

## KROHN-RHODES COMPLEXITY PSEUDOVARITIES ARE NOT FINITELY BASED \*

JOHN RHODES<sup>1</sup> AND BENJAMIN STEINBERG<sup>2</sup>

**Abstract.** We prove that the pseudovariety of monoids of Krohn-Rhodes complexity at most  $n$  is not finitely based for all  $n > 0$ . More specifically, for each pair of positive integers  $n, k$ , we construct a monoid of complexity  $n + 1$ , all of whose  $k$ -generated submonoids have complexity at most  $n$ .

**Mathematics Subject Classification.** 20M07.

### 1. INTRODUCTION

The Krohn-Rhodes theorem [10] shows that any semigroup  $S$  – in this paper all semigroups are finite – divides a wreath product of aperiodic semigroups and groups (a semigroup is *aperiodic* if all its subgroups are trivial [5]; a semigroup  $S$  *divides*  $T$  if  $S$  is a quotient of a subsemigroup of  $T$  – in this case  $S$  is said to be a *divisor* of  $T$  [5, 12]). The Krohn-Rhodes *complexity* of  $S$ , denoted  $c(S)$ , is the least number of group factors appearing in any such wreath product decomposition of  $S$  [11, 12, 26, 29]. The problem of finding an algorithm to compute the complexity of a semigroup has been the driving open problem in the field for nearly 40 years. The first author has recently announced a solution to the problem: the proof is in preparation.

Eilenberg [5] introduced the notion of a pseudovariety as an organizing tool in the theory. Recall that a *pseudovariety* of semigroups (monoids) is a class of semigroups (monoids) closed under taking divisors and forming direct products.

---

*Keywords and phrases.* Complexity, finite basis problem, the presentation lemma.

\* *The second author was supported in part by NSERC and by POCTI approved project POCTI/32817/MAT/2000 in participation with the European Community Fund FEDER.*

<sup>1</sup> Department of Mathematics, University of California at Berkeley, Berkeley, CA 94720, USA; rhodes@math.berkeley.edu

<sup>2</sup> School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada; bsteinbg@math.carleton.ca

Let  $\mathbf{A}$  denote the pseudovariety of aperiodic semigroups (monoids) and  $\mathbf{G}$  the pseudovariety of groups. Define  $\mathbf{C}_0 = \mathbf{A}$  and, inductively,

$$\mathbf{C}_n = \mathbf{A} * \mathbf{G} * \mathbf{C}_{n-1},$$

where  $*$  denotes the semidirect product of pseudovarieties [5]. Then

$$\mathbf{C}_n = \{S \mid c(S) \leq n\}.$$

In this paper, we shall deal with the monoidal version of the problem since the analogous results for semigroups follow from our monoidal results.

The goal of this paper is to prove that  $\mathbf{C}_n$  is not finitely based for any positive integer  $n$ : that is, there is no finite set of pseudoidentities [1] defining  $\mathbf{C}_n$ . This result is significant because it shows there that is no “cheap” algorithm for deciding complexity by simply checking a finite list of computable pseudoidentities. To accomplish our goal, we prove the following stronger result, which is our main theorem.

**Theorem 1.1.** *For each  $n, k > 0$  there is a monoid  $S_{n,k}$  of complexity  $n+1$ , each of whose  $k$ -generated submonoids has complexity at most  $n$ .*

Obtaining the finite basis result from the above theorem is standard, so we proceed to do it now.

**Theorem 1.2.** *For each  $n > 0$ ,  $\mathbf{C}_n$  is not finitely based.*

*Proof.* Let us assume by way of contradiction that  $\mathbf{C}_n$  is finitely based. Then it can be defined by a finite set  $E$  of pseudoidentities in, say,  $k$  variables. Since any substitution of these variable into  $S_{n,k}$  lives inside of a  $k$ -generated submonoid and such submonoids belong to  $\mathbf{C}_n$ , it follows that  $S_{n,k}$  satisfies  $E$ . But  $c(S_{n,k}) = n+1$ , a contradiction.  $\square$

We remark that Theorem 1.1 implies that, for  $n > 0$ , any pseudovariety of semigroups in the interval  $[\mathbf{C}_n, \mathbf{LC}_n]$  is not finitely based, where  $\mathbf{LC}_n$  is the pseudovariety of semigroups whose monoid subsemigroups belong to  $\mathbf{C}_n$ . It was shown by the first author [4, 15] (see also [25]) that  $\mathbf{C}_1 \neq \mathbf{LC}_1$ ; in fact, in general  $\mathbf{C}_n \neq \mathbf{LC}_n$  (announced by Rhodes in the seventies and written up in [18] using techniques from this paper).

To prove Theorem 1.1 for  $n = 1$ , we make use of the second author’s variant [25] of the presentation lemma [4]. The construction of  $S_{1,k}$  is inspired by an example of the first author [4, 15], but with a twist due to the second author. The case  $n > 1$  is dealt with by applying the iterated Rees matrix techniques, first introduced by Zalcstein [31], that have been exploited to great advantage by the first author [15–17, 20].

The paper is essentially divided into two parts: the case  $n = 1$  and the case  $n > 1$ . The case  $n = 1$  begins with some background on the presentation lemma and then gets into the construction of  $S_{1,k}$ ; the case  $n > 1$  begins with some strengthening of the results of [19, 20] and then uses iterated matrix techniques to construct  $S_{n,k}$  for  $n > 1$ .

## HISTORICAL NOTE

An earlier version of this paper, authored just by the second author and containing only the result for  $n = 1$ , was previously circulated; shortly afterwards, in joint work, the authors extended the result to the general case, leading to the paper in its current form.

## 2. THE PRESENTATION LEMMA

The presentation lemma was proved by the first author in the seventies, but was first published in [4]. It arose out of the work in [20, 27] and especially [15]. Tilson [30], in an unpublished paper, formulated a coordinate-free version. This was expanded on and generalized by the second author in [25] and it is this version of things that we shall use here.

We begin by recalling the fundamental lemma of complexity [14, 29], which states that

$$\mathbf{C}_n = \mathbf{A} \textcircled{m} (\mathbf{G} * \mathbf{C}_{n-1}),$$

where  $\textcircled{m}$  denotes the Malcev product of pseudovarieties; recall that  $S \in \mathbf{V} \textcircled{m} \mathbf{W}$  if  $S$  has a relational morphism to a member of  $\mathbf{W}$  such that the inverse images of idempotents belong to  $\mathbf{V}$ ; a *relational morphism*  $\varphi : S \rightarrow T$  of semigroups (monoids) is a map  $\varphi : S \rightarrow 2^T \setminus \emptyset$  such that  $s_1\varphi s_2\varphi \subseteq (s_1 s_2)\varphi$  ( $1 \in 1\varphi$ ) [5].

Let  $S$  be a monoid and  $J$  a regular  $\mathcal{J}$ -class. Then the second author defined [25] a *cross-section* for  $J$  over a pseudovariety  $\mathbf{V}$  to be a relational morphism  $\varphi : S \rightarrow T \in \mathbf{V}$  such that, for  $x, y \in J$ ,

$$x\varphi \cap y\varphi \neq \emptyset \text{ and } x \mathcal{H} y \implies x = y.$$

The second author then proved [25] (which follows from [13], Prop. 5.7, of which he was unaware):

**Theorem 2.1.**  *$S \in \mathbf{A} \textcircled{m} \mathbf{V}$  if and only if there is a cross-section over  $\mathbf{V}$  for every regular  $\mathcal{J}$ -class of  $S$ .*

In particular,  $S \in \mathbf{C}_n$ ,  $n > 1$ , if and only if each regular  $\mathcal{J}$ -class of  $S$  has a cross-section over  $\mathbf{G} * \mathbf{C}_{n-1}$ . The second author's version [25] of the presentation lemma [4] characterizes when a regular  $\mathcal{J}$ -class has a cross-section over  $\mathbf{G} * \mathbf{V}$ .

**Theorem 2.2** (presentation lemma). *S has a cross-section over  $\mathbf{G} * \mathbf{V}$  for a regular  $\mathcal{J}$ -class J if and only if  $(R, S)$  has a presentation over  $\mathbf{V}$  where R is an  $\mathcal{R}$ -class of J (the existence of a presentation is independent of the choice of R).*

Of course, we now owe the reader an explanation as to what is a presentation. We first need to recall the notion of a parameterized relational morphism of partial transformation semigroups [5,25]. In this paper, we do **not** assume that partial transformation semigroups are faithful. A parameterized relational morphism  $\Phi : (X, S) \rightarrow (Q, T)$  of partial transformation semigroups consists of a fully defined relation  $\varphi_1 : X \rightarrow Q$  and a relational morphism  $\varphi_2 : S \rightarrow T$  such that, for each  $x \in X, s \in S$  for which  $xs$  is defined,

$$x\varphi_1 s\varphi_2 \subseteq (xs)\varphi_1. \tag{2.1}$$

Let us set up some notation: if  $f$  is a relation, then  $\#f$  shall denote the graph of  $f$ . The derived partial transformation semigroup of  $\Phi$  is  $\mathcal{D}_\Phi = (\#\varphi_1, D_\Phi)$ , where  $D_\Phi$  consists of elements  $(q, (s, t), q')$  with  $qt \subseteq q'$  and  $(s, t) \in \#\varphi_2$  and where the action is given by

$$(x, q)(q, (s, t), q') = \begin{cases} (xs, q') & xs \neq \emptyset \\ \emptyset & \text{otherwise;} \end{cases} \tag{2.2}$$

see [5]. Here, following [5], we write  $qt \subseteq q'$  to mean either  $qt$  is undefined, or  $qt = q'$ . We shall always view  $\mathcal{D}_\Phi$  as an automaton with state set  $\#\varphi_1$ , alphabet  $D_\Phi$  and with transitions given by (2.2).

A congruence on an automaton  $\mathcal{A}$  is an equivalence relation  $\mathcal{P}$  on the state set such that

$$q \mathcal{P} q' \text{ and } qa, q'a \neq \emptyset \implies qa \mathcal{P} q'a. \tag{2.3}$$

The quotient automaton  $\mathcal{A}/\mathcal{P}$  is defined in the natural way; namely there is an arrow labelled by  $a$  from the class of  $q$  to the class of  $q'$  if and only if there exist  $\tilde{q} \mathcal{P} q$  and an edge  $\tilde{q} \xrightarrow{a} \tilde{q}'$  of  $\mathcal{A}$  with  $\tilde{q}' \mathcal{P} q'$ . A congruence is called *injective* if the dual condition holds:

$$qa, q'a \neq \emptyset \text{ and } qa \mathcal{P} q'a \implies q \mathcal{P} q'. \tag{2.4}$$

This happens precisely when the transition monoid of  $\mathcal{A}/\mathcal{P}$  acts by injective partial functions.

Finally, we can define a presentation. If  $R$  is a regular  $\mathcal{R}$ -class of  $S$ , then recall that  $S$  acts on the right of  $R$  by partial transformations *via* the Schützenberger representation (called the right mapping representation in [12]) and so there results a partial transformation semigroup  $(R, S)$  (which is not in general faithful). A

*presentation* for  $(R, S)$  over  $\mathbf{V}$  is a pair  $(\Phi, \mathcal{P})$  where  $\Phi : (R, S) \rightarrow (Q, T)$  is a parameterized relational morphism with  $T \in \mathbf{V}$  and  $\mathcal{P}$  is an injective congruence on  $\mathcal{D}_\Phi$  such that:

$$(x, q) \mathcal{P} (y, q') \implies q = q' \text{ and either } x = y \text{ or } x \not\mathcal{H} y. \tag{2.5}$$

### 3. THE CONSTRUCTION AND COMPLEXITY OF $S_{1,k}$

Let  $p_1, p_2, p_3, \dots$  be the primes in increasing order and let  $k \geq 2$  be a positive integer (clearly it suffices to consider  $k \geq 2$  in Th. 1.1). We begin the construction of  $S_{1,k}$  by describing its 0-minimal ideal as a Rees matrix semigroup.

Set  $m = p_1 \cdots p_k$  and  $\overline{p}_i = m/p_i$ . In the following definitions, if  $X$  is a set,  $X'$  will denote a disjoint copy of  $X$ . Let

$$A = \bigcup_{i=1}^k \mathbb{Z}_{\overline{p}_i} \cup \bigcup_{i=1}^k \mathbb{Z}'_{\overline{p}_i} \cup \{0, \dots, m-1\};$$

$$B = \mathbb{Z}_m \cup \mathbb{Z}'_m.$$

If  $r \in \mathbb{Z}$ , we write  $[r]$  for the class of  $r$  in  $\mathbb{Z}_m$ ,  $[r]'$  for the class of  $r$  in  $\mathbb{Z}'_m$ ,  $[r]_i$  for the class of  $r$  in  $\mathbb{Z}_{\overline{p}_i}$  and  $[r]'_i$  for the class of  $r$  in  $\mathbb{Z}'_{\overline{p}_i}$ . Let  $G = \{\pm 1\} \cong \mathbb{Z}_2$ . We define a matrix  $C : B \times A \rightarrow G \cup 0$  by prescribing the non-zero entries, namely

$$C_{[r],[r]_i} = C_{[r]',[r]'_i} = C_{[r]',r} = 1, \tag{3.1}$$

where  $0 \leq r \leq m-1$ . Observe that  $C$  is a zero-one matrix without zero rows or columns and without identical rows or columns. In fact,

$$C = \begin{pmatrix} P & 0_m & 0_m \\ 0_m & P & I_m \end{pmatrix}$$

where  $P$  is the  $m \times \sum_{i=1}^k \overline{p}_i$  matrix whose rows are the characteristic vectors of the incidence structure with vertices the elements of  $\mathbb{Z}_m$  and with blocks given by the cosets of the  $\overline{p}_i \mathbb{Z}_m$ ,  $i = 1, \dots, k$ , and where  $0_m$ , respectively,  $I_m$  is the  $m \times m$  zero, respectively, identity matrix. In plain language, an entry in  $C$  is 1 if it is in a row and column corresponding to elements that are equal modulo an appropriate integer (subject to restrictions involving being primed *vs.* unprimed; *cf.* (3.1)).

For example, when  $k = 2$  (so  $m = 2 \cdot 3 = 6$ ,  $\overline{p}_1 = 6/2 = 3$ ,  $\overline{p}_2 = 6/3 = 2$ ) the matrix is:

| $C$    | $[0]_1$ | $[1]_1$ | $[2]_1$ | $[0]_2$ | $[1]_2$ | $[0]'_1$ | $[1]'_1$ | $[2]'_1$ | $[0]'_2$ | $[1]'_2$ | 0 | 1 | 2 | 3 | 4 | 5 |
|--------|---------|---------|---------|---------|---------|----------|----------|----------|----------|----------|---|---|---|---|---|---|
| $[0]$  | 1       | 0       | 0       | 1       | 0       | 0        | 0        | 0        | 0        | 0        | 0 | 0 | 0 | 0 | 0 | 0 |
| $[1]$  | 0       | 1       | 0       | 0       | 1       | 0        | 0        | 0        | 0        | 0        | 0 | 0 | 0 | 0 | 0 | 0 |
| $[2]$  | 0       | 0       | 1       | 1       | 0       | 0        | 0        | 0        | 0        | 0        | 0 | 0 | 0 | 0 | 0 | 0 |
| $[3]$  | 1       | 0       | 0       | 0       | 1       | 0        | 0        | 0        | 0        | 0        | 0 | 0 | 0 | 0 | 0 | 0 |
| $[4]$  | 0       | 1       | 0       | 1       | 0       | 0        | 0        | 0        | 0        | 0        | 0 | 0 | 0 | 0 | 0 | 0 |
| $[5]$  | 0       | 0       | 1       | 0       | 1       | 0        | 0        | 0        | 0        | 0        | 0 | 0 | 0 | 0 | 0 | 0 |
| $[0]'$ | 0       | 0       | 0       | 0       | 0       | 1        | 0        | 0        | 1        | 0        | 1 | 0 | 0 | 0 | 0 | 0 |
| $[1]'$ | 0       | 0       | 0       | 0       | 0       | 0        | 1        | 0        | 0        | 1        | 0 | 1 | 0 | 0 | 0 | 0 |
| $[2]'$ | 0       | 0       | 0       | 0       | 0       | 0        | 0        | 1        | 1        | 0        | 0 | 0 | 1 | 0 | 0 | 0 |
| $[3]'$ | 0       | 0       | 0       | 0       | 0       | 1        | 0        | 0        | 0        | 1        | 0 | 0 | 0 | 1 | 0 | 0 |
| $[4]'$ | 0       | 0       | 0       | 0       | 0       | 0        | 1        | 0        | 1        | 0        | 0 | 0 | 0 | 0 | 1 | 0 |
| $[5]'$ | 0       | 0       | 0       | 0       | 0       | 0        | 0        | 1        | 0        | 1        | 0 | 0 | 0 | 0 | 0 | 1 |

Let  $I = \mathcal{M}^0(G, A, B, C)$  be the associated Rees matrix semigroup [12]. The monoid  $S_{1,k}$  will be an ideal extension of  $I$  and will act faithfully on both the left and right of  $I$ ; that is,  $S_{1,k}$  will be a group mapping monoid with distinguished 0-minimal ideal  $I$  [12]. Set  $J = I \setminus 0$ . Note that since  $I$  is a zero-one matrix with no identical rows or columns, it follows quite easily [12] that  $I$  acts faithfully on the right and left of itself.

Let  $H = \langle h \rangle$  be a cyclic group of order  $m$  generated by  $h$ , written multiplicatively. Let  $t$  be a new element whose action will be defined below and let  $N = HtH = \{h^i t h^j \mid 0 \leq i, j \leq m - 1\}$ . As a set, we define

$$S_{1,k} = H \cup N \cup I.$$

The group of units of  $S_{1,k}$  will be  $H$ . It's clear how  $H$  multiplies against elements of  $S_{1,k} \setminus J$ ; we now define how  $H$  acts on  $J$ ; it suffices to consider  $h$ . Define

$$(a, g, [r])h = (a, g, [r - 1]) \tag{3.2}$$

$$(a, g, [r]')h = (a, g, [r - 1]') \tag{3.3}$$

$$h([r]_i, g, b) = ([r + 1]_i, g, b) \tag{3.4}$$

$$h([r]'_i, g, b) = ([r + 1]'_i, g, b) \tag{3.5}$$

$$h(r, g, b) = \begin{cases} (r + 1, g, b) & r \neq m - 1 \\ (0, g, b) & r = m - 1. \end{cases} \tag{3.6}$$

Note that there are  $2k + 1$  orbits of  $H$  on the  $\mathcal{R}$ -classes of  $J$ ; this will play an important role in the proof.

It's clear how  $N$  multiplies against  $H \cup 0$ . Define  $N^2 = 0$ . It remains to show how  $N$  multiplies against  $J$ . For this, it suffices to show how  $t$  acts on  $J$ . Define

$$(a, g, [0]')t = (a, -g, [0]) \tag{3.7}$$

$$(a, g, [1]')t = (a, g, [1]) \tag{3.8}$$

$$t([0]_i, g, b) = (0, -g, b) \tag{3.9}$$

$$t([1]_i, g, b) = (1, g, b) \tag{3.10}$$

and all other products involving  $t$  and  $J$  to be 0.

It is straightforward to check the associativity of  $S_{1,k}$ . It is clear from the definitions that  $U = H \cup N \cup 0$  is a monoid acting faithfully on the left of  $I$  by left translations and faithfully on the right of  $I$  by right translations. So the only checks to be made involve products of the form  $(a, g, b)u(\tilde{a}, \tilde{g}, \tilde{b})$  with  $u \in U \setminus 0$  (this is just checking the linked equations [12]); we provide a sample computation – the other verifications are similar.

$$\begin{aligned} ((a, g, [0]')t)([0]_i, \tilde{g}, b) &= (a, -g, [0])([0]_i, \tilde{g}, b) = (a, -g\tilde{g}, b) \\ (a, g, [0]')(t([0]_i, \tilde{g}, b)) &= (a, g, [0]')(0, -\tilde{g}, b) = (a, -g\tilde{g}, b). \end{aligned}$$

We try here to motivate the construction for those familiar with presentation lemma arguments. If  $\mathcal{M}^0(G, A, B, C)$  is a Rees matrix semigroup, then two elements of  $B$  are said to be *attached* if there is an element  $a \in A$  such that  $C_{ba} \neq 0 \neq C_{b'a}$ . TCA then denotes the transitive closure of being attached: this is an equivalence relation on  $B$ . Dual definitions apply to  $A$ . See [4, 6, 15, 20, 24–26] for more information (the latter two papers use TA where we use TCA). The idea of the construction of  $S_{1,k}$  is that the two  $H$ -orbits on the  $\mathcal{L}$ -classes form TCA-blocks of  $B$ . However, removing  $H$ -orbits on the  $\mathcal{R}$ -classes collapses this. Having opposite signs in (3.7) and (3.8) forces the complexity to be two as long as the  $H$ -orbits on the  $\mathcal{L}$ -classes remain TCA blocks, but as soon as the TCA structure is ruined, the complexity drops to one. Note that in order to define the action of  $t$  as we have, we need that  $[0]$  and  $[1]$  are not attached in  $B$  and  $0$  and  $1$  are not attached in  $A$ ; this accounts for why we have a copy of  $I_m$  in  $C$ .

Recall that the *depth* of a semigroup  $S$  is the size of the longest chain of  $\mathcal{J}$ -classes containing non-trivial groups [28]. The depth decomposition theorem [28] states that the depth is an upper bound for complexity. Since the  $\mathcal{J}$ -class structure of  $S_{1,k}$  is

$$H >_{\mathcal{J}} N >_{\mathcal{J}} J >_{\mathcal{J}} 0,$$

it follows that the depth of  $S_{1,k}$  is two and hence  $c(S_{1,k}) \leq 2$ ; clearly  $c(S_{1,k}) \geq 1$ . Before proving that  $c(S_{1,k}) = 2$ , we state the following elementary group-theoretic lemma whose proof we omit.

**Lemma 3.1.** *Let  $G$  be a group,  $H_1, \dots, H_r \leq G$  and  $K = \langle H_1, \dots, H_r \rangle$ . Define  $g \equiv_i g'$  if  $H_i g = H_i g'$ . Then the equivalence relation  $\equiv$  generated by the  $\equiv_i$  is given by  $g \equiv g' \iff Kg = Kg'$ .  $\square$*

**Theorem 3.2.**  $c(S_{1,k}) = 2$ .

*Proof.* Suppose, by way of contradiction, that  $c(S_{1,k}) = 1$ . Then

$$S_{1,k} \in \mathbf{A} \textcircled{m}(\mathbf{G} * \mathbf{A})$$

and so there must be a cross-section for  $J$  over  $\mathbf{G} * \mathbf{A}$ . Hence, by the presentation lemma (Th. 2.2), there is a presentation  $(\Phi, \mathcal{P})$  over  $\mathbf{A}$  for  $(R, S_{1,k})$  where  $R = [0]_1 \times G \times B \leq J$ . Suppose  $\Phi = (\varphi_1, \varphi_2) : (R, S_{1,k}) \rightarrow (Q, T)$  with  $T$  aperiodic.

Since  $T$  is aperiodic and  $H$  is a group, a standard argument (cf. [4, 25]) shows that there is an idempotent  $e \in T$  such that  $H \subseteq e\varphi_2^{-1}$ . Choose  $p \in ([0]_1, 1, [0]')\varphi_1$  and set  $q' = pe$ . Then

$$[0]_1 \times 1 \times \mathbb{Z}'_m = ([0]_1, 1, [0]')H \subseteq (pe)\varphi_1^{-1} = q'\varphi_1^{-1}$$

by (2.1). So  $([0]_1 \times 1 \times \mathbb{Z}'_m) \times q' \subseteq \#\varphi_1$ .

The following claim is an example of what the first author calls the ‘‘Tie-your-shoes’’ Trivium [4, 25].

**Claim 3.3.** Let  $r, l \in \mathbb{Z}$ . Then

$$((([0]_1, 1, [r]'), q'), \mathcal{P} (([0]_1, 1, [l]'), q')). \tag{3.11}$$

*Proof.* Define  $[r]' \equiv [l]'$  if (3.11) holds. Clearly  $\equiv$  is an equivalence relation on  $\mathbb{Z}'_m$ . Suppose first that  $[r]'_i = [l]'_i$ , where  $i \in \{1, \dots, k\}$  and let  $s = ([r]'_i, 1, [r]')$ . Choose  $\tilde{s} \in s\varphi_2$ . Then in  $\mathcal{D}_\Phi$  we have:

$$\begin{aligned} (([0]_1, 1, [r]'), q')(q', (s, \tilde{s}), q'\tilde{s}) &= (([0]_1, 1, [r]'), q'\tilde{s}) \\ &= (([0]_1, 1, [l]'), q')(q', (s, \tilde{s}), q'\tilde{s}). \end{aligned}$$

Since  $\mathcal{P}$  is an injective congruence, we conclude (3.11) holds when  $[r]'_i = [l]'_i$ .

It now follows that  $\equiv$  contains the equivalence relations of congruence modulo  $\overline{p_i}\mathbb{Z}'_m$  for each  $i = 1, \dots, k$  and hence, by Lemma 3.1, it contains the equivalence relation on  $\mathbb{Z}'_m$  of congruence modulo  $\sum_{i=1}^k \overline{p_i}\mathbb{Z}'_m$ . But since

$$\gcd(\overline{p_1}, \dots, \overline{p_k}) = 1,$$

$\sum_{i=1}^k \overline{p_i}\mathbb{Z}'_m = \mathbb{Z}'_m$ , establishing the claim. □

Let  $t_0 \in t\varphi_2$ ; notice that  $t_0e \in t\varphi_2\varphi_1 \subseteq t\varphi_2$ , so without loss of generality we may assume  $t_0e = t_0$ . Then, by (3.9), (3.10) and (2.1),

$$[0]_1 \times G \times \mathbb{Z}_m = ([0]_1 \times 1 \times \mathbb{Z}'_m)tH \subseteq (q't_0e)\varphi_1^{-1} = q\varphi_1^{-1},$$

where  $q = q't_0 = q't_0e$ . Hence  $([0]_1 \times G \times \mathbb{Z}_m) \times q \subseteq \#\varphi_1$ .



The proof of the following claim is identical to that of the proof of Claim 3.3.

**Claim 3.4.** Let  $r, l \in \mathbb{Z}$  and  $g = \pm 1$ . Then

$$([0]_1, g, [r]), q \mathcal{P} ([0]_1, g, [l]), q.$$

Now let us observe that

$$([0]_1, 1, [0]'), q'(q', (t, t_0), q) = ([0]_1, -1, [0]), q \tag{3.12}$$

$$([0]_1, 1, [1]'), q'(q', (t, t_0), q) = ([0]_1, 1, [1]), q. \tag{3.13}$$

Since  $\mathcal{P}$  is a congruence, Claim 3.3, (3.12) and (3.13) show that

$$([0]_1, -1, [0]), q \mathcal{P} ([0]_1, 1, [1]), q. \tag{3.14}$$

So using Claim 3.4 and (3.14), we obtain

$$([0]_1, -1, [0]), q \mathcal{P} ([0]_1, 1, [0]), q,$$

contradicting the definition of a presentation (2.5) since

$$([0]_1, -1, [0]) \mathcal{H} ([0]_1, 1, [0]).$$

Thus  $c(S_{1,k}) = 2$ , as desired. □

#### 4. PROOF OF THEOREM 1.1: THE CASE $n = 1$

We have already shown that  $c(S_{1,k}) = 2$ . It remains to show that every  $k$ -generated submonoid of  $S_{1,k}$  has complexity at most one. Let

$$X = \{t_1, \dots, t_k\} \subseteq S_{1,k}$$

and let  $S$  be the submonoid generated by  $X$ . If  $X \subseteq S_{1,k} \setminus H$ , then

$$S \leq (S_{1,k} \setminus H) \cup 1 = U.$$

But  $U$  is a submonoid of depth one and so  $c(S) \leq c(U) = 1$ .

Thus we are left with the case that  $t_i \in H$  for some  $i$ . We now take advantage of there being  $2k + 1$  orbits of  $H$  on the  $\mathcal{R}$ -classes of  $J$ . Let  $Y = X \setminus t_i$ . Then  $Y$  has  $k - 1$  elements and so there exists  $j \in \{1, \dots, k\}$  such that **no** element of either the form  $([r]_j, g, b)$  or the form  $([r]'_j, g, b)$  belongs to  $Y$ . It is straightforward to verify that

$$S' = S_{1,k} \setminus \left( (\mathbb{Z}_{\overline{p_j}} \cup \mathbb{Z}'_{\overline{p_j}}) \times G \times B \right) \tag{4.1}$$

is a submonoid of  $S_{1,k}$  and  $X \subseteq S'$ . Thus  $c(S) \leq c(S')$  and so to complete the proof of Theorem 1.1, it suffices to show  $c(S') = 1$ . To do this we need to show, by

the fundamental lemma of complexity and Theorem 2.1, that each regular  $\mathcal{J}$ -class of  $S'$  has a cross-section over  $\mathbf{G} * \mathbf{A}$ .

Clearly  $\varphi : S' \rightarrow H \in \mathbf{G} * \mathbf{A}$  given by

$$x\varphi = \begin{cases} x & x \in H \\ H & \text{otherwise} \end{cases}$$

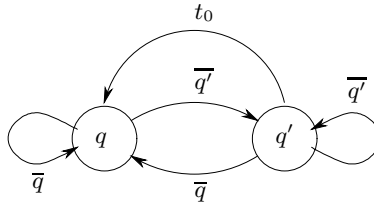
is a cross-section for  $H$ . Let  $J' = J \cap S'$ ; note that  $J'$  is a regular  $\mathcal{J}$ -class of  $S'$  and that the  $\mathcal{J}$ -class structure for  $S'$  is

$$H >_{\mathcal{J}} N >_{\mathcal{J}} J' >_{\mathcal{J}} 0.$$

Let  $R = [0]_a \times G \times B$ , where  $a \neq j$ . Then  $R$  is an  $\mathcal{R}$ -class belonging to  $J'$  and so by the presentation lemma (Th. 2.2) to show that there is a cross-section for  $J'$  over  $\mathbf{G} * \mathbf{A}$ , it suffices to find a presentation for  $(R, S')$  over  $\mathbf{A}$ . We will exploit the TCA structure of  $J'$  – in particular that the TCA blocks of  $J$  split into multiple blocks in  $J'$ .

To motivate the construction of our presentation, we provide the following intuition. The two  $H$ -orbits on  $B$  are “ $\mathbf{A}$ -pointlike” and so shall be represented in an aperiodic partial transformation semigroup  $(Q, T)$  by states  $q, q'$  with  $q$  corresponding to the unprimed orbit and  $q'$  to the primed orbit. We shall cover  $H$  by 1 and cover  $t$  by an element  $t_0$ . The elements of  $J'$  shall be covered by appropriate constant maps.

Formally, let  $Q = \{q, q'\}$  and let  $T$  be the transition monoid of the automaton below.



Then  $(Q, T)$  is a faithful partial transformation semigroup of rank 1 maps and hence  $T$  is aperiodic. In fact,

$$T \cong \mathcal{M}^0(\{1\}, 2, 2, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}) \cup 1$$

where  $\bar{q} = (1, 1, 1)$ ,  $\bar{q}' = (1, 1, 2)$  and  $t_0 = (2, 1, 1)$ .

We define a parameterized relational morphism

$$\Phi = (\varphi_1, \varphi_2) : (R, S') \rightarrow (Q, T)$$

as follows:

$$([0]_a, g, b)\varphi_1 = \begin{cases} q & b \in \mathbb{Z}_m \\ q' & b \in \mathbb{Z}'_m; \end{cases}$$

$\#\varphi_2$  is the submonoid of  $S' \times T$  generated by

$$(H \times 1) \cup (((A \times G \times \mathbb{Z}_m) \cap S') \times \bar{q}) \cup ((A \times G \times \mathbb{Z}'_m) \cap S') \times \bar{q}') \cup (t, t_0). \tag{4.2}$$

It is straightforward to verify that  $\Phi$  is a parameterized relational morphism. Indeed, to verify (2.1), it suffices to verify that if  $(x, y)$  is in (4.2) and  $r \in R$  is such that  $rx$  is defined, then  $r\varphi_1 y \subseteq (rx)\varphi_1$ . But this is clear from (4.2) and the construction of  $(Q, T)$ .

Define an equivalence relation  $\mathcal{P}$  on  $\mathcal{D}_\Phi$  by

$$([0]_a, g, [r], q) \mathcal{P} ([0]_a, g', [s], q) \iff g = g', r \equiv s \pmod{p_j}$$

$$([0]_a, g, [r'], q') \mathcal{P} ([0]_a, g', [s'], q') \iff g = g', r \equiv s \pmod{p_j}. \tag{4.3}$$

Clearly (2.5) holds. Thus to prove  $(\Phi, \mathcal{P})$  is a presentation, it suffices to show  $\mathcal{P}$  is an injective congruence.

**Proposition 4.1.**  *$\mathcal{P}$  is a congruence.*

*Proof.* Suppose

$$x = ([0]_a, g, [r'], q') \mathcal{P} ([0]_a, g, [s'], q') = y$$

and  $z \in \mathcal{D}_\Phi$  is such that  $xz, yz \neq \emptyset$ . There are three cases. Suppose first  $z = (q', (h^i, 1), q')$ , then

$$xz = ([0]_a, g, [r - i]', q'), \quad yz = ([0]_a, g, [s - i]', q')$$

and since  $r \equiv s \pmod{p_j}$ , we have  $r - i \equiv s - i \pmod{p_j}$ . Thus  $xz \mathcal{P} yz$ .

Now suppose  $z = (q', (h^i t h^l, t_0), q)$ . Since  $xz, yz \neq \emptyset$ , either  $[r]' = [s]'$  or  $\{[r - i]', [s - i]'\} = \{[0]', [1]'\}$ . But since  $r \equiv s \pmod{p_j}$ , the second case would imply  $0 \equiv 1 \pmod{p_j}$ , a contradiction. Thus  $x = y$  and so  $xz = yz$ .

The remaining case is  $z = (q', ([l]'_i, g', b), u), \tilde{q})$  some  $i \neq j, u \in T$ . But  $xz, yz$  defined implies  $[r]'_i = [l]'_i = [s]'_i$  and

$$xz = ([0]_a, g g', b), \tilde{q}) = yz.$$

So in all cases  $xz \mathcal{P} yz$ . If  $x, y \in ([0]_a \times G \times \mathbb{Z}_m) \times q, x \mathcal{P} y$  and  $xz, yz \neq \emptyset$ , then an analogous argument, but without the second case, shows that  $xz \mathcal{P} yz$ . We conclude that  $\mathcal{P}$  is a congruence.  $\square$

**Proposition 4.2.**  *$\mathcal{P}$  is injective.*

*Proof.* Suppose  $x = ([0]_a, g, [r]', q'), y = ([0]_a, g', [s]', q')$  and  $z \in \mathcal{D}_\Phi$  is such that  $xz, yz \neq \emptyset$  and  $xz \mathcal{P} yz$ . We show  $x \mathcal{P} y$ . Again, there are three cases. Suppose first  $z = (q', (h^i, 1), q')$ , then

$$xz = ([0]_a, g, [r - i]', q'), \quad yz = ([0]_a, g', [s - i]', q').$$

So  $xz \mathcal{P} yz$  implies  $g = g'$  and  $r - i \equiv s - i \pmod{p_j}$ . But then  $r \equiv s \pmod{p_j}$  and so  $x \mathcal{P} y$ .

Suppose now  $z = (q', (h^i t h^l, t_0), q)$ . Since  $xz$  and  $yz$  are defined, either  $[r]' = [s]'$  or  $\{[r - i]', [s - i]'\} = \{[0]', [1]'\}$ . In the former case, multiplying through by  $z$  and using that  $xz \mathcal{P} yz$  shows that  $g = g'$  and hence  $x = y$ . So assume the latter case. Without loss of generality, we may assume  $[r - i]' = [0]'$ ,  $[s - i]' = [1]'$ . Then

$$(([0]_a, -g, [r - i - l]), q) = xz \mathcal{P} yz = (([0]_a, g', [s - i - l]), q).$$

Hence  $r - i - l \equiv s - i - l \pmod{p_j}$ , whence  $0 \equiv 1 \pmod{p_j}$ , a contradiction. Thus only the former case arises.

The remaining case is  $z = (q', (([l]'_i, g_0, b), u), \tilde{q})$  some  $i \neq j$ ,  $u \in T$ . But  $xz, yz$  defined implies  $[r]'_i = [l]'_i = [s]'_i$ . Hence  $r \equiv s \pmod{\bar{p}_i}$ . Since  $p_j \mid \bar{p}_i$ , we conclude  $r \equiv s \pmod{p_j}$ . Also

$$xz = (([0]_a, g g_0, b), \tilde{q}), \quad yz = (([0]_a, g' g_0, b), \tilde{q}).$$

Since  $xz \mathcal{P} yz$ , we have  $g g_0 = g' g_0$  and so  $g = g'$ . Thus  $x \mathcal{P} y$ .

The case  $x, y \in ([0]_a \times G \times \mathbb{Z}_m) \times q$ ,  $xz, yz \neq \emptyset$  and  $xz \mathcal{P} yz$  is similar, but again the second case doesn't arise. This completes the proof that  $\mathcal{P}$  is injective.  $\square$

These propositions finish the proof that  $(\Phi, \mathcal{P})$  is a presentation and the verification that  $c(S') = 1$ . This establishes Theorem 1.1 and its corollary, Theorem 1.2, for the case  $n = 1$ .

## 5. TYPES I AND II SEMIGROUPS, STABILIZER PAIRS AND POINTLIKE SETS

The goal of this section is to generalize the results of [19, 20] about membership to pointlike sets; we believe the results to be of interest in their own right; they shall be applied in the next section to calculate the complexity of the  $S_{n,k}$ .

Types I and II subsemigroups were introduced in [19, 20]; see also [9, 22, 26]. Let **ER** be the pseudovariety of semigroups whose idempotents generate an  $\mathcal{R}$ -trivial semigroup. Let  $S$  be a semigroup and  $W \leq S$  be a subsemigroup. Then  $W$  is a *Type I* subsemigroup of  $S$  if, for all relational morphisms  $\varphi : S \rightarrow T \in \mathbf{A}$ , there is a semigroup  $T' \leq T$  with  $T' \in \mathbf{ER}$  and  $W \leq T' \varphi^{-1}$ . It is proven in [19] that if  $W$  is generated by a chain  $L_1 >_{\mathcal{L}} \dots >_{\mathcal{L}} L_n$  of its  $\mathcal{L}$ -classes, then it is a Type I subsemigroup.

If  $S$  is a semigroup, the *Type II* subsemigroup (also called the *group kernel*) of  $S$  is

$$\mathbf{K}_{\mathbf{G}}(S) = \bigcap_{\varphi: S \rightarrow G \in \mathbf{G}} 1\varphi^{-1},$$

where  $\varphi$  ranges over all relational morphisms to groups. It was proved by Ash [3], and independently by Ribes and Zalesskiĭ [23], that  $\mathbf{K}_{\mathbf{G}}(S)$  is the smallest subsemigroup of  $S$  containing the set  $E(S)$  of idempotents of  $S$ , which is closed under weak conjugation; see [9] for details.

We shall need the more general notion of a  $\mathbf{V}$ -stabilizer pair (cf. [25]). Fix a semigroup  $S$  and a pseudovariety  $\mathbf{V}$ . Then  $(s, A) \subseteq S \times 2^S$  is a  $\mathbf{V}$ -stabilizer pair if, for all relational morphisms  $\varphi : S \rightarrow T$  with  $T \in \mathbf{V}$ , there exists  $t \in T$  such that  $s \in t\varphi^{-1}$  and  $A \subseteq \text{Stab}_T(t)\varphi^{-1}$ , where

$$\text{Stab}_T(t) = \{u \in T \mid tu = t\}$$

is the right stabilizer of  $t$  in  $T$ . Notice that if  $(x, A)$  is a  $\mathbf{V}$ -stabilizer pair, then  $(x, \langle A \rangle)$  is as well, so we normally assume that  $A$  is a subsemigroup. Observe that  $(s, A)$  is a  $\mathbf{V}$ -stabilizer pair if and only if the graph with 1 vertex labelled by  $s$  and  $|A|$  loops labelled by  $A$  is  $\mathbf{V}$ -inevitable in the sense of Almeida [2] (cf. Ash [3]); see [22] for the related notion of a Type  $\mathbf{V}$  subsemigroup.

Clearly if  $s \in S$ , then  $(s, K_{\mathbf{G}}(S))$  is a  $\mathbf{G}$ -stabilizer pair. We now relate Type I semigroups to  $\mathbf{A}$ -stabilizer pairs; the  $\mathbf{A}$ -stabilizer pairs were characterized in general by Henckell [8]. The following lemma extracts ideas from [22].

**Lemma 5.1.** *Suppose  $W \leq S$  is a Type I subsemigroup and  $e$  is an idempotent in the minimal ideal of  $W$ . Then  $(e, W)$  is an  $\mathbf{A}$ -stabilizer pair.*

*Proof.* Let  $\varphi : S \rightarrow T \in \mathbf{A}$  be a relational morphism. Then since  $W$  is a Type I subsemigroup, there is a subsemigroup  $U \leq T$  with  $U \in \mathbf{ER}$  such that  $W \leq U\varphi^{-1}$ . By shrinking down  $U$ , we can assume  $W\varphi \supseteq U$ . Let  $\psi : W \rightarrow U$  be the restriction. Then  $\psi$  can be factored  $\alpha^{-1}\beta$  where  $\alpha : M \rightarrow W$  and  $\beta : M \rightarrow U$  are onto homomorphisms. Let  $R_e$  be the  $\mathcal{R}$ -class of  $e$  in  $W$ . It is in fact a minimal right ideal of  $W$ , so [12] there is a minimal right ideal  $\tilde{R}$  of  $M$  with  $\tilde{R}\alpha = R_e$ . Let  $R' = \tilde{R}\beta$ ; then  $R'$  is a minimal right ideal of  $U$  [12]. Since  $U \in \mathbf{A} \cap \mathbf{ER}$ ,  $R'$  consists of a single idempotent  $\tilde{e}$  and  $\tilde{e}U = \tilde{e}$ . Hence  $U \leq \text{Stab}_T(\tilde{e})$ . Choosing  $f \in \tilde{R}$  such that  $f\alpha = e$ , we obtain  $\tilde{e} = f\beta \in e\psi$ . Recalling that  $\psi$  is the restriction of  $\varphi$ , we obtain  $W \leq \text{Stab}_T(\tilde{e})\varphi^{-1}$  and  $e \in \tilde{e}\varphi^{-1}$ , thereby establishing that  $(e, W)$  is an  $\mathbf{A}$ -stabilizer pair.  $\square$

Recall that  $X \leq S$  is called  $\mathbf{V}$ -pointlike if, for all relational morphisms  $\varphi : S \rightarrow T$  with  $T \in \mathbf{V}$ , there exists  $t \in T$  such that  $X \leq t\varphi^{-1}$ ;  $X$  is called  $\mathbf{V}$ -idempotent pointlike if one can always choose  $t$  to be an idempotent. Notice that if  $X = X^2$  and  $X$  is  $\mathbf{V}$ -pointlike, then  $X$  is  $\mathbf{V}$ -idempotent pointlike; we remark that Henckell has proved the converse for certain pseudovarieties, including the complexity pseudovarieties [7]. We use  $\text{PL}_{\mathbf{V}}(S)$  to denote the semigroup of  $\mathbf{V}$ -pointlike subsets of  $S$ .

Our reason for considering stabilizer pairs is the following result from [25].

**Lemma 5.2.** *Suppose  $(s, A)$  is a  $\mathbf{V}$ -stabilizer pair for  $S$  with  $A \leq S$  a subsemigroup. Let  $B \in \text{PL}_{\mathbf{W}}(A)$ . Then  $sB \in \text{PL}_{\mathbf{W}*\mathbf{V}}(S)$ .*

We shall use the above lemma in conjunction with the following lemma.

**Lemma 5.3.** *Suppose  $X \in \text{PL}_{\mathbf{V}}(K_{\mathbf{G}}(S))$ . Then*

$$X \in \text{PL}_{\mathbf{V} \circledast \mathbf{G}}(S) \leq \text{PL}_{\mathbf{V}*\mathbf{G}}(S).$$

*Proof.* Let  $\varphi : S \rightarrow T \in \mathbf{V} \textcircled{m} \mathbf{G}$  be a relational morphism. Then there is a relational morphism  $\psi : T \rightarrow G \in \mathbf{G}$  with  $U = 1\psi^{-1} \in \mathbf{V}$ . By definition  $\mathbf{K}_{\mathbf{G}}(S) \leq 1\psi^{-1}\varphi^{-1} = U\varphi^{-1}$ . Let  $\rho : \mathbf{K}_{\mathbf{G}}(S) \rightarrow U$  be the restriction of  $\varphi$ . Since  $U \in \mathbf{V}$ , there exists  $u \in U$  with  $X \subseteq u\rho^{-1}$ . Hence  $X \leq u\varphi^{-1}$ , as desired.  $\square$

The following corollary generalizes the results of [20] to pointlikes.

**Corollary 5.4.** *Let  $S$  be a semigroup,  $W \leq S$  a Type I subsemigroup,  $X \in \text{PL}_{\mathbf{C}_i}(\mathbf{K}_{\mathbf{G}}(W))$  and  $e$  be an idempotent in the minimal ideal of  $W$ . Then  $eX \in \text{PL}_{\mathbf{C}_{i+1}}(S)$ .*

*Proof.* By Lemma 5.3,  $X \in \text{PL}_{\mathbf{C}_i * \mathbf{G}}(W)$ . Since, by Lemma 5.1  $(e, W)$  is an  $\mathbf{A}$ -stabilizer pair in  $S$ , Lemma 5.2 shows that  $eX$  is a  $\mathbf{C}_i * \mathbf{G} * \mathbf{A} = \mathbf{C}_{i+1}$ -pointlike subset of  $S$ .  $\square$

### 6. THE CONSTRUCTION AND COMPLEXITY OF $S_{n,k}$ FOR $n > 1$

The idea in this section is to use iterative matrix constructions to create a semigroup  $S_{n,k}$  containing  $S_{1,k}$  in such a way that the group of units of  $S_{1,k}$  is  $\mathbf{C}_{n-1}$ -pointlike in  $S_{n,k}$ . We first construct some auxiliary semigroups. Fix, for each  $i > 0$ , a cyclic group  $G_i = \langle g_i \rangle$  of order at least three, with identity  $e_i$ . Define recursively sequences of semigroups  $U_1, U_2, \dots$  and  $V_1, V_2, \dots$  as follows. Set  $U_1 = G_1$ ,  $V_1 = \emptyset$ . Define recursively,  $V_i$  to be the Rees matrix semigroup  $\mathcal{M}(U_{i-1}, G_i, G_i, C_i)$  where  $C_i$  is the  $|G_i| \times |G_i|$  matrix with entries  $g_{i-1}$  on the diagonal and  $e_{i-1}$  in all other positions, *i.e.*

$$C_i = \begin{pmatrix} g_{i-1} & e_{i-1} & e_{i-1} & \cdots \\ e_{i-1} & g_{i-1} & e_{i-1} & \cdots \\ & & \ddots & \\ e_{i-1} & e_{i-1} & \cdots & g_{i-1} \end{pmatrix}. \tag{6.1}$$

Define  $U_i = V_i \cup G_i$  where left and right multiplication of  $G_i$  against  $V_i$  are given by

$$\begin{aligned} (a, u, b)g_i &= (a, u, bg_i^{-1}) \\ g_i(a, u, b) &= (g_i a, u, b). \end{aligned} \tag{6.2}$$

It is straightforward to verify that  $U_i$  is a monoid with group of units  $G_i$  and  $V_i$  is an ideal in  $U_i$ . We “canonically” identify  $U_{i-1}$  with the subsemigroup  $e_i \times U_{i-1} \times g_i$  of  $U_i$ . Notice that  $U_1$  is the maximal subgroup of the minimal ideal of  $U_i$ , for all  $i > 0$ . See [16, 17] for more on this type of construction.

**Proposition 6.1.**  $\langle E(U_i) \rangle = V_i \cup e_i$ .

*Proof.* We prove the result by induction on  $i$ . Clearly the result holds when  $i = 1$ . Let  $i > 1$ . Since  $|G_i| > 2$ , a straightforward calculation (*cf.* [6, 15]), considering

the first two rows and three columns of (6.1), shows that  $\mathcal{M}(G_{i-1}, G_i, G_i, C_i)$  is idempotent-generated, from whence it easily follows

$$\langle E(V_i) \rangle = \mathcal{M}(\langle E(U_{i-1}) \cup G_{i-1} \rangle, G_i, G_i, C_i). \tag{6.3}$$

Applying induction to (6.3), we obtain the desired result. □

**Proposition 6.2.**  *$U_i$  is a Type I subsemigroup of itself.*

*Proof.* We prove by induction that  $U_i$  is generated by a chain of its  $\mathcal{L}$ -classes. This is clear for  $U_1$  since it is a group. In general,  $U_i = \langle G_i \cup U_{i-1} \rangle$ . By induction  $U_{i-1}$  is generated by a chain  $L_1 >_{\mathcal{L}} \dots >_{\mathcal{L}} L_r$  of its  $\mathcal{L}$ -classes and so, since  $G_i$  is an  $\mathcal{L}$ -class of  $U_i$  and  $G_i >_{\mathcal{L}} L_1$ ,  $U_i$  is generated by a chain of its  $\mathcal{L}$ -classes. □

**Proposition 6.3.**  *$U_1$  is a  $\mathbf{C}_{i-1}$ -pointlike subset of  $U_i$ .*

*Proof.* The proof is by induction. Since  $U_1$  is a group, it is  $\mathbf{A}$ -pointlike and so the result holds for  $i = 1$ . Suppose the result holds for  $i \geq 1$ ; so  $U_1 \in \text{PL}_{\mathbf{C}_{i-1}}(U_i)$ . Then we have:

- $U_i \leq \langle E(U_{i+1}) \rangle \leq \mathbf{K}_{\mathbf{G}}(U_{i+1})$  by Proposition 6.1;
- $e_1$  is in the minimal ideal of  $U_{i+1}$ ;
- $U_{i+1}$  is a Type I subsemigroup of itself by Proposition 6.2.

Thus  $U_1 = e_1 U_1$  is a  $\mathbf{C}_i$ -pointlike subset of  $U_{i+1}$  by Corollary 5.4. □

**Corollary 6.4.**  *$c(U_i) = i$ .*

*Proof.* Proposition 6.3 shows that  $U_i$  has a non-trivial  $\mathbf{C}_{i-1}$ -pointlike set and so  $c(U_i) \geq i$ . Since  $U_i$  has depth  $i$ ,  $c(U_i) \leq i$  by the depth decomposition theorem [28]. □

We now construct the semigroups  $S_{n,k}$ . Fix  $k \geq 2$ . We define recursively two sequences of semigroups:  $(S_{n,k}), (T_{n,k})$ , for  $n \geq 1$ . Of course,  $S_{1,k}$  has already been defined; set  $T_{1,k} = S_{1,k} \setminus H$ . Let  $G_1 = H$  and  $g_1 = h$ . Let  $e_1$  denote the identity of  $G_1$ . For  $i > 1$ , let  $G_i = \langle g_i \rangle$  be a cyclic group of order 3, with identity  $e_i$ . Define recursively,

$$T_{n,k} = \mathcal{M}(S_{n-1,k}, G_n, G_n, C_n) / (G_n \times 0 \times G_n)$$

where  $C_i$  is as in (6.1). Define  $S_{n,k} = T_{n,k} \cup G_n$  where  $G_n$  acts against  $T_{n,k}$  as per (6.2). It is easy to check that  $S_{n,k}$  is a monoid with group of units  $G_n$  and that  $T_{n,k}$  is an ideal in  $S_{n,k}$ . Finally set  $S_{n,1} = S_{n,2}$  and  $T_{n,1} = T_{n,2}$ .

Analogously to the case of the  $U_i$ , we “canonically” identify  $S_{n-1,k}$  with the subsemigroup  $e_n \times S_{n-1,k} \times g_n$  of  $S_{n,k}$ . In particular, we identify  $S_{1,k}$  with a subsemigroup of  $S_{n,k}$ . By construction one sees that

$$S_{n,k} = U_n \cup N_n \cup J_n \cup 0$$

where  $N_n$  is a null  $\mathcal{J}$ -class,  $J_n$  is a regular  $\mathcal{J}$ -class with maximal subgroup of order 2 (essentially  $N$  and  $J$  of  $S_{1,k}$  blown up) and  $U_n$  is as above. The  $\mathcal{J}$ -classes of  $S_{n,k}$ , in fact, form a chain of length  $n + 3$ , the top  $n$   $\mathcal{J}$ -classes coming from  $U_n$

followed by  $N_n >_{\mathcal{J}} J_n >_{\mathcal{J}} 0$ . We may conclude that the depth of  $S_{n,k}$  is  $n + 1$  and so  $c(S_{n,k}) \leq n + 1$  by the depth decomposition theorem [28].

**Proposition 6.5.**  $c(S_{n,k}) = n + 1$ .

*Proof.* By Proposition 6.3,  $G_1 = U_1$  is a  $\mathbf{C}_{n-1}$ -pointlike subset of  $U_n$  and hence  $S_{n,k}$ . Since  $G_1$  is a monoid, it is, in fact,  $\mathbf{C}_{n-1}$ -idempotent pointlike. Also  $G_1$  is the group of units of our canonically embedded copy of  $S_{1,k}$  in  $S_{n,k}$ . Now the exact same presentation lemma computations performed in Section 3 to show that  $c(S_{1,k}) = 2$  apply here to show that  $c(S_{n,k}) = n + 1$ ; the sole difference is that one now uses the fact that  $G_1$  is  $\mathbf{C}_{n-1}$ -idempotent pointlike to justify that it relates to an idempotent under any relational morphism to a semigroup in  $\mathbf{C}_{n-1}$ .  $\square$

### 7. PROOF OF THEOREM 1.1: THE GENERAL CASE

Suppose that  $X \subseteq S_{n,k}$  has  $k$  elements and let  $S$  be the submonoid generated by  $X$ . Suppose first that  $X \subseteq T_{n,k}$ . Then since  $T_{n,k} \cup e_n$  has depth  $n$ , we see  $c(S) \leq c(T_{n,k} \cup e_n) \leq n$ . So we may assume that some element of  $X$  belongs to  $G_n$ . Arguing as in Section 4, there is a  $j \in \{1, \dots, k\}$  such that if  $S'$  is the monoid defined as per (4.1), then  $X$  is contained in the subsemigroup  $S'_{n,k}$  of  $S_{n,k}$  obtained from  $S'$  by performing the same construction used to create  $S_{n,k}$  from  $S_{1,k}$ . We show  $c(S'_{n,k}) = n$ . It will then follow that  $c(S) \leq c(S'_{n,k}) \leq n$ , completing the proof.

One has that  $S'_{n,k} = U_n \cup N_n \cup J'_n \cup 0$  where  $J'_n$  is a  $\mathcal{J}$ -class of  $S'_{n,k}$  obtained from  $J_n$  by removing certain  $\mathcal{R}$ -classes. Again, the  $\mathcal{J}$ -classes of  $S'_{n,k}$  form a chain of length  $n + 3$  with the top  $n$   $\mathcal{J}$ -classes in  $U_n$  and where  $N_n >_{\mathcal{J}} J'_n >_{\mathcal{J}} 0$ . Since, by Corollary 6.4,  $c(U_n) = n$ , we obtain  $c(S'_{n,k}) \geq n$ .

Let  $\tilde{J}$  be the minimal ideal of  $U_n$ . Then  $I = \tilde{J} \cup N_n \cup J'_n \cup 0$  is an ideal of  $S'_{n,k}$ . By the ideal theorem [29],

$$c(S'_{n,k}) \leq c(S'_{n,k}/I) + c(I). \tag{7.1}$$

Since  $S'_{n,k}/I$  has depth  $n - 1$ , the depth decomposition theorem [28] implies

$$c(S'_{n,k}/I) \leq n - 1. \tag{7.2}$$

Recall that we view  $U_1 = G_1$  as canonically embedded in  $\tilde{J}$  as a maximal subgroup with identity  $e_1$ . Since  $\tilde{J}$  is the unique maximal  $\mathcal{J}$ -class of  $I$  and contains a non-trivial group, by the reduction theorem [21, 28], we have  $c(I) = c(e_1 I e_1)$ . But  $e_1 I e_1$  is just the canonically embedded copy of  $S'$  in  $S'_{n,k}$  and we have shown in Section 4 that  $c(S') = 1$ , whence  $c(I) = 1$ . Putting this together with (7.1) and (7.2) shows that  $c(S'_{n,k}) \leq n$ , completing the proof of Theorem 1.1 and establishing its corollary, Theorem 1.2.



*Acknowledgements.* The second author would like to thank Jean-Eric Pin for some helpful comments, in particular for pointing out [13], Proposition 5.7, and the referees for some useful suggestions.

## REFERENCES

- [1] J. Almeida, *Finite Semigroups and Universal Algebra*. World Scientific, Singapore (1994).
- [2] J. Almeida, Hyperdecidable pseudovarieties and the calculation of semidirect products. *Internat. J. Algebra Comput.* **9** (1999) 241–261.
- [3] C.J. Ash, Inevitable graphs: A proof of the Type II conjecture and some related decision procedures. *Internat. J. Algebra Comput.* **1** (1991) 127–146.
- [4] B. Austin, K. Henckell, C. Nehaniv and J. Rhodes, Subsemigroups and complexity via the presentation lemma. *J. Pure Appl. Algebra* **101** (1995) 245–289.
- [5] S. Eilenberg, *Automata, Languages and Machines*. Academic Press, New York, Vol. A (1974); Vol. B (1976).
- [6] R.L. Graham, On finite 0-simple semigroups and graph theory. *Math. Syst. Theor.* **2** (1968) 325–339.
- [7] K. Henckell, Idempotent pointlikes. *Internat. J. Algebra Comput.* (To appear).
- [8] K. Henckell, Stable pairs. *Internat. J. Algebra Comput.* (Submitted).
- [9] K. Henckell, S. Margolis, J.-E. Pin and J. Rhodes, Ash’s type II Theorem, profinite topology and Mal’cev products: Part I. *Internat. J. Algebra Comput.* **1** (1991) 411–436.
- [10] K. Krohn and J. Rhodes, Algebraic theory of machines, I: Prime decomposition theorem for finite semigroups and machines. *Trans. Amer. Math. Soc.* **116** (1965) 450–464.
- [11] K. Krohn and J. Rhodes, Complexity of finite semigroups. *Ann. Math.* **88** (1968) 128–160.
- [12] K. Krohn, J. Rhodes and B. Tilson, Lectures on the algebraic theory of finite semigroups and finite-state machines Chapters 1, 5–9 (Chapter 6 with M.A. Arbib), in *The Algebraic Theory of Machines, Languages, and Semigroups*, edited by M.A. Arbib. Academic Press, New York (1968).
- [13] J.-E. Pin, *Varieties of Formal Languages*. Plenum, New York (1986).
- [14] J. Rhodes, The fundamental lemma of complexity for arbitrary finite semigroups. *Bull. Amer. Math. Soc.* **74** (1968) 1104–1109.
- [15] J. Rhodes, Kernel systems – A global study of homomorphisms on finite semigroups. *J. Algebra* **49** (1977) 1–45.
- [16] J. Rhodes, Infinite iteration of matrix semigroups. I. Structure theorem for torsion semigroups. *J. Algebra* **98** (1986) 422–451.
- [17] J. Rhodes, Infinite iteration of matrix semigroups. II. Structure theorem for arbitrary semigroups up to aperiodic morphism. *J. Algebra* **100** (1986) 25–137.
- [18] J. Rhodes and B. Steinberg, Complexity pseudovarieties are not local; type II subsemigroups can fall arbitrarily in complexity. *Internat. J. Algebra Comput.* (Submitted).
- [19] J. Rhodes and B. Tilson, Lower bounds for complexity of finite semigroups. *J. Pure Appl. Algebra* **1** (1971) 79–95.
- [20] J. Rhodes and B. Tilson, Improved lower bounds for the complexity of finite semigroups. *J. Pure Appl. Algebra* **2** (1972) 13–71.
- [21] J. Rhodes and B. Tilson, A reduction theorem for complexity of finite semigroups. *Semigroup Forum* **10** (1975) 96–114.
- [22] J. Rhodes and B. Tilson, Local complexity of finite semigroups, in *Algebra, Topology, and Category Theory (collection of papers in honor of Samuel Eilenberg)*. Academic Press, New York (1976) 149–168.

- [23] L. Ribes and P.A. Zalesskiĭ, On the profinite topology on a free group. *Bull. London Math. Soc.* **25** (1993) 37–43.
- [24] B. Steinberg, On an assertion of J. Rhodes and the finite basis and finite vertex rank problems for pseudovarieties. *J. Pure Appl. Algebra* **186** (2004) 91–107.
- [25] B. Steinberg, On aperiodic relational morphisms. *Semigroup Forum*. (Accepted).
- [26] B. Tilson, Decomposition and complexity of finite semigroups. *Semigroup Forum* **3** (1971) 189–250.
- [27] B. Tilson, Complexity of two- $\mathcal{J}$ -class semigroups. *Adv. Math.* **11** (1973) 215–237.
- [28] B. Tilson, Depth decomposition theorem. Chapter XI in [5].
- [29] B. Tilson, Complexity of semigroups and morphisms. Chapter XII in [5].
- [30] B. Tilson, Presentation lemma... the short form. (Unpublished 1995).
- [31] Y. Zalcstein, Group-complexity and reversals of finite semigroups. *Math. Syst. Theor.* **8** (1974/75) 235–242.