LARGEST 2-GENERATED SUBSEMIGROUPS OF THE SYMMETRIC INVERSE SEMIGROUP

J. M. André, V. H. Fernandes and J. D. Mitchell

Abstract The symmetric inverse monoid $\mathcal{I}_n$ is the set of all partial permutations of an n-element set. The largest possible size of a 2-generated subsemigroup of $\mathcal{I}_n$ is determined. Examples of semigroups with these sizes are given. Consequently, if $M(n)$ denotes this maximum, it is shown that $M(n)/|\mathcal{I}_n| \to 1$ as $n \to \infty$. Furthermore, we may deduce, the already known fact, that $\mathcal{I}_n$ embeds as a local submonoid of an inverse 2-generated subsemigroup of $\mathcal{I}_{n+1}$.

AMS 2000 *Mathematics subject classification:* Primary 20M20
Secondary 20M18

1. Introduction and the statements of the main theorems

The topic of embedding a semigroup into a 2-generated semigroup is classical. Sierpiński [11] and Banach [1] proved that every countable semigroup, being isomorphic to a semigroup of mappings on $\mathbb{N}$, can be embedded in a 2-generated subsemigroup of the monoid of all mappings from $\mathbb{N}$ to $\mathbb{N}$. Evans [2] and Neumann [8] followed with their own proofs, involving presentations and wreath products, respectively. As a consequence of Neumann's proof it follows that any finite semigroup can be embedded in a finite 2-generator semigroup. A more elementary method can be used to prove the same result. If $\mathcal{T}_n$ denotes the monoid of all mappings from an n-element set to itself, then the semigroup theoretic analogue of Cayley's theorem for groups states that every semigroup with $n-1$ elements embeds in a subsemigroup of $\mathcal{T}_n$. In McAlister *et al.* [7] it is shown that $\mathcal{T}_n$ embeds in a 2-generator subsemigroup of $\mathcal{T}_{n+1}$. Thus Neumann's result is obtained.

The topic of this paper is, however, not semigroups in general but a special class of semigroups called *inverse semigroups*. Ash (see Hall [4]) proved that every countable inverse semigroup S can be embedded in a 4-generator inverse semigroup T. That is, a 4-generator subsemigroup that happens to be an inverse semigroup itself. A *partial permutation* of a set X is just an injective mapping with domain contained in or equal to X. Ash's result can be obtained by proving that any countable collection of partial permutations on $\mathbb{N}$ can be generated by two such partial permutations and their inverses; see [3, Proposition 4.2]. If S happens to be finite, then it is also shown in [4] that S embeds in a finite T. A different proof of this is given in [7]. Again analogous to Cayley's theorem, every inverse semigroup embeds in the *symmetric inverse monoid* $\mathcal{I}_n$, the monoid of all partial permutations of an n-element set. The result then follows from the fact that $\mathcal{I}_n$ embeds in an 2-generator inverse subsemigroup of $\mathcal{I}_{n+2}$; see [7].

Recently, Holzer and König [5] attempted to answer the question: what is the largest possible size of a 2-generated subsemigroup of $\mathcal{T}_n$? Their paper connects the standard study of 2-generated semigroups to theoretical computer science. Amongst other things, Holzer and König show that, when n is prime, the largest 2-generated subsemigroup of $\mathcal{T}_n$ lies in a class of explicitly defined semigroups. The precise semigroup in this class, with largest size, is, as yet, unknown except for small values of n. Answering the question when n is not a prime seems to be a rather difficult problem. After attempting to find such an answer, without success, we followed Pólya's advice [10], and considered a seemingly more straightforward question. The outcome of this consideration is the topic of this paper. The intention is to prove the following theorems:

Theorem 1.1. *If $n \geq 10$ is even, then the largest size of a 2-generated subsemigroup of $\mathcal{I}_n$ is*

$$\mathfrak{e}(n) = \epsilon(n) + \frac{1}{36}(n^6 + 3n^5 + 13n^4 - 411n^3 + 1390n^2 - 1320n + 36)(n-3)! + \sum_{r=0}^{n-4} \binom{n}{r}^2 r!,$$

where $\epsilon(n) = 3(n-3)$, if $3 \nmid n$, and $\epsilon(n) = 2(n-3)$, if $3|n$. Moreover, there are inverse subsemigroups of $\mathcal{I}_n$ generated by 2 elements with size $\mathfrak{e}(n)$.

Theorem 1.2. *If $n \geq 7$ is odd,then the largest size of a 2-generated subsemigroup of $\mathcal{I}_n$ is*

$$\mathfrak{o}(n) = 2n - 4 + \frac{1}{4}(n^4 + 2n^3 - 23n^2 + 36n - 12)(n-2)! + \sum_{r=0}^{n-3} \binom{n}{r}^2 r!.$$

Moreover, there are inverse subsemigroups of $\mathcal{I}_n$ generated by 2 elements with size $\mathfrak{o}(n)$.

These theorems are proved in Sections 3 and 4. The cases when $n < 10$ is even and when $n < 7$ is odd are considered in Section 5. The semigroup $\mathcal{I}_n$ is itself 2-generated when $n < 3$. A corollary of the construction, in Section 4, of subsemigroups with sizes $\mathfrak{o}(n)$ and $\mathfrak{e}(n)$, is a slight improvement of the main theorem of [7]. That is, $\mathcal{I}_n$ can be embedded, as a local submonoid, in an inverse 2-generated subsemigroup of $\mathcal{I}_{n+1}$. It is stated in the acknowledgements of [7] that this result was obtained by the referee of the paper. For undefined terms in, and further information about, semigroup theory consult [6].

2. Preliminaries

Before beginning the proofs of Theorems 1.1 and 1.2, a few observations and definitions are required. If X is a subset of a semigroup S, then denote by $\langle\, X \,\rangle$ the subsemigroup generated by X. That is, the semigroup where every element can be given as a product of elements from X. The *domain* of $\alpha \in \mathcal{I}_n$ is the set $\mathrm{dom}(\alpha) = \{\, x \,:\, x\alpha \text{ is defined} \,\}$, and the *image* of $\alpha \in \mathcal{I}_n$ is the set $\mathrm{im}(\alpha) = \{\, x\alpha \,:\, x \in \mathrm{dom}(\alpha) \,\}$. The *rank* of α is simply the size of its image, denoted by $\mathrm{rank}(\alpha)$. If α is a permutation of its image, then $\langle\, \alpha \,\rangle$ is a cyclic group. Thus it is possible to refer to the order of α, which is denoted by $|\alpha|$.

There are $\binom{n}{r}$ possible domains and $\binom{n}{r}$ possible images of elements in $\mathcal{I}_n$ with rank r. Moreover, there are $r!$ partial permutations with a fixed image and kernel of rank r. It follows that the number of elements of rank r in $\mathcal{I}_n$ is $\binom{n}{r}^2 r!$. Summing over all r gives

$$|\mathcal{I}_n| = \sum_{r=0}^{n} \binom{n}{r}^2 r!.$$

The same line of thought can be used to find an upper bound for the size of any subsemigroup U of $\mathcal{I}_n$. If the elements with rank r in U admit $d(r)$ distinct domains and $i(r)$ distinct images, then, as above, there are at most $d(r)i(r)r!$ elements with rank r in U. So, summing over all r yields

$$|U| \leq \sum_{r=0}^{n} d(r)i(r)r!. \tag{2.1}$$

The form of $\mathfrak{e}(n)$ and $\mathfrak{o}(n)$ given in Theorems 1.1 and 1.2 arose as simplifications of the slightly longer expressions given below:

$$\mathfrak{e}(n) = \epsilon(n) + (n-3)^2(n-1)! + \left[\binom{n}{2} - 3\right]^2 (n-2)! + \left[\binom{n}{3} - 1\right]^2 (n-3)! + \sum_{r=0}^{n-4} \binom{n}{r}^2 r! \tag{2.2}$$

and

$$\mathfrak{o}(n) = 2n - 4 + (n-2)^2\,(n-1)! + \left[\binom{n}{2} - 1\right]^2 (n-2)! + \sum_{r=0}^{n-3} \binom{n}{r}^2 r!. \tag{2.3}$$

These lengthier versions of $\mathfrak{e}(n)$ and $\mathfrak{o}(n)$ also make their relationship with $|\mathcal{I}_n|$ more apparent.

3. Not larger than $\mathfrak{e}(n)$ or $\mathfrak{o}(n)$

In this section, we prove that any 2-generated subsemigroup of $\mathcal{I}_n$ has size at most $\mathfrak{e}(n)$, in the even case, and at most $\mathfrak{o}(n)$, in the odd case. At several points in this section, an upper bound on the order of any element of the symmetric group of degree $m \leq n$ is required. The largest order of an element in $\mathcal{S}_m$ is known as *Landau's function* $\lambda(m)$, and it is the greatest least common divisor of any partition of m. Several tight bounds are known for Landau's function. However, for our purposes it will suffice to note that, if $m \geq 4$, and $\alpha \in \mathcal{S}_m$, then by induction on m we obtain

$$|\alpha| \leq (m-1)!. \tag{3.1}$$

Let us begin in earnest by proving that any pair of nonpermutations in $\mathcal{I}_n$ generate semigroups with size less than $\mathfrak{e}(n)$.

Lemma 3.1. *If $\alpha, \beta \in \mathcal{I}_n \setminus \mathcal{S}_n$ and $n \geq 5$, then $|\langle\, \alpha, \beta\,\rangle| \leq \mathfrak{e}(n) < \mathfrak{o}(n)$.*

Proof. By (2.2) and (2.3),

$$\mathfrak{o}(n) - \mathfrak{e}(n) \geq \frac{1}{3}(n-3)!(13n^3 - 54n^2 + 47n + 15) - n + 5 \geq (n-3)! - n + 5 > 0,$$

when $n \geq 5$. Therefore $\mathfrak{e}(n) < \mathfrak{o}(n)$ for all $n \geq 5$.

If a and b are elements missing from the images of α and β, then any element in $\langle\, \alpha, \beta\,\rangle$ is missing either a or b from its image. Likewise, if $c \notin \operatorname{dom}(\alpha)$ and $d \notin \operatorname{dom}(\beta)$, then either $c \notin \operatorname{dom}(\mu)$ or $d \notin \operatorname{dom}(\mu)$ for all $\mu \in \langle\, \alpha, \beta\,\rangle$. Thus it is not possible to choose all the elements missing from $\mathrm{im}(\mu)$ or $\mathrm{dom}(\mu)$ from the complement of $\{a, b\}$ or $\{c, d\}$, respectively. It follows that the number of distinct domains, and images, that elements of $\langle\, \alpha, \beta \,\rangle$ with rank r admit is at most $\binom{n}{r} - \binom{n-2}{r-2}$. Inequality (2.1) tells us that

$$|\langle\, \alpha, \beta \,\rangle| \leq \sum_{r=0}^{n-1} \left[\binom{n}{r} - \binom{n-2}{r-2}\right]^2 r!. \tag{3.2}$$

Now, the proof is completed by showing that the coefficients of each of the terms $r!$ in (3.2) are not greater than the corresponding coefficients in (2.2). When $r = 0, 1, \ldots, n-4$ this is obvious. Simplify the remaining terms in (3.2) to obtain

$$4(n-1)! + \left[\binom{n}{2} - \binom{n-2}{2}\right]^2 (n-2)! + \left[\binom{n}{3} - \binom{n-2}{3}\right]^2 (n-3)!.$$

Comparing these coefficients with those in (2.2), $4 \leq (n-3)^2$, $\binom{n-2}{2} \geq 3$, and $\binom{n-2}{3} \geq 1$ when $n \geq 5$ and the result follows. □

If $\alpha, \beta \in \mathcal{S}_n$, then $|\langle\, \alpha, \beta \,\rangle| \leq n! < \mathfrak{e}(n)$ when $n \geq 4$. Therefore it remains to prove that any permutation together with any nonpermutation in $\mathcal{I}_n$ generate a subsemigroup with size less than $\mathfrak{e}(n)$, in the even case, and less than $\mathfrak{o}(n)$, in the odd case. The next simple lemma is used in the proof of both cases. Denote by α_i the cycle of $\alpha \in \mathcal{S}_n$ containing the number i.

Lemma 3.2. *If $\alpha \in \mathcal{S}_n$ and $\beta \in \mathcal{I}_n \setminus \mathcal{S}_n$ with $a \notin \mathrm{dom}(\beta)$ and $b \notin \mathrm{im}(\beta)$, then*

$$|\langle\, \alpha, \beta \,\rangle| \leq |\alpha| + \sum_{r=0}^{s} \left[\binom{n}{r} - \binom{n-t}{n-r}\right]^2 r!,$$

where $s = \mathrm{rank}(\beta)$ and $t = \max\{|\alpha_a|, |\alpha_b|\}$.

Proof. Any element $\mu \neq \alpha^i$, for any i, of $\langle \alpha, \beta \rangle$ can be written as $\alpha^i\beta\omega\beta\alpha^j$, or $\alpha^i\beta\alpha^j$, for some i, j and $\omega \in \langle \alpha, \beta \rangle$. Thus, $a\alpha^{-i} \notin \mathrm{dom}(\mu)$ and $b\alpha^j \notin \mathrm{im}(\mu)$. In other words, there is an element in α_a that is not in $\mathrm{dom}(\mu)$ and an element in α_b that is not in $\mathrm{im}(\mu)$. So, as in the proof of Lemma 3.1, the number of distinct domains that elements of $\langle\, \alpha, \beta \,\rangle$ with rank r admit is at most $\binom{n}{r} - \binom{n-|\alpha_a|}{n-r} \leq \binom{n}{r} - \binom{n-t}{n-r}$. Likewise, the number of distinct images that elements of $\langle \alpha, \beta \rangle$ with rank r admit is at most $\binom{n}{r} - \binom{n-|\alpha_b|}{n-r} \leq \binom{n}{r} - \binom{n-t}{n-r}$.

The inequality in the lemma now follows from (2.1) and the fact that for all $\mu \in \langle \alpha, \beta \rangle$, $\mathrm{rank}(\mu) \leq s$ or $\mathrm{rank}(\mu) = n$. □

Using Lemma 3.2 it is now possible to prove the main result of this section in the case that n is even.

Lemma 3.3. *If $n \geq 10$ is even, $\alpha \in \mathcal{S}_n$, and $\beta \in \mathcal{I}_n \setminus \mathcal{S}_n$, then $|\langle\, \alpha, \beta \,\rangle| \leq \mathfrak{e}(n)$.*

Proof. Let $a \notin \mathrm{dom}(\beta)$ and $b \notin \mathrm{im}(\beta)$. Assume without loss of generality that $|\alpha_a| \leq |\alpha_b|$. If $|\alpha_b| = n-3$, then the inequality $|\langle \alpha, \beta \rangle| \leq \mathfrak{e}(n)$ follows directly from Lemma 3.2. When $|\alpha_b| \leq n-4$, it suffices to prove that

$$|\alpha| + \sum_{r=n-3}^{n-1} \left[\binom{n}{r} - \binom{4}{n-r}\right]^2 r! < \epsilon(n) + \sum_{r=n-3}^{n-1} \left[\binom{n}{r} - \binom{3}{n-r}\right]^2 r!.$$

This is equivalent to proving that

$$(n-1)! = (n-1)(n-2)(n-3)! \leq \epsilon(n) + (6n^3 - 25n^2 + 6n + 25)(n-3)!,$$

since $|\alpha| \leq (n-1)!$ by (3.1). To prove the second inequality it is enough to show that $(n-1)(n-2) < 6n^3 - 25n^2 + 6n + 25$ for $n \geq 10$ since $\epsilon(n) > 0$ when $n \geq 4$. It is possible to do this using elementary calculus. Indeed, take the real-valued functions $f(x) = x^2 - 3x + 2 = (x-1)(x-2)$ and $g(x) = 6x^3 - 25x^2 + 6x + 25$. Then $f(10) = 72 < 3585 = g(10)$. Moreover, if $x \geq 3$, then $f'(x) < 2x < 2x(9x-25) < 18x^2 - 50x + 6 = g'(x)$.

It remains to consider what happens when $|\alpha_b| = n-2, n-1$, or n. Note that in this case, since n is even, $|\alpha| \leq n$. If N is the number of elements of $\langle\, \alpha, \beta \,\rangle$ of rank $n-1$, we prove that

$$N \leq |\alpha|^2 (n-2)! \leq n^2 (n-2)!. \tag{3.3}$$

If $\text{rank}(\beta) < n-1$, then there are no elements of rank $n-1$ and (3.3) is satisfied. Assume that $\text{rank}(\beta) = n-1$. There are two cases to consider.

First, if $b\alpha^i \neq a$, for all i, then any product of αs and βs, containing more than 1 occurrence of β, has rank at most $n-2$. Consequently, there are at most $|\alpha|^2 \leq n^2$ elements of rank $n-1$.

Second, if there exists $i \in \mathbb{Z}$ such that $b\alpha^i = a$, then $\text{dom}(\alpha^i\beta) = \text{im}(\alpha^i\beta)$ and the unique element not in this set is b. Note that since $\alpha^i\beta$ is a permutation of its domain, which has size $n-1$, $|\alpha^i\beta| \leq (n-2)!$ by (3.1). As in the previous case, we will prove that every element of $\langle\, \alpha, \beta \,\rangle$ with rank $n-1$ has the form $\alpha^j(\alpha^i\beta)^k\alpha^l$ for some j, k, l. To this end observe that if $x\alpha^k = x$, for some k and some x in α_b, then $y\alpha^k = y$ for all y in α_b. Moreover, since $|\alpha_b| = n-2, n-1$ or n, and n is even, it follows that α^k is the identity 1_n permutation. Taking the contrapositive, if $\alpha^k \neq 1_n$, then $y\alpha^k \neq y$ for all y in α_b. In particular, $b\alpha^k \neq b$. Therefore every element of the form $\omega_1(\alpha^i\beta)\alpha^k(\alpha^i\beta)\omega_2$, $\omega_1, \omega_2 \in \langle \alpha, \beta \rangle$ and $\alpha^k \neq 1_n$, has rank at most $n-2$. It follows from this that if $\beta\alpha^k\beta$ is a factor of an element in $\langle\, \alpha, \alpha^i\beta \,\rangle = \langle\, \alpha, \beta \,\rangle$ with rank $n-1$, then $k = i$. Thus any element of rank $n-1$ has the form $\alpha^j(\alpha^i\beta)^k\alpha^l$ and there are at most $|\alpha|^2\,|\alpha^i\beta| \leq n^2(n-2)!$ elements of this type. Hence

$$h(n) = n + n^2(n-2)! + \sum_{r=0}^{n-2} \binom{n}{r}^2 r! \geq |\langle\, \alpha, \beta \,\rangle|.$$

To complete the proof we show that

$$\mathfrak{e}(n) - h(n) = \epsilon(n) - n + \left(n^4 - \frac{40}{3}n^3 + 41n^2 - \frac{110}{3}n + 1\right)(n-3)! > 0,$$

when $n \geq 10$.

Now, $\epsilon(n) - n > n - 6 > 0$ when $n \geq 7$ and so it suffices to prove that

$$n^4 - \frac{40}{3}n^3 + 41n^2 - \frac{110}{3}n + 1 > 0$$

when $n \geq 10$. As above, take the real valued function $k(x) = x^4 - \frac{40}{3}x^3 + 41x^2 - \frac{110}{3}x + 1$. Then $k(10) = 401$ and $k'(x) = 4x^3 - 40x^2 + 82x - \frac{110}{3} > 4x^3 - 40x^2 + 80x - 40 =$

$4x(x^2 - 10x + 20) - 40$. Now, $x(x - 10) \geq 0 > -19$ when $x \geq 10$. Thus $x^2 - 10x + 20 > 1$ and so $k'(x) > 0$ when $x \geq 10$. □

Finally, and again using Lemma 3.2, it is possible to prove the main result in the case that n is odd.

Lemma 3.4. *If $n \geq 7$ is odd, $\alpha \in \mathcal{S}_n$, and $\beta \in \mathcal{I}_n \setminus \mathcal{S}_n$, then $|\langle\, \alpha, \beta \,\rangle| \leq \mathfrak{o}(n)$.*

Proof. Let $a \notin \operatorname{dom}(\beta)$ and $b \notin \operatorname{im}(\beta)$. Assume without loss of generality that $|\alpha_a| \leq |\alpha_b|$. If $|\alpha_b| = n-2$, then the inequality $|\langle\, \alpha, \beta \,\rangle| \leq \mathfrak{o}(n)$ follows directly from Lemma 3.2. If $|\alpha_b| \leq n - 3$, then, by Lemma 3.2, it suffices to prove that

$$|\alpha| + \sum_{r=n-2}^{n-1} \left[\binom{n}{r} - \binom{3}{n-r}\right]^2 r! < 2n - 4 + \frac{1}{4}(n^4 + 2n^3 - 23n^2 + 36n - 12)(n-2)!$$

or, equivalently, to prove that

$$(n-1)! \leq 2n - 4 + (4n^2 - 9n - 3)(n-2)!,$$

since $|\alpha| < (n-1)!$. When $n \geq 3$, $2n(2n - 5) > 2$ and so $4n^2 - 9n - 3 > n - 1$ and the result follows in this case.

Now, assume that the length of $|\alpha_b|$ is $n - 1$ or n. As in the proof of Lemma 3.3, if N denotes the number of elements of $\langle\, \alpha, \beta \,\rangle$ with rank $n - 1$, then

$$N \leq |\alpha|^2\,(n-2)! \leq n^2(n-2)!.$$

Therefore $|\langle\, \alpha, \beta \,\rangle| \leq n + n^2(n-2)! + \sum_{r=0}^{n-2} \binom{n}{r}^2 r!$. Now, $2n - 4 > n$ when $n \geq 5$ and the coefficients of $r!$, $r \neq n - 2$, in the two sums are equal. So, we need only verify that the coefficient of $(n-2)!$ in $\mathfrak{o}(n)$, as shown in Theorem 1.2, is greater than that in the last sum. In other words, we must prove that

$$\begin{aligned}\frac{1}{4}(n^4 + 2n^3 - 23n^2 + 36n - 12) &- \left[n^2 + \binom{n}{2}^2\right] \\ &= \frac{1}{4}(n^4 + 2n^3 - 23n^2 + 36n - 12) - \frac{1}{4}(n^4 - 2n^3 + 5n^2) \\ &= \frac{1}{4}(4n^3 - 28n^2 + 36n - 12) > 0.\end{aligned}$$

But $0 < 4n(n-6)(n-1) - 12$ when $n \geq 7$ and $4n(n-6)(n-1) - 12 = 4n(n^2 - 7n + 6) - 12 < 4n(n^2 - 7n + 9) - 12 = 4n^3 - 28n^2 + 36n - 12$, as required. It follows that $|\langle\, \alpha, \beta \,\rangle| \leq \mathfrak{o}(n)$ for $n \geq 7$. □

4. Realising $\mathfrak{e}(n)$ and $\mathfrak{o}(n)$

In this section, we complete the proofs of Theorems 1.1 and 1.2 by proving that there are 2-generated subsemigroups of $\mathcal{I}_n$ with size $\mathfrak{e}(n)$ and $\mathfrak{o}(n)$. This necessitates two examples to cover the cases when n is odd, and when n is even.

The proof of the following elementary result, reportedly first proved in [9], will be required to prove that our two examples are 2-generated.

Lemma 4.1. *If $n \neq 4$ and α is any nonidentity permutation of degree n, or $n = 4$ and $\alpha \neq (1\,2)(3\,4)$, $(1\,3)(2\,4)$, or $(1\,4)(2\,3)$, then there exists $\beta \in \mathcal{S}_n$ such that $\langle\, \alpha, \beta \,\rangle = \mathcal{S}_n$.*

The first of our examples, $\mathcal{O}(n)$ is defined to be

- all powers of the permutation $\alpha = (1\,2\,\cdots\,n-2)(n-1\,n)$;
- all elements $\mu \in \mathcal{I}_n$ where there exist $d, i \in \{1, 2, \ldots, n-2\}$ such that $d \notin \mathrm{dom}(\mu)$ and $i \notin \mathrm{im}(\mu)$.

If $\mu \in \mathcal{O}(n)$, then $\mu^{-1} : x\mu \mapsto x$, $x \in \mathrm{im}(\mu)$, is the unique inverse of μ in $\mathcal{I}_n$. But there exist $i, d \in \{1, 2, \ldots, n-2\}$ such that $d \notin \mathrm{dom}(\mu) = \mathrm{im}(\mu^{-1})$ and $i \notin \mathrm{im}(\mu) = \mathrm{dom}(\mu^{-1})$. This implies that $\mu^{-1} \in \mathcal{O}(n)$ and so $\mathcal{O}(n)$ is an inverse subsemigroup of $\mathcal{I}_n$. The next lemma shows that $\mathcal{O}(n)$ has the desired size and number of generators.

Lemma 4.2. *If $n \geq 5$ is odd, then $|\mathcal{O}(n)| = \mathfrak{o}(n)$ and $\mathcal{O}(n)$ is 2-generated.*

Proof. The first conclusion, that $|\mathcal{O}(n)| = \mathfrak{o}(n)$, follows immediately by (2.3), and since n is odd. Since $n-2$ is odd, $\alpha^{n-2} = (n-1n)$. Thus, if

$$\beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ - & 3 & 4 & \cdots & n & 2 \end{pmatrix},$$

then together α^{n-2} and β generate all permutations on $\{2, 3, \ldots, n\}$. So, $\beta^{n-1} = 1_{\{2,\ldots,n\}}$, the partial identity with domain $\{2, \ldots, n\}$. If $m = 0, 1, \ldots, n-3$, then

$$\alpha^{-m}\beta^{n-1}\alpha^m = 1_{\{1,2,\ldots,n\}\setminus\{m+1\}}$$

and so

$$1_{\{m+2,\ldots,n\}} = \beta^{n-1}(\alpha^{-1}\beta^{n-1}\alpha)(\alpha^{-2}\beta^{n-1}\alpha^2)\cdots(\alpha^{-m}\beta^{n-1}\alpha^m).$$

The partial identity $1_{\{n\}}$ is produced by taking the composition $1_{\{n-1,n\}}\pi 1_{\{n-1,n\}}$ where $\pi \in \langle\, \alpha^{n-2}, \beta \,\rangle$ is the permutation on $\{2, 3, \ldots, n\}$ that swaps $n-2$ and $n-1$. Likewise, the empty mapping is produced by taking the composition $1_{\{n\}}\sigma 1_{\{n\}}$ where σ is the permutation that swaps n and $n-1$.

Let $\mu \in \mathcal{O}(n)$ be arbitrary with $d, i \in \{1, 2, \ldots, n-2\}$ such that $d \notin \mathrm{dom}(\mu)$ and $i \notin \mathrm{im}(\mu)$. If $\mathrm{rank}(\mu) = n$ or 0, then μ is a power of α or the empty mapping. Either way $\mu \in \langle\, \alpha, \beta \,\rangle$.

Assume that $\mathrm{rank}(\mu) = n - m$ for some $m \in \{1, 2, \ldots, n-1\}$. Then $1 \notin \mathrm{dom}(\mu)\alpha^{-d+1}$ and $1 \notin \mathrm{im}(\mu)\alpha^{-i+1}$. It follows that 1 is in neither the domain nor the image of $\alpha^{d-1}\mu\alpha^{-i+1}$. Therefore there exists a (partial) permutation $\hat{\mu} \in \langle\, \alpha, \beta \,\rangle$ of $\{2, 3, \ldots, n\}$ such that $\hat{\mu}|_{\mathrm{dom}(\mu)\alpha^{-d+1}} = \alpha^{d-1}\mu\alpha^{-i+1}$.

Then let ν be any permutation of $\{2, 3, \ldots, n\}$ such that

$$\{m+1, \ldots, n\}\nu = \mathrm{dom}(\mu)\alpha^{-d+1}.$$

Of course, $\nu \in \langle\, \alpha, \beta \,\rangle$. With this definition

$$\alpha^{-d+1}\nu^{-1}1_{\{m+1,\ldots,n\}}\nu\alpha^{d-1} = \alpha^{-d+1}1_{\mathrm{dom}(\mu)\alpha^{-d+1}}\alpha^{d-1} = 1_{\mathrm{dom}(\mu)}.$$

So, to conclude, if $x \in \mathrm{dom}(\mu)$, then

$$(x)1_{\mathrm{dom}(\mu)}\alpha^{-d+1}\hat{\mu}\alpha^{i-1} = (x\alpha^{-d+1})\hat{\mu}\alpha^{i-1} = (x\alpha^{-d+1})\alpha^{d-1}\mu\alpha^{-i+1}\alpha^{i-1} = x\mu,$$

and $1_{\mathrm{dom}(\mu)}\alpha^{-d+1}\hat{\mu}\alpha^{i-1}$ is undefined on the complement of $\mathrm{dom}(\mu)$. Thus $\mu \in \langle \alpha, \beta \rangle$. □

The second of the required semigroups, $\mathcal{E}(n)$, is defined to be

- all powers of the permutation $\alpha = (1\,2 \cdots n-3)(n-2\;n-1)$, or $(1\,2\cdots n-3)(n-2\;n-1\;n)$, when $3|n$ or $3\nmid n$, respectively;
- all elements $\mu \in \mathcal{I}_n$ with $d, i \in \{1, 2, \ldots, n-3\}$ satisfying $d \notin \mathrm{dom}(\mu)$ and $i \notin \mathrm{im}(\mu)$.

It is possible to verify that $\mathcal{E}(n)$ is an inverse subsemigroup of $\mathcal{I}_n$ in the same way that $\mathcal{O}(n)$ was shown to be.

Lemma 4.3. *If $n \geq 6$ is even, then $|\mathcal{E}(n)| = \mathfrak{e}(n)$ and $\mathcal{E}(n)$ is 2-generated.*

Proof. As in the proof of Lemma 4.2, the first conclusion, that $|\mathcal{E}(n)| = \mathfrak{e}(n)$, follows immediately by (2.2), and since n is even. If $3|n$, then $\alpha^{n-3} = (n-2\;n-1)$, and if $3\nmid n$, then $\alpha^{n-3} = (n-2\;n-1\;n)$. In either case, Lemma 4.1 guarantees that it is possible to find a permutation β of $\{2, 3, \ldots, n\}$ such that together α^{n-3} and β generate all permutations of $\{2, 3, \ldots, n\}$. For example, if $3|n$, then β can be

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ - & 3 & 4 & \cdots & n & 2 \end{pmatrix},$$

and if $3\nmid n$, then β can be

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-2 & n-1 & n \\ - & 3 & 4 & \cdots & 2 & n & n-1 \end{pmatrix}.$$

The rest of the proof is, more or less, identical to that of Lemma 4.2 and, for brevity, it is omitted. □

5. Small values, asymptotics, and embedding $\mathcal{I}_n$ in $\mathcal{I}_{n+1}$

As the title suggests, in this section some small values of the maximum size $M(n)$ of a 2-generated subsemigroup of $\mathcal{I}_n$ are given. When $n \geq 7$ and odd, or $n \geq 10$ and even, $M(n)$ is precisely $\mathfrak{o}(n)$ or $\mathfrak{e}(n)$, respectively. The asymptotic behaviour of the ratio $M(n)/|\mathcal{I}_n|$ is also studied. The first few values of $M(n)$ are given in Tables 1 and 2. The values when $n = 3$ or 4, were obtained by computation. The remaining values, when $n = 5, 6$, or 8, were obtained using Lemma 3.1 and arguments analogous to those used in the proof of Lemmas 3.3 and 3.4. The largest 2-generated subsemigroups of $\mathcal{I}_n$ in these cases are not always the same as the semigroups $\mathcal{O}(n)$ and $\mathcal{E}(n)$. The following two examples describe 2-generated semigroups with the largest possible size when $n = 3, 4, 5, 6$, and 8.

n	4	6	8	10	12	14
$M(n)$	141^*	8509^*	1079625^*	200798485	48777044515	15243109621301

Table 1.

n	3	5	7	9	11	13	15
$M(n)$	31^*	934^*	103692	15561168	3180734980	860918107056	299336064843732

Table 2.

Example 5.1. If $n = 3$, then the partial permutations

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 \\ - & 1 & 3 \end{pmatrix},$$

generate an inverse subsemigroup of $\mathcal{I}_n$ with size 31. Moreover, this semigroup consists of all partial permutations of $\{1, 2, 3\}$ with rank at most 2 and the powers of α. The semigroup $\mathcal{O}(5)$ has size 934.

Example 5.2. When $n = 4, 6$ or 8, the semigroups with the largest possible size are found by taking a cycle α of order n in $\mathcal{S}_n$ together with a group element β of rank $n-1$ with maximum possible order, that is, $3, 6$, or 12, respectively. The semigroup $\langle\, \alpha, \beta \,\rangle$ contains all the elements of rank at most $n-2$, $n^2|\beta|$ elements of rank $n-1$ and the n powers of α.

The paper is concluded by making some easy observations.

Lemma 5.3. *The sequence $M(n)/|\mathcal{I}_n|$ tends to* 1 *as n tends to ∞.*

Proof. The sequence $\mathfrak{o}(n)/|\mathcal{I}_n|$ tends to 1 as n tends to infinity. Thus, since $\mathfrak{o}(n) \leq \mathfrak{e}(n+1)$, the result follows. $\square$

From the definition of the semigroups $\mathcal{O}(n)$ and $\mathcal{E}(n)$ we deduce the following results. As mentioned in the introduction this is already known, see [7].

Theorem 5.4. *The inverse semigroup $\mathcal{I}_n$, $n \geq 4$, can be embedded, as a local submonoid, in an inverse* 2*-generated subsemigroup of $\mathcal{I}_{n+1}$.*

Proof. It is well-known that the symmetric inverse monoid on the set $\{2, 3, \ldots, n\}$ is generated by the permutations $(2\,3)$, $(2\,3\,\ldots\,n)$ and the idempotent

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ - & - & 3 & \cdots & n-1 & n \end{pmatrix},$$

see, for example, [6, Exercise 5.11.6]. From the definition of $\mathcal{O}(n)$ and $\mathcal{E}(n)$ it is clear that these three partial permutations are elements of both of these monoids. $\square$

Acknowledgements. The first and second authors were (partially) supported by the FCT and FEDER within the project POCTI-ISFL-1-143 of the Centro de Álgebra da Universidade de Lisboa. The third author would like to acknowledge the support of EPSRC grant number GR/S/56085/01.

References

1. S. Banach, Sur un theorème de M. Sierpiński, *Fund. Math.* **25** (1935) 5-6.
2. T. Evans, Embedding theorems for multiplicative systems and projective geometries, *Proc. Amer. Math. Soc.* **3** (1952) 614-620.
3. P.M. Higgins, J. M. Howie, J. D. Mitchell and N, Ruškuc, Countable versus uncountable ranks in infinite semigroups of transformations and relations, *Proc. Edinb. Math. Soc.* **46** (2003) 531-544.
4. T. E. Hall, Inverse and regular semigroups and amalgamation: a brief survey, in *Symp. on Regular Semigroups, Northern Illinois University, 1979.*
5. M. Holzer and B. König, On deterministic finite automata and syntactic monoid size, *Theoret. Comput. Sci.* **327** (2004) 319-347.
6. J.M. Howie, *Fundamentals of semigroup theory*, London Mathematical Society, New Series **12**, Oxford Science Publications, The Clarendon Press, Oxford University Press (1995).
7. D. B. McAlister, J. B. Stephen, and A. S. Vernitski, Embedding $\mathcal{I}_n$ in a 2-generator inverse subsemigroup of $\mathcal{I}_{n+2}$, *Proc. Edinb. Math. Soc.* (2) **45** (2002) 1-4.
8. B. H. Neumann, Embedding theorems for semigroups, *J. London Math. Soc.* **35** 1960 184-192.
9. S. Picard, Sur les bases du groupe symetrique et du groupe alternant, *Math. Ann.* **116** (1939) 752-767.
10. G. Pólya, *How to solve it*, Princeton Science Library, Princeton University Press, (1988).
11. W. Sierpiński, Sur les suites infinies de fonctions définies dans les ensembles quelconques, *Fund. Math.* **24** (1935) 209-212.

J. M. André and V. H. Fernandes:
Centro de Álgebra da Universidade de Lisboa,
Av. Prof. Gama Pinto, 2,
1649-003 Lisboa, Portugal
and
Departamento de Matemática,
Faculdade de Ciências e Tecnologia
da Universidade Nova de Lisboa,
Monte da Caparica,
2829-516 Caparica,
Portugal.
email: jmla@fct.unl.pt and vhf@fct.unl.pt

J. D. Mitchell:
Mathematical Institute,
University of St Andrews,
North Haugh,
St Andrews,
Fife,
KY16 9SS
Scotland.
email: jdm3@st-and.ac.uk