ne 0$ in both instances. It follows from Lemma 4.3(iii) that dom $p \subseteq X \times \{j\}$ say. Of course if $p = 0$ then p is regular. Otherwise by (i) $p = p|_{X \times \{j\}} = \lambda_{i,j,k}$ for some $0 \le i \le n-1$, $0 \le k \le m-1$. By Theorem 3.6(ii), p is a member of a subsemigroup of T isomorphic to $(S \times B)/I$, and in particular p is a regular member of T. □

Proposition 4.4 shows that any finite semigroup may be embedded in a finite regular semigroup T generated by two group elements, thereby providing a new proof of Theorem 1.3. However, the semigroup T preserves the idempotent structure of S in that $E(T)$ consists of copies of $E(S)$ together with the conjugates under β of α^2.

THEOREM 4.4 (Structure of T).

 (i) H_β is the group of units of T, which is cyclic of order m. Moreover $D_\alpha <_{\mathcal{J}} H_\beta$ and $D_\alpha = \{\beta^r \alpha^\varepsilon \beta^s : \varepsilon = 1, 2\}$.
 (ii) The monoid T has an ideal T_1 with $\gamma <_{\mathcal{J}} \alpha$ for all $\gamma \in T_1$ where $T_1 = \{\lambda_{i,j,k}\} \cup \{0\}$ $(0 \le i \le n - 1, 0 \le j, k \le m - 1)$.
 (iii) $T = H_\beta \cup D_\alpha \cup T_1$ with the union a disjoint union.
 (iv) The set of idempotents of T is given by $E(T) = E \cup F \cup \{\iota, 0\}$, where $E = \{\lambda(e, i, i) : e \in E(S), 0 \le i \le m - 1\}$ and $F = \{\beta^j \alpha^2 \beta^{-j} : 0 \le j \le m - 1\}$. Moreover, each $\rho \in E(T)$ maps identically on its second entry, meaning that $(X \times \{i\})\rho \subseteq X \times \{i\}$.
 (v) The principal factor $D_\alpha \cup \{0\}$ of T is of cardinal $1 + 2m^2$ and is a Brandt semigroup $\mathcal{M}^0[\mathbb{Z}_2, m, m, I_m]$.

Proof.

 (i) As in Section 3, H_β is the group of units of T of cardinal m. Also $\gamma <_{\mathcal{J}} \beta$ for any $\gamma \in S\alpha S$ and so $D_\alpha <_{\mathcal{J}} H_\beta$. By Lemma 4.3(i), $\alpha = \alpha^3$ and so $A = \{\beta^r \alpha^\varepsilon \beta^s : \varepsilon = 1, 2\} \subseteq D_\alpha$. Conversely, if $\alpha \le_{\mathcal{J}} \gamma$ with $\gamma \in T \setminus (A \cup H_\beta)$ then $\alpha \le_{\mathcal{J}} \gamma \le_{\mathcal{J}} \alpha \beta^r \alpha$ for some $r \not\equiv 0 \pmod{m}$ and by Lemma 4.3(iii), it would follow that dom α was contained in a single interval of T, contrary to the definition of α. Hence $A = D_\alpha$, thus establishing (i).
 (ii) As in the proof of Lemma 3.5, we have that $T_1 \subseteq T$ and that T_1 is an ideal of T follows from the formulae (16)–(20). From Lemma 3.5 we have that $\gamma \notin H_\beta$ whence $\gamma \le_{\mathcal{J}} \alpha$ and that the inequality is strict follows from Proposition 4.4(i) and the fact that, unlike dom γ, dom α is not contained in a single interval.
 (iii) It follows from parts (i) and (ii) that $H_\beta \cup D_\alpha \cup T_1 \subseteq T$ and the union is a disjoint union. Conversely take any $\gamma \in T \setminus \{H_\beta \cup D_\alpha\}$. By part (i), Lemma 4.3(iii) applies to γ whence by Proposition 4.4(i) it follows that $\gamma \in T_1$, as required.
 (iv) Clearly all the members listed in $E(T)$ are indeed idempotents. For any $\lambda = \lambda_{i,j,k} \in T_1$ we have $\lambda^2 = 0$ unless $k = j$, in which case $\lambda^2 = \lambda$ if and only if $\alpha_i = e \in E(S)$ and so $\lambda = \lambda(e, j, j) \in E$. From part (iii) it follows that all other members $p \in E(T)$, other than 0 and ι, lie in D_α and so have the form $p = \beta^j \alpha^\varepsilon \beta^k$ where $(\varepsilon \in \{1, 2\})$. We next check that if $j + k \equiv 0 \pmod{m}$ then $p = p^2$ if and only if $\varepsilon = 2$. The reverse implication just says that all members of F are idempotents, which has already been noted, so let us suppose that, contrary to our claim, $\varepsilon = 1$ and we have $p = \beta^j \alpha \beta^{-j}$ with that $p = p^2$. Then $\beta^j \alpha \beta^{-j} = \beta^j \alpha^2 \beta^{-j}$, which in turn implies that $\alpha = \alpha^2$, which is false as $X \times \{m_n\}$ is an interval that meets dom $\alpha = $ dom α^2 but $(X \times \{m_n\})\alpha \subseteq X \times \{m_0\}$, $(X \times \{m_n\})\alpha^2 \subseteq X \times \{m_n\}$.

  Let us therefore examine the case where $j + k \not\equiv 0 \pmod{m}$ for some $0 \le j, k \le m - 1$. Since $p = p^2$ and the product p^2 contains a factor of the form $\alpha \beta^t \alpha$ with $t \not\equiv 0 \pmod{m}$, it now follows by Lemma 4.3(iii) and the fact that $p = p^2$ that both dom p and ran p are contained in $X \times \{i\}$ say. However,

since dom $\alpha = \operatorname{dom} \alpha^2 = X \times \{m_t\}_{0 \le t \le 2n-1}$, it follows from Lemma 4.3(ii) that dom $p = \operatorname{dom} \beta^j \alpha^\varepsilon \beta^k = X \times \{m_t - j\}_{0 \le t \le 2n-1}$ ($\varepsilon \in \{1, 2\}$). In particular, dom p is not contained within a single set of the form $X \times \{i\}$ and this contradicts the assumption that $p \in E(T)$. Therefore, the set $E(T)$ is as described. The final assertion is clearly true for idempotents 0 and ι and those in T_1. By above, any idempotent $\rho \in F$ satisfies dom $\rho \subseteq X \times \{i\}$ say and since any idempotent maps identically on its range it follows that $(X \times \{i\})\rho \subseteq X \times \{i\}$ from which the claim follows.

(v) There are $2m^2$ expressions of the form $\beta^r \alpha^\varepsilon \beta^s$: ($\varepsilon \in \{1, 2\}$, $0 \le r, s \le m - 1$) and so the cardinality claim will follow by showing they are pairwise distinct. If not, we would have an equality of the form $\alpha^{\varepsilon_1} = \beta^r \alpha^{\varepsilon_2} \beta^s = \gamma$ say, for some $\varepsilon_1, \varepsilon_2 \in \{1, 2\}$. By Lemma 4.3(ii), dom $\gamma \subseteq \{X \times \{(m_t - r) \pmod m)$, $0 \le t \le 2n - 1\}$ and dom γ has non-empty intersection with each of these intervals. Since $|S| \ge 3$ it follows by Lemma 2.5 that $r = 0$ and in the same way we infer likewise that $s = 0$ as well.

Since D_α is a regular $\mathcal{D}$-class, the principal factor $P = D_\alpha \cup \{0\}$ is a completely 0-simple semigroup. By part (i) and Lemma 4.3 parts (ii) and (iii) we see that for $\gamma = \beta^r \alpha^\varepsilon \beta^s \in D_\alpha$ we have $R_\gamma = \{\beta^r \alpha^\varepsilon \beta^t; \varepsilon \in \{1, 2\}, 0 \le t \le m - 1\}$, $L_\gamma = \{\beta^t \alpha^\varepsilon \beta^s, \varepsilon \in \{1, 2\}, 0 \le t \le m - 1\}$ and so $H_\gamma = \{\beta^r \alpha^\varepsilon \beta^s : \varepsilon \in \{1, 2\}\}$. In particular $H_\alpha = \{\alpha, \alpha^2\} \cong \mathbb{Z}_2$. By the previous paragraph it follows that there are m $\mathcal{R}$-classes and m $\mathcal{L}$-classes of D_α, so that $P \cong \mathcal{M}^0[\mathbb{Z}_2, m, m, M]$ is the Rees matrix form of this principal factor for some $m \times m$ matrix M. To complete the proof we only need to know that the idempotents of P form a semilattice, for then P is a regular 0-simple semigroup with commuting idempotents, which is necessarily a Brandt semigroup, whence M can be taken to be the identity matrix. However, the product of any two distinct idempotents $e = \beta^j \alpha^2 \beta^{-j}$ and $f = \beta^k \alpha^2 \beta^{-k}$ is $\beta^j \alpha^2 \beta^{k-j} \alpha^2 \beta^k$ and since $k \not\equiv j \pmod m$ it follows from (i) above together with Lemma 4.3(iii) that $ef \notin D_\alpha$ so that *in the principal factor $D_\alpha \cup \{0\}$, the product of any two distinct idempotents is 0* and in particular $E(D_\alpha \cup \{0\})$ is a semilattice, as required. $\qquad \square$

THEOREM 4.5.

(a) *Any finite orthodox semigroup S may be embedded in a finite orthodox semigroup T generated by two group elements.*

(b) *Any finite orthodox monoid S^1 may be embedded as a semigroup into a finite 2-generated orthodox monoid T whose subband of idempotents satisfy the same semigroup identities.*

Proof.

(a) From Proposition 4.4, we need only check that, given that S is orthodox, the idempotents of our containing semigroup T form a band. Consider $E(T) = E \cup F \cup \{0\}$ as described in Theorem 4.5. Products involving 0 are 0 and the product of any two members of E is also 0 unless they have identical second and third co-ordinates j say. In this case we have a product of idempotents in the semigroup $T_{1,j} \cong S$ by Theorem 3.6(ii): in particular the product is itself an idempotent as S is orthodox.

Next, let $\rho = \beta^j \alpha^2 \beta^{-j}$ and $\mu = \beta^k \alpha^2 \beta^{-k}$ be two distinct members of F. Since the product $\rho\mu$ has the factor $\alpha\beta^{-j+k}\alpha$ with $k - j \not\equiv 0 \pmod m$, it follows

from Theorem 4.5 (iii) and (v) that either $\rho\mu = 0$ or dom $\rho\mu \subseteq X \times \{i\}$ say. Routine calculation then gives that, if defined, $(x, i) \cdot \rho\mu = (x \cdot ef, i)$ for some idempotents $e, f \in E(S)$. Since $ef \in E(S)$ it follows that $\rho\mu = \lambda(ef, i, i) \in E(T)$. In detail we have, working modulo m with $i + j \equiv m_t \pmod m$ say:

$$(x, i) \cdot \rho = (x, i) \cdot \beta^j \alpha^2 \beta^{-j} = (x, m_t) \cdot \alpha^2 \beta^{-j} = (x \cdot \alpha_{t\pm n}, m_{t\pm n}) \cdot \alpha\beta^{-j}$$
$$= (x \cdot \alpha_{t\pm n}\alpha_t, m_t)\beta^{-j} = (x \cdot \alpha_{t\pm n}\alpha_t, i);$$

now α_t is inverse to $\alpha_{t\pm n}$, so this final product can be written as $(x \cdot e, i)$, where $e = \alpha_{t\pm n}\alpha_t \in E(S)$. By the same token, applying this calculation now to $(x \cdot e, i) \cdot \mu$ yields the required expression $(x \cdot ef, i)$ where $ef \in E(S)$ as claimed previously. Hence $\rho\mu = \lambda(ef, i, i) \in E$.

Finally let $\lambda = \lambda(e, i, i) \in E$ and $\rho = \beta^j\alpha^2\beta^{-j} \in F$ as above. If $\lambda\rho \neq 0$ then $\lambda\rho$ has the form $\lambda\rho = (ef, i, i) \in E(T)$ as $E(S)$ is a band. On the other hand $\rho\lambda \neq 0$ implies that $(x, i) \cdot \rho\lambda = (x \cdot fe, i, i)$ for some $f \in E(S)$ whence $\rho\lambda \in E(T)$. In detail the relevant calculations are as follows. If $\lambda\rho \neq 0$ then dom $\lambda\rho \subseteq X \times \{i\}$, $i + j \equiv m_t \pmod m$ say and

$$(x, i) \cdot \lambda\rho = (x \cdot e, i) \cdot \beta^j\alpha^2\beta^{-j} = (x \cdot e, m_t) \cdot \alpha^2\beta^{-j} = (x \cdot e\alpha_{t\pm n}, m_{t\pm n}) \cdot \alpha\beta^{-j}$$
$$= (x \cdot e\alpha_{t\pm n}\alpha_t, m_t) \cdot \beta^{-j} = (x \cdot e\alpha_{t\pm n}\alpha_t, i),$$

and, as before, $\alpha_{t\pm n}\alpha_t = f \in E(S)$ and so $ef \in E(S)$ as S is orthodox. Hence $(x, i) \cdot \lambda\rho = (x \cdot ef, i)$ and it follows that $\lambda\rho = \lambda(ef, i, i) \in E$.

Now consider $\rho\lambda$ and suppose that $\rho\lambda \neq 0$. We have by Lemma 3.2 applied to ρ that dom $\rho\lambda \subseteq X \times \{k\}$ say. However $(X \times \{k\})\rho$ meets dom $\lambda \subseteq X \times \{i\}$ and since ρ is idempotent we have that ρ maps the interval $X \times \{i\}$ into itself and we deduce that $k = i$. Now we have $i + j \equiv m_t \pmod m$ say and we obtain:

$$(x, i) \cdot \rho\lambda = (x, i) \cdot \beta^j\alpha^2\beta^{-j}\lambda = (x, m_t) \cdot \alpha^2\beta^{-j}\lambda = (x \cdot \alpha_{t\pm n}, m_{t\pm n}) \cdot \alpha\beta^{-j}\lambda$$
$$= (x \cdot \alpha_{t\pm n}\alpha_t, m_t)\beta^{-j}\lambda = (x \cdot \alpha_{t\pm n}\alpha_t, i) \cdot \lambda = (x \cdot fe, i),$$

where $f = \alpha_{t\pm n}\alpha_t \in E(S)$ as before and again $fe \in E(S)$ as S is orthodox. Therefore $\rho\lambda = \lambda(fe, i, i) \in E$, as required to complete the proof.

(b) Following Remark 3.8, only the case where $|E(S^1)| \geq 2$ is of interest. As in the proof of Corollary 3.7, we may take a typical semigroup identity $\phi : p = q$ satisfied by S^1 to be homotypical, meaning that each variable in ϕ appears in both p and q. Since we are considering identities on bands, we may assume that ϕ has more than one variable. We need to check is that $E(T)$ also satisfies ϕ.

By Lemma 4.3(iii) it follows that any product uv of two distinct members $u, v \in F = E(T) \cap D_\alpha$ falls out of D_α and lies in T_1. It follows, again from Lemma 4.3(iii), that either $uv = 0$ (the empty map) or dom(uv), ran(uv) are contained in some interval Y_i say. In the latter case $uv = (u|Y_i)(v|Y_i)$. Since the restrictions $u_i = u|Y_i$ and $v_i = v|Y_i$ each belong to $E_i = \{\lambda(e, i, i) : e \in S\}$, the product $uv = u_iv_i$ is equal to a product of two idempotents in E_i.

Now let us consider the words $p(x_1, \ldots, x_t)$ and $q(x_1, \ldots, x_r)(r \geq 2)$ of the identity ϕ and let us substitute elements of $E(T)$ to obtain products $P = p(t_1, \ldots, t_r)$ and $Q = q(t_1, \ldots, t_r)$. We need to verify that $P = Q$. Since each

product involves at least 2 members of $E(T)$, it follows from the argument of above that each t_j may be replaced by a member of $E(T_1)$ without changing the value of either of the products P and Q, so without loss we may assume that $t_1, \ldots, t_r \in E(T_1)$. Hence each $t_j \in E_i$ for some i that depends on j. Consider the set of subscripts $I = \{i : t_j \in E_i\}$. If $|I| = 1$ then both P and Q are products of idempotents in some $E_i \cong E(S)$ and so $P = Q$ as $E(S)$ satisfies ϕ. On the other hand, if $|I| \geq 2$ then $P = Q = 0$ as each of P and Q contains a product of the form uv with $u \in E_i$, $v \in E_j$ with $i \neq j$. In either event, it follows that ϕ is satisfied by $E(T)$ also, thus completing the proof of Theorem 4.6(b). $\square$

Specialising to the case where $E(S)$ is a semilattice and noting that $E(S)$ is a semilattice if and only if the same is true of $E(S^1)$ gives the main corollary (Corollary 2.2) of the construction of [**8**] that the finite symmetric inverse semigroup I_n embeds in a 2-generator inverse susbsemigroup of I_{n+2}.

COROLLARY 4.6. *(McAlister, Stephen and Vernitski)* *Every finite inverse semigroup may be embedded in a finite 2-generated semigroup that is an inverse semigroup.*

REFERENCES

1. C. Benzaken and H. C. Mayr, Noti on de demi-bande: Demi-bandes de type deux, *(French) Semigroup Forum* **10**(2) (1975), 115–128.

2. T. Evans, Embedding theorems for multiplicative systems and projective geometries, *Proc. American Math. Soc* **3** (1952), 614–620.

3. T. E. Hall, Inverse and regular semigroups and amalgamation: a brief survey, in *Proc. of the Symposium on regular semigroups, Northern Illinois University*, (1979), 49–79.

4. P. M. Higgins, *Techniques of semigroup theory* (OUP, Oxford, 1992).

5. J. M. Howie, *Fundamentals of semigroup theory* (OUP, Oxford, 1995).

6. R. P. Hunter, *On Certain Two Generator Monoids*, Semigroup Forum, Vol. **47** (1993), 96–100.

7. S. Margolis, *Maximal pseudovarieties of finite monoids and semigroups* Russian Mathematics (Izvestiya VUZ, Matematika), 1995, 39:1.

8. D. B. McAlister, J. B. Stephen and A. Vernitski, Embedding I_n in a 2-generator inverse subsemigroup of I_{n+2}, *Proceedings of the Edinburgh Mathematical Society* (2002) 45, 1–4.

9. A. M. Mian and S. D. Chowla, On the B_2-sequences of Sidon, *Proc. Nat. Acad. Sci. India* **A14** (1944), 3–4.

10. B. H. Neumann, Embedding theorems for semigroups, *J. London Math. Soc.* **35** (1960), (184–192).

11. W. Sierpinski, Sur les suites infinies de fonctions dîfinies dans les ensembles quelconques, *Fund. Math.* **24** (1935), 209–212.