Pré-Publicações do Departamento de Matemática
Universidade de Coimbra
Preprint Number 09–28

PROFINITE GROUPS ASSOCIATED TO SOFIC SHIFTS ARE FREE

ALFREDO COSTA AND BENJAMIN STEINBERG

Abstract: We show that the maximal subgroup of the free profinite semigroup associated by Almeida to an irreducible sofic shift is a free profinite group, generalizing an earlier result of the second author for the case of the full shift (whose corresponding maximal subgroup is the maximal subgroup of the minimal ideal). A corresponding result is proved for certain relatively free profinite semigroups. We also establish some other analogies between the kernel of the free profinite semigroup and the $\mathscr{J}$-class associated to an irreducible sofic shift.

Keywords: Free profinite semigroups, free profinite groups, sofic shifts, symbolic dynamics.
AMS Subject Classification (2000): 20E18, 20M07.

1. Introduction

The study of maximal subgroups of free profinite semigroups has recently received quite a bit of attention in the literature [5, 6, 10, 14, 29, 33]. Almeida discovered how to associate to each irreducible symbolic dynamical system a maximal subgroup of a free profinite semigroup [2,4,6]. In [4,6] he announced that this subgroup is invariant under conjugacy of dynamical systems, but flaws were detected in the arguments sketched in [4]. The first author used a different approach to successfully prove the conjugacy invariance of the maximal group [14]. The resolution of the flaws in [4] led to the paper [8], making possible for its authors to produce a proof according to the original approach of Almeida; such a proof appears in [16].

In [5], Almeida studied the case of minimal systems associated to primitive substitutions and under certain hypotheses, the corresponding maximal subgroup was shown to be a free profinite group. An example of a non-free maximal subgroup, with rank two, associated to a primitive substitution was also obtained in [5]. It has since been proved by Almeida and the first author that the maximal subgroup associated to the Thue-Morse dynamical

Received August 06, 2009.
The authors acknowledge the support of the research programme AutoMathA of ESF. The first author was supported by FCT project PTDC/MAT/65481/2006 and FCT post-doctoral grant SFRH/BPD/46415/2008. The second author was supported in part by NSERC and the DFG.

system is not free profinite and has rank three [7]. In particular, a question of Margolis from 1997 as to whether all maximal subgroups of a free profinite semigroup are free was answered in the negative. Margolis also asked at this time whether all maximal subgroups were projective profinite groups and whether the maximal subgroup of the minimal ideal was a free profinite group. The first question was answered in the positive by Rhodes and the second author [29], whereas the second was answered positively by the second author [33].

The maximal subgroup of the minimal ideal is the maximal subgroup of the free profinite semigroup on X associated to the full shift $X^{\mathbb{Z}}$, which is an example of an irreducible sofic shift. It is then natural to ask whether the maximal subgroup associated to any irreducible sofic shift is free. A sofic shift is minimal if and only if it is periodic. In this case, Almeida and Volkov established early on that the corresponding maximal subgroup is free procyclic [10]. In this paper we show that the maximal subgroup associated to a non-minimal irreducible sofic shift is a free profinite group of countable rank, thereby generalizing the result for the minimal ideal [33]. An interesting feature of the proof is the crucial role played by the invariance of the subgroup under conjugacy of dynamical systems. A consequence of our results is that there is a dense set of idempotents whose corresponding maximal subgroups are free. Actually, we prove a stronger result that applies to certain relatively free profinite groups; the precise statement is left to the body of the article.

Several intermediate results established in the paper are likely to be of interest to researchers in symbolic dynamics and finite semigroup theory. For instance, we characterize the syntactic semigroups of irreducible sofic shifts as precisely the generalized group mapping semigroups [23,30] with aperiodic 0-minimal ideal. Fischer covers can then be interpreted as the corresponding Schützenberger graphs.

The paper is organized as follows. The first section consists of preliminaries about semigroups and languages. This is followed by a section on sofic shifts. The necessary background on sofic shifts and their relationship with free profinite semigroups is given, as well as several new results. The fourth section reviews the wreath product of partial transformation semigroups and establishes our notational conventions for iterated wreath products. The fifth section states our main result and proves it modulo a technical lemma. The following section proves the technical lemma, which is based on the argument of [33]. Other results from [10] about the minimal ideal of the free profinite semigroup are generalized to the minimal $\mathscr{J}$-class associated to arbitrary irreducible sofic subshifts. Namely, in the seventh section the existence of computable idempotents in such $\mathscr{J}$-classes is established; in the last section, using the notion of entropy, we obtain a characterization of this $\mathscr{J}$-class that is used to prove that, roughly speaking, we can not reach its elements starting with strict factors and using only iterations of certain endomorphisms and compositions of implicit operations with low arity.

2. Semigroups and languages

Throughout this paper we shall use basic notions from semigroup theory that can be found in standard texts [3, 13, 18, 20, 23, 30]. In particular, recall that Green's (equivalence) relation $\mathscr{J}$ is defined on a semigroup S by putting $s \mathrel{\mathscr{J}} t$ if s and t generate the same two-sided principal ideal. The $\mathscr{J}$-class of an element s is denoted J_s. We use the notation $s \leq_{\mathscr{J}} t$ to indicate that the two-sided ideal generated by s is contained in that generated by t. This is a preorder descending to an order $S/\mathscr{J}$. Sometimes we use $s \geq_{\mathscr{J}} J$ as shorthand for $J_s \geq_{\mathscr{J}} J$. Similarly defined are the $\mathscr{R}$- and $\mathscr{L}$-relations, where right (respectively, left) ideals replace two-sided ideals. Analogous notation is used for $\mathscr{L}$- and $\mathscr{R}$-classes. The intersection of $\mathscr{R}$ and $\mathscr{L}$ is denoted $\mathscr{H}$. The $\mathscr{H}$-class of an idempotent e of a semigroup S is a group, called the *maximal subgroup* at e. It can alte rnatively be defined as the group of units of the monoid eSe.

By a *compact semigroup* S, we mean a non-empty semigroup with a compact Hausdorff topology such that multiplication is jointly continuous. A *profinite semigroup* is a projective limit of finite semigroups, or equivalently a compact totally disconnected semigroup. Basic information about compact and profinite semigroups can be found in [30, Chapter 3]. A $\mathscr{J}$-class of a compact semigroup S is *regular* if it contains an idempotent, or equivalent all its elements are von Neumann regular. If S is a compact semigroup and $e, f \in S$ are $\mathscr{J}$-equivalent idempotents, then $G_e \cong G_f$ and so each regular $\mathscr{J}$-class has a unique maximal subgroup up to isomorphism of topological groups. Every compact semigroup has a unique minimal ideal, which is necessarily principal and hence closed. The minimal ideal is always a regular $\mathscr{J}$-class.

If X is a set, the free semigroup on X is denoted X^+; the corresponding free monoid is X^*; the respective profinite completions are denoted $\widehat{X^+}$ and $\widehat{X^*}$.

A subset $L \subseteq X^+$ is often called a *language*. A language is *rational* if it can be recognized by a finite state automaton. Equivalently, L is rational if there is a finite semigroup S and a homomorphism $\varphi\colon X^+ \to S$ so that $L = \varphi^{-1}\varphi(L)$. The category of onto morphisms recognizing $L \subseteq X^+$ has a terminal object $\lambda\colon X^+ \to S_L$ called the *syntactic morphism* of L. The semigroup S_L is called the *syntactic semigroup* of L and is the quotient of X^+ by the congruence that puts $x \equiv y$ if, for all $u, v \in X^*$, one has $uxv \in L \iff uyv \in L$. See [17] for details.

3. Sofic shifts

3.1. Definitions and notation. A good reference for the notions that we shall use here from symbolic dynamics is [25]. Let $X^{\mathbb{Z}}$ be the set of biinfinite sequences of letters of X indexed by $\mathbb{Z}$. The *shift* on $X^{\mathbb{Z}}$ is the bijective map σ_X (or just σ) from $X^{\mathbb{Z}}$ to $X^{\mathbb{Z}}$ defined by $\sigma_X((x_i)_{i\in\mathbb{Z}}) = (x_{i+1})_{i\in\mathbb{Z}}$. The *orbit* of $x \in X^{\mathbb{Z}}$ is the set $\{\sigma^k(x) \mid k \in \mathbb{Z}\}$. We endow $X^{\mathbb{Z}}$ with the product topology with respect to the discrete topology of X. A *symbolic dynamical system* is a non-empty closed subset $\mathscr{X}$ of some $X^{\mathbb{Z}}$ invariant under σ. Symbolic dynamical systems are also called *shift spaces* or *subshifts*.

Two subshifts $\mathscr{X} \subseteq X^{\mathbb{Z}}$ and $\mathscr{Y} \subseteq Y^{\mathbb{Z}}$ are *topologically conjugate* if there is a homeomorphism $\varphi\colon \mathscr{X} \to \mathscr{Y}$ commuting with shift: $\varphi \circ \sigma_X = \sigma_Y \circ \varphi$. Such a homeomorphism is also called a *topological conjugacy*. Since we will consider no other form of conjugacy, we drop the reference to its topological nature.

Let $x = (x_i)_{i\in\mathbb{Z}}$ be an element of $X^{\mathbb{Z}}$. We may represent it by

$$x = \ldots x_{-3}x_{-2}x_{-1}.x_0x_1x_2\ldots$$

where the central dot indicates that the 0 coordinate of x is the letter at its immediate right.

By a *factor of* $(x_i)_{i\in\mathbb{Z}}$ we mean a word $x_ix_{i+1}\cdots x_{i+n-1}x_{i+n}$ (briefly denoted by $x_{[i,i+n]}$), where $i \in \mathbb{Z}$ and $n \geq 0$. If $\mathscr{X}$ is a subset of $X^{\mathbb{Z}}$ then we denote by $L(\mathscr{X})$ the set of factors of elements of $\mathscr{X}$. A subset L of a semigroup S is said to be *factorial* if it is closed under taking factors, and it is *prolongable* if for every element u of L there are elements $a, b \in S$ such that $aub \in L$. It is easy to prove that the correspondence $\mathscr{X} \mapsto L(\mathscr{X})$ is an order isomorphism between the lattice of subshifts of $X^{\mathbb{Z}}$ and the lattice of non-empty, factorial, prolongable languages in X^+ [25, Proposition 1.3.4].

A subset L of a semigroup S is said to be *irreducible* if, for all $u, v \in L$, there exists $w \in S$ so that $uwv \in L$. Notice that, for factorial sets, irreducibility implies prolongability since if $u \in L$, then $uwuw'u \in L$ for some $w, w' \in S$ and hence $wuw' \in L$ since L is factorial. A shift $\mathscr{X}$ is said to be *irreducible* if $L(\mathscr{X})$ is an irreducible subset of X^+; this is equivalent to saying that $\mathscr{X}$ has a dense forward orbit [25]. One says that $\mathscr{X}$ is *minimal* if it contains no proper subshift. Minimal shifts are irreducible [25].

3.2. Sofic shifts. It is natural to consider those shifts whose associated language is rational.

Definition 3.1 (Sofic shift)**.** A shift $\mathscr{X}$ is *sofic* if $L(\mathscr{X})$ is rational.

A shift of *finite type* is a shift $\mathscr{X}$ such that $L(\mathscr{X}) = X^+ \setminus X^*FX^*$ for some finite set F. Therefore finite type shifts are sofic. Sofic shifts are exactly the quotients (or factors) of shifts of finite type.

Recall that a shift is called *periodic* if it is the (finite) orbit of a word of the form $x_u = \ldots uu.uuu \ldots$ with $u \in X^+$. The following is well known.

Lemma 3.2. *A sofic shift is minimal if and only if it is periodic.*

Proof: It is easy to see that every periodic shift is minimal. Suppose conversely that $\mathscr{X}$ is a minimal sofic shift. Since $L(\mathscr{X})$ is an infinite factorial rational language, by the Pumping Lemma we can find a non-empty word $u \in X^+$ so that $u^n \in L(\mathscr{X})$ for all $n \geq 0$. The orbit of $x_u = \ldots uuu.uuuu \ldots$ is then a subshift of $\mathscr{X}$, which is hence periodic by minimality. ∎

An example of an irreducible sofic shift is the *full shift* $X^{\mathbb{Z}}$.

3.3. Coding. Let N be a positive integer. Let Y_N be the alphabet X^N. We shall use the notation $[u]$ for a word $u \in X^N$ when we want to consider it as a letter of Y_N.

Let $N > 0$ and define $\beta_N \colon X^{\mathbb{Z}} \to Y_N^{\mathbb{Z}}$ by

$$\beta_N((x_i)_{i\in\mathbb{Z}}) = ([x_{[i,i+N-1]}])_{i\in\mathbb{Z}}.$$

For example,

$$\beta_3(\cdots x_{-3}x_{-2}x_{-1}.x_0x_1x_2\cdots) = \\ \cdots[x_{-2}x_{-1}x_0][x_{-1}x_0x_1].[x_0x_1x_2][x_1x_2x_3][x_2x_3x_4]\cdots$$

Given a subset $\mathscr{X}$ of $X^{\mathbb{Z}}$, denote by $\mathscr{X}^{[N]}$ the set $\beta_N(\mathscr{X})$. The following is [25, Example 1.5.10].

Lemma 3.3. *If $\mathscr{X}$ is a subshift of $X^{\mathbb{Z}}$, then $\mathscr{X}^{[N]}$ is a subshift of $(Y_N)^{\mathbb{Z}}$ and the map $\beta_N\colon \mathscr{X} \to \mathscr{X}^{[N]}$ is a conjugacy.*

Given a word u, denote by $\mathsf{alph}(u)$ the set of letters occurring in u. We extend this notation to shifts $\mathscr{X} \subseteq X^{\mathbb{Z}}$ by putting $\mathsf{alph}(\mathscr{X}) = X \cap L(\mathscr{X})$.

Lemma 3.4. *Let $\mathscr{X}$ be a sofic shift, which is not minimal. Then there is a conjugate shift $\mathscr{Y}$ of $\mathscr{X}$ for which there is a non-empty word $z \in L(\mathscr{Y})$ such that $z^+ \subseteq L(\mathscr{Y})$ and $\mathsf{alph}(z) \subsetneq \mathsf{alph}(\mathscr{Y})$.*

Proof: Suppose that $\mathscr{X} \subseteq X^{\mathbb{Z}}$ is a sofic shift, but not minimal. By the Pumping Lemma, there is a non-empty word w so that $w^+ \subseteq L(\mathscr{X})$. The orbit of $x_w = \dots www.wwww\dots$ is periodic and thus a minimal shift contained in $\mathscr{X}$. Since $\mathscr{X}$ is not minimal, the set $L(\mathscr{X}) \setminus L(x_w)$ contains some element v. Because $x_w = x_{w^m}$ for all $m > 0$, we may as well suppose that $|w| \geq |v|$. Using that $L(\mathscr{X})$ is prolongable, we may in fact assume $|w| = |v|$. The fact that $v \notin L(x_w)$ then translates into saying that v is not a cyclic conjugate of w. Set $N = |w| = |v|$.

Recall that $\mathscr{X}^{[N]}$ is conjugate to $\mathscr{X}$ by Lemma 3.3. Suppose that $w = a_1 \cdots a_N$ with the $a_i \in X$. Then setting

$$z = [a_1 \cdots a_N][a_2 \cdots a_N a_1] \cdots [a_N a_1 a_2 \cdots a_{N-1}]$$

we have $z^+ \subseteq L(\mathscr{X}^{[N]})$ (as $\beta_N(x_w) \in \mathscr{X}^{[N]}$). But since v is not a cyclic conjugate of w, we have $[v] \notin \mathsf{alph}(z)$. On the other hand, since v has length N and is a factor of some $x \in \mathscr{X}$, the letter $[v]$ is a factor of $\beta_N(x) \in \mathscr{X}^{[N]}$. Thus $[v] \in \mathsf{alph}(\mathscr{X}^{[N]})$. ∎

3.4. Regular $\mathscr{J}$-classes of compact semigroups. The goal of this subsection is to establish a bijection between regular $\mathscr{J}$-class of a compact semigroup S and non-empty, factorial, irreducible subsets (*FI-subsets*) of S which are closed topologically. This sets the stage for the connection with symbolic dynamics. We begin with a lemma on inverse images of such sets. We remark that a factorial set is a union of $\mathscr{J}$-classes. If S is a compact semigroup, S^1 denotes S with a functorially adjoined identity element 1, which is topologically an isolated point.

Lemma 3.5. *Let $\varphi\colon S \to T$ be a homomorphism of semigroups and suppose $\emptyset \neq L \subseteq T$. Then:*

(1) *If L is factorial, $\varphi^{-1}(L)$ is factorial;*

(2) *If φ is surjective and L is irreducible, then $\emptyset \neq \varphi^{-1}(L)$ is irreducible.*

Proof: For (1), if w is a factor of $\varphi^{-1}(L)$, evidentally $\varphi(w)$ is a factor of L and so $\varphi(w) \in L$, whence $w \in \varphi^{-1}(L)$. Thus $\varphi^{-1}(L)$ is factorial. On the other hand, suppose φ is onto and L is irreducible. Assume $u, v \in \varphi^{-1}(L)$ and choose $w \in T$ so that $\varphi(u)w\varphi(v) \in L$. Then if $\widetilde{w}$ is a preimage of w, one has $u\widetilde{w}v \in \varphi^{-1}(L)$. This completes the proof. ∎

The following proposition characterizes the closed FI-subsets of a compact semigroup. It combines the fundamental idea of Rhodes for lifting regular $\mathscr{J}$-classes [23, 30] and an idea of Almeida on irreducible shifts [6]. If A is a subset of a semigroup, we denote by $\mathrm{Fact}(A)$ the set of all factors of A.

Proposition 3.6. *Let S be a compact semigroup.*

1. *If A is a closed, non-empty, factorial, irreducible subset, then there is a unique minimal $\mathscr{J}$-class $J(A)$, called the* ***apex*** *of A, such that $J(A) \subseteq A$. Moreover, J is regular and $A = \mathrm{Fact}(J(A))$.*
2. *If J is a regular $\mathscr{J}$-class, then $\mathrm{Fact}(J)$ is a closed, non-empty, factorial, irreducible subset with apex J.*

Consequently, regular $\mathscr{J}$-classes of S are in bijection with closed FI-subsets.

Proof: To prove (1), first observe that A is a union of $\mathscr{J}$-classes. We next show that every element $s \in A$ is $\mathscr{J}$-above a minimal $\mathscr{J}$-class of A. Let $\mathscr{C}$ be the set of all closed ideals of S intersecting A, which are contained in the principal ideal generated by s. Then $\mathscr{C}$ is non-empty (as it contains the principal ideal generated by s) and by compactness the intersection of any descending chain of elements of $\mathscr{C}$ meets A in a non-empty subset, and hence belongs to $\mathscr{C}$. Thus $\mathscr{C}$ has a minimal element I by Zorn's Lemma. If $a \in A \cap I$, then the principal ideal generated by a intersects A and is contained in I. Thus I is a principal ideal by minimality and so A contains a minimal $\mathscr{J}$-class, which is $\mathscr{J}$-below s.

Suppose J_1, J_2 are minimal $\mathscr{J}$-classes of A (perhaps equal). Let $u \in J_1$ and $v \in J_2$. Then by irreducibility, there exists $w \in S$ so that $uwv \in A$. Clearly, $uwv \leq_{\mathscr{J}} J_1, J_2$. We conclude by minimality that $J_1 = J_2$ and $J_1^2 \cap J_1$ is non-empty. Thus J_1 is regular and unique. From now on we denote it $J(A)$. Clearly, $\mathrm{Fact}(J(A)) \subseteq A$. Conversely, if $a \in A$, then we know a is $\mathscr{J}$-above a minimal $\mathscr{J}$-class of A, which must be $J(A)$ by uniqueness. This establishes (1).

For (2), first note that if $\{x_\alpha\}$ is a net in $\mathrm{Fact}(J)$ converging to $x \in S$, then we can find, for each α, elements $u_\alpha, v_\alpha \in S^1$ so that $u_\alpha x_\alpha v_\alpha \in J$. By passing to a subnet, we may assume that $u_\alpha \to u$ and $v_\alpha \to v$ and hence $u_\alpha x_\alpha v_\alpha \to uxv$. Then since $\mathscr{J}$-classes of a compact semigroup are closed [30, Proposition 3.1.9] it follows that $uxv \in J$ and so $x \in \mathrm{Fact}(J)$. We conclude $\mathrm{Fact}(J)$ is closed. It is clearly factorial. Suppose $u, v \in \mathrm{Fact}(J)$. Then we can find $x, y, x', y' \in S^1$ so that $xuy, x'vy' \in J$. Since J is regular, we can find an element $w \in J$ so that $xuywx'vy' \in J$. Indeed, there is an $\mathscr{R}$-class R of J so that $L_{xuy} \cap R$ contains an idempotent and an $\mathscr{L}$-class L of J with $R_{x'vy'} \cap L$ containing an idempotent. We can then take w to be any element of the $\mathscr{H}$-class $R \cap L$. Hence $uywx'v \in \mathrm{Fact}(J)$ and $ywx' \in S$. Thus $\mathrm{Fact}(J)$ is irreducible. Evidentally, J is minimal in $\mathrm{Fact}(J)$ and hence is the apex of $\mathrm{Fact}(J)$. This completes the proof. ∎

As a corollary, we deduce a result on lifting regular $\mathscr{J}$-classes for compact semigroups [30, Lemma 3.1.14]. The analogue for finite semigroups is well known [23, 30]. If A is a subset of a semigroup S, then $E(A)$ denotes the idempotent elements of A.

Lemma 3.7. *Let $\varphi\colon S \to T$ be a continuous surjective homomorphism of compact semigroups and let J be a regular $\mathscr{J}$-class of T. Then:*

1. *There is a unique minimal $\mathscr{J}$-class J' of S so that $\varphi(J') \subseteq J$, which moreover is the apex of $\varphi^{-1}(\mathrm{Fact}(J))$;*
2. *The $\mathscr{J}$-class J' is regular and $\varphi(J') = J$;*
3. *Each $\mathscr{R}$-class, $\mathscr{L}$-class and $\mathscr{H}$-class of J' maps onto a corresponding class of J;*
4. *$\varphi(E(J')) = E(J)$.*

In particular, each maximal subgroup of J' maps homomorphically onto a maximal subgroup of J and each maximal subgroup of J is the image of a maximal subgroup of J'.

Proof: By Proposition 3.6, the set $\mathrm{Fact}(J)$ is a closed FI-subset. Hence, by Lemma 3.5, $\varphi^{-1}(\mathrm{Fact}(J))$ is a closed FI-subset and thus contains by Proposition 3.6 a unique minimal $\mathscr{J}$-class J', which moreover is regular, and $\varphi^{-1}(\mathrm{Fact}(J)) = \mathrm{Fact}(J')$. Suppose $x \in J$ where $x = \varphi(s)$ with $s \in \mathrm{Fact}(J')$. Then we can find $u, v \in S^1$ so that $usv \in J'$. Then $\varphi(usv) \in J$. Since φ is onto, we can find $a, b \in S^1$ so that $\varphi(ausvb) = x$. Hence $ausvb \in J'$ by minimality. We conclude $\varphi(J') \supseteq J$. But $\varphi(J')$ must be contained in a $\mathscr{J}$-class of T so $\varphi(J') = J$.

Suppose R is an $\mathscr{R}$-class of J' and that $t \mathrel{\mathscr{R}} \varphi(r)$ with $r \in R$. Then we can find $s \in S$ so that $\varphi(r)\varphi(s) = t$. Then $rs \leq_{\mathscr{J}} r$ and so $rs \in J'$ by minimality, whence $rs \mathrel{\mathscr{R}} r$ by stability of compact semigroups [30, Chapter 3]. Thus $t \in \varphi(R)$.

Next suppose G' is a maximal subgroup of J' with identity e. Let G be the $\mathscr{H}$-class of J containing the image of G'. If $g \in G$ and $s \in S$ is any preimage of g, then $\varphi(ese) = g$ and so, by minimality, $ese \in J'$. Stability shows in fact $ese \in G'$. Thus $\varphi(G') = G$. Now let H' be an $\mathscr{H}$-class $\mathscr{L}$-equivalent to G' and let H be the $\mathscr{H}$-class of J into which H' maps. Fix $h \in H'$; so $\varphi(h) \in H$. Green's Lemma implies that

$$H = \varphi(h)G = \varphi(h)\varphi(G') = \varphi(hG') = \varphi(H').$$

Because every $\mathscr{H}$-class in a regular $\mathscr{J}$-class is $\mathscr{L}$-equivalent to a maximal subgroup, this completes the proof of (3).

Finally, to prove (4) suppose that $e \in E(J)$ and let $A = \varphi^{-1}(e) \cap J' \neq \emptyset$. Since $\mathscr{J}$-classes in a compact semigroup are closed [30, Proposition 3.1.9], the set A is closed. But if $s, t \in A$, then $\varphi(st) = e$ and $st \leq_{\mathscr{J}} s$. Thus by minimality $st \in J'$ and so $st \in A$. Thus A is compact semigroup and hence contains an idempotent [30, Corollary 3.1.2]. ■

If $\mathbf{V}$ is a variety of finite semigroups, then $\widehat{F}_{\mathbf{V}}(X)$ denotes the free pro-$\mathbf{V}$ semigroup on X [3,30].

Lemma 3.8. *Let L be a subset of X^+. Let $\iota\colon X^+ \to \widehat{F}_{\mathbf{V}}(X)$ be the canonical morphism. If L is irreducible then the subset $\overline{\iota(L)}$ of $\widehat{F}_{\mathbf{V}}(X)$ is irreducible. Moreover, if L is factorial and $\mathbf{V}$ contains the syntactic semigroup of L, then $\overline{\iota(L)}$ is factorial.*

Proof: Suppose $u, v \in \overline{\iota(L)}$. Then $u = \lim \iota(u_n)$ and $v = \lim \iota(v_n)$ for some sequences $\{u_n\}$, $\{v_n\}$ of elements of L. For each n, there is $w_n \in X^+$ such that $u_n w_n v_n \in L$. It follows that $uwv \in \overline{\iota(L)}$ for some accumulation point w of $\{\iota(w_n)\}$. This completes the proof of irreducibility.

Suppose $\mathbf{V}$ contains the syntactic semigroup of L. Then $\overline{\iota(L)}$ is open and $\iota^{-1}\left(\overline{\iota(L)}\right) = L$ [3]. Let $u \in \overline{\iota(L)}$. Take a factorization $u = xwy$, where x and y are allowed to be 1. Then $x = \lim \iota(x_n)$, $w = \lim \iota(w_n)$, and $y = \lim \iota(y_n)$, for some sequences $\{x_n\}$, $\{w_n\}$, $\{y_n\}$ of elements of X^* (where $\iota(1) = 1$). Since $\overline{\iota(L)}$ is open, for all sufficiently large n, we have

$x_n w_n y_n \in \iota^{-1}\Bigl(\overline{\iota(L)}\Bigr) = L$. Since L is factorial, this implies that $w \in \overline{\iota(L)}$, thus $\overline{\iota(L)}$ is factorial. ■

If $\mathbf{V}$ contains the variety of finite nilpotent semigroups, then ι is an embedding of X^+ in $\widehat{F}_{\mathbf{V}}(X)$, and thus we consider ι to be an inclusion map. There are sofic shifts $\mathscr{X}$ such that $\overline{L(\mathscr{X})}$ is not factorial in $\widehat{F}_{\mathbf{LSl}}(X)$ [16, Proposition 3.3], where $\mathbf{LSl}$ is the variety of finite semigroups whose local submonoids are semilattices.

From Proposition 3.6 and the first part of Lemma 3.8 we immediately deduce the following result of Almeida announced in [6] and proved in [2].

Proposition 3.9. *Let $\mathscr{X} \subseteq X^{\mathbb{Z}}$ be an irreducible shift. Let $\mathbf{V}$ be a variety of finite semigroups such that $\overline{\iota(L(\mathscr{X}))}$ is factorial, where $\iota\colon X^+ \to \widehat{F}_{\mathbf{V}}(X)$ is the canonical morphism. Then there is a unique minimal $\mathscr{J}$-class, denoted $J(\mathscr{X})$, of $\widehat{F}_{\mathbf{V}}(X)$ intersecting $\overline{\iota(L(\mathscr{X}))}$. Moreover, $J(\mathscr{X})$ is regular and is $\mathscr{J}$-below each element of $\overline{\iota(L(\mathscr{X}))}$.*

It was proved in [8] that if $\mathbf{V}$ is a variety of finite semigroups such that $\mathbf{V} = \mathbf{A} ⓜ \mathbf{V}$ then $\overline{L}$ is a factorial subset of $\widehat{F}_{\mathbf{V}}(X)$ whenever L is a factorial subset of X^+. Hence, thanks also to Lemma 3.8, one can define the $\mathscr{J}$-class $J(\mathscr{X})$ in Proposition 3.9 whenever at least one of the following conditions holds:

(1) $\mathbf{V} = \mathbf{A} ⓜ \mathbf{V}$;
(2) $\mathbf{V}$ contains the syntactic semigroup of $L(\mathscr{X})$.

The maximal subgroup of $J(\mathscr{X})$ is called the *profinite group associated to the irreducible shift $\mathscr{X}$*; it is known to be a conjugacy invariant of $\mathscr{X}$ if $\mathbf{V} = \mathbf{V} * \mathbf{D}$, where $\mathbf{D}$ is the variety of finite semigroups whose idempotents are right zeroes, and $\mathbf{V}$ contains the two-element finite semilattice [14].

It is easy to see that if $\mathbf{H}$ is a variety of finite groups then the variety $\overline{\mathbf{H}}$ of finite semigroups whose subgroups are in $\mathbf{H}$ is an example of a variety of finite semigroups satisfying the equations $\mathbf{V} = \mathbf{A} ⓜ \mathbf{V}$ and $\mathbf{V} = \mathbf{V} * \mathbf{D}$ [18,30].

3.5. Sofic shifts and generalized group mapping semigroups. In this section we establish a connection between irreducible sofic shifts and generalized group mappings semigroups with aperiodic 0-minimal ideals, which we term AGGM-semigroups to be consistent with the notation of [30].

Definition 3.10 (AGGM-semigroup)**.** A finite semigroup S is called *generalized group mapping* if it acts faithfully on the left and right of its minimal ideal or it has a 0-minimal ideal on which it acts faithfully on both the left and right. The ideal in question, called the *distinguished ideal*, is unique and regular [30, Proposition 4.6.22]. If the ideal is aperiodic, then we call S an AGGM-*semigroup*.

Generalized group mapping semigroups were introduced by Krohn and Rhodes in their work on the complexity of finite semigroups; see [22, 23, 28, 30, 34].

Notice that an AGGM-semigroup is either trivial or contains a 0 and the distinguished ideal is 0-minimal. If S is an AGGM-semigroup, then by the *distinguished* $\mathscr{J}$*-class* of S, we mean the unique $\mathscr{J}$-class if S is trivial and otherwise we mean $I \setminus \{0\}$ where I is the distinguished ideal. It follows from [30, Proposition 4.6.37] that S is an AGGM-semigroup if and only if there is a regular $\mathscr{J}$-class J of S with the following property: for all $s, t \in S$, one has $s = t$ if and only if, for all $x, y \in J$,

$$xsy \in J \iff xty \in J.$$

Moreover, in this case J is the distinguished $\mathscr{J}$-class. From now on, if S is an X-generated profinite semigroup, then $[w]_S$ will denote the image of a word $w \in X^+$ in S.

Theorem 3.11. *Let S be a finite X-generated semigroup. Then S is the syntactic semigroup of $L(\mathscr{X})$ for an irreducible sofic shift $\mathscr{X} \subseteq X^{\mathbb{Z}}$ if and only if it is an* AGGM-*semigroup.*

Proof: Suppose first that $\mathscr{X}$ is a sofic shift and S is the syntactic semigroup of $L(\mathscr{X})$. If $\mathscr{X} = X^{\mathbb{Z}}$, then S is trivial and there is nothing to prove. So assume $\mathscr{X}$ is a proper shift. Then S has a 0 and $L(\mathscr{X})$ is the full inverse image of $S \setminus \{0\}$ since S is the syntactic semigroup of a coideal in X^+. Let J be a minimal non-zero $\mathscr{J}$-class of S. We first claim that J is regular. Indeed, if $[u]_S \in J$, then by irreducibility we can find $w \in X^+$ so that $uwu \in L(\mathscr{X})$. Then $0 \neq [uwu]_S \leq_{\mathscr{J}} [u]_S$ and so by minimality $[uwu]_S \in J$. Hence $[wu]_S \in J$ and so $J^2 \neq 0$. Thus J is regular. Now suppose that $[s]_S, [t]_S$ are such that, for all $x, y \in J$, one has $x[s]_S y \in J \iff x[t]_S y \in J$. Let $u, v \in X^+$ and assume that $usv \in L(\mathscr{X})$. Let $[z] \in J$. By irreducibility, we can find $w_1, w_2 \in X^+$ so that $zw_1usvw_2z \in L(\mathscr{X})$. Set $x = [zw_1u]_S$ and $y = [vw_2z]_S$. Then $x, y \in J$ and $x[s]_S y \in J$. Thus $x[t]_S y \in J$ and hence

$zw_1utvw_2z \in L(\mathscr{X})$. It follows $utv \in L(\mathscr{X})$. A symmetric argument shows that $utv \in L(\mathscr{X})$ implies $usv \in L(\mathscr{X})$. Thus $[s]_S = [t]_S$. This establishes that S is an AGGM-semigroup.

Conversely, assume S is an AGGM-semigroup. Let J be the distinguished $\mathscr{J}$-class of S and let $\pi\colon X^+ \to S$ be the canonical surjection. Then $\mathrm{Fact}(J) = S \setminus \{0\}$ is a non-empty, factorial, irreducible subset of S by Proposition 3.6. Thus $\pi^{-1}(S \setminus \{0\})$ is a non-empty, factorial, irreducible rational subset of X^+ (by Lemma 3.5) and hence of the form $L(\mathscr{X})$ for an irreducible sofic shift $\mathscr{X} \subseteq X^{\mathbb{Z}}$. It remains to show that S is the syntactic semigroup of $\pi^{-1}(S \setminus \{0\})$. To prove this, it suffices to verify that, given $m, n \in S$ such that $rms \neq 0 \iff rns \neq 0$ for all $r, s \in S^1$, one has $m = n$. By the remark before the theorem, it suffices to prove that, for all $x, y \in J$, we have $xmy \in J \iff xny \in J$. But $xmy \in J$ if and only if $xmy \neq 0$, if and only if $xny \neq 0$, if and only if $xny \in J$. This completes the proof of the theorem. ∎

Remark 3.12. The Fischer cover [11, 19] of an irreducible sofic shift $\mathscr{X}$ is nothing more than the Schützenberger graph associated to the faithful right action of the syntactic semigroup of $L(\mathscr{X})$ on an $\mathscr{R}$-class of its distinguished $\mathscr{J}$-class.

The $\mathscr{J}$-classes corresponding to irreducible sofic shifts admit the following topological characterization.

Proposition 3.13. *Let* $\mathbf{V}$ *be a variety of finite semigroups. Then a regular* $\mathscr{J}$*-class* J *of* $\widehat{F}_{\mathbf{V}}(X)$ *(for a finite set* X*) is of the form* $J(\mathscr{X})$ *for an irreducible sofic shift* $\mathscr{X}$ *with* $L(\mathscr{X})$ *a* $\mathbf{V}$*-recognizable set if and only if* $\mathrm{Fact}(J)$ *is clopen.*

Proof: Let $\iota\colon X^+ \to \widehat{F}_{\mathbf{V}}(X)$ denote the canonical morphism. Suppose first that $J = J(\mathscr{X})$ for an irreducible sofic shift $\mathscr{X}$ with $L(\mathscr{X})$ a $\mathbf{V}$-recognizable set. Let $\lambda\colon \widehat{F}_{\mathbf{V}}(X) \to S_{\mathscr{X}}$ be the continuous homomorphism induced by the syntactic morphism for $L(\mathscr{X})$. Then $\mathrm{Fact}(J) = \overline{\iota(L(\mathscr{X}))} = \lambda^{-1}(S_{\mathscr{X}} \setminus \{0\})$ and hence is clopen.

Conversely, suppose $\mathrm{Fact}(J)$ is clopen. Proposition 3.6 shows that $\mathrm{Fact}(J)$ is factorial and irreducible. Then $L = \iota^{-1}(\mathrm{Fact}(J))$ is a $\mathbf{V}$-recognizable language and $\overline{\iota(L)} = \mathrm{Fact}(J)$ [3]; in particular, $L \neq \emptyset$. Moreover, it is factorial by Lemma 3.5. It remains to prove that L is irreducible. It will then follow that $L = L(\mathscr{X})$ and $J = J(\mathscr{X})$ for an appropriate irreducible sofic shift $\mathscr{X}$. Suppose $u, v \in L$ and $\iota(u)w\iota(v) \in \mathrm{Fact}(J)$ with $w \in \widehat{F}_{\mathbf{V}}(X)$. Then $w = \lim \iota(w_n)$

for some sequence $\{w_n\} \subseteq X^+$. Then $\iota(uw_nv) \to \iota(u)w\iota(v) \in \mathrm{Fact}(J)$ and hence, as $\mathrm{Fact}(J)$ is open, for n large enough $uw_nv \in \iota^{-1}(\mathrm{Fact}(J)) = L$. This completes the proof of irreducibility. ■

An important lemma that we shall exploit frequently is the following.

Lemma 3.14. *Let $\mathscr{X} \subseteq X^{\mathbb{Z}}$ be an irreducible sofic shift whose syntactic semigroup is contained in a variety of finite semigroups $\mathbf{V}$ and suppose we have a commutative diagram of continuous surjective morphisms*

$$\begin{tikzcd} \widehat{F}_{\mathbf{V}}(X) \arrow[r, "\varphi"] \arrow[dr, "\lambda"'] & S \arrow[d, "\psi"] \\ & S_{\mathscr{X}} \end{tikzcd}$$

where $\lambda\colon \widehat{F}_{\mathbf{V}}(X) \to S_{\mathscr{X}}$ is the continuous extension of the syntactic morphism of $L(\mathscr{X})$. Then:

1. *$\varphi(J(\mathscr{X}))$ is a regular $\mathscr{J}$-class J of S;*
2. *J is the unique minimal $\mathscr{J}$-class of S with $\psi(J)$ contained in the distinguished $\mathscr{J}$-class of $S_{\mathscr{X}}$;*
3. *$J(\mathscr{X})$ is the unique minimal $\mathscr{J}$-class of $\widehat{F}_{\mathbf{V}}(X)$ mapping into J;*
4. *The image under φ of each maximal subgroup of $J(\mathscr{X})$ is a maximal subgroup of J.*

Proof: Let J_0 be the distinguished $\mathscr{J}$-class of $S_{\mathscr{X}}$ and suppose that J is the unique minimal $\mathscr{J}$-class of T with $\psi(J) \subseteq J_0$ guaranteed by Lemma 3.7. Then J is regular. To complete the proof, it suffices by Lemma 3.7 to verify that $J(\mathscr{X})$ is minimal among $\mathscr{J}$-classes of $\widehat{F}_{\mathbf{V}}(X)$ mapping under φ into J. Suppose that $u \leq_{\mathscr{J}} J(\mathscr{X})$ with $\varphi(u) \in J$. Then $\psi(\varphi(u)) \in J_0$ and hence $u \in \overline{L(\mathscr{X})}$. It follows that $u \in J(\mathscr{X})$ by definition of $J(\mathscr{X})$. ■

The following lemma is an immediate consequence of Lemma 3.4. The hypothesis $\mathbf{V} = \mathbf{V} * \mathbf{D}$ is there to guarantee that $J(\mathscr{Y})$ is well defined, since for two conjugate shifts $\mathscr{X}$ and $\mathscr{Y}$, the syntactic semigroup of $L(\mathscr{X})$ belongs to $\mathbf{V}$ if and only if the syntactic semigroup of $L(\mathscr{Y})$ does [15].

Lemma 3.15. *Let $\mathscr{X} \subseteq X^{\mathbb{Z}}$ be an irreducible sofic shift whose syntactic semigroup is contained in a variety of finite semigroups $\mathbf{V}$ with $\mathbf{V} = \mathbf{V} * \mathbf{D}$ and $\mathbf{V}$ containing all finite semilattices. There there is a conjugate irreducible sofic shift $L(\mathscr{Y})$ over an alphabet Y, an idempotent $e \in J(\mathscr{Y})$ and a word $z \in Y^+$ so that $e = z^\omega e$ and $\mathsf{alph}(z) \subsetneq \mathsf{alph}(\mathscr{Y})$.*

Proof: Let $\mathscr{Y}$ and z be as in Lemma 3.4. Then $z^\omega \in \overline{z^+} \subseteq \overline{L(\mathscr{Y})}$ and so by minimality of $J(\mathscr{Y})$, we can find $x, y \in \widehat{F}_{\mathbf{V}}(Y)^1$ so that $xz^\omega y \in J(\mathscr{Y})$. Since $J(\mathscr{Y})$ is regular, there are idempotents $f, f' \in J(\mathscr{Y})$ so that $fxz^\omega yf' = xz^\omega y$. Consequently, $z^\omega yf' \in J(\mathscr{Y})$. By regularity of $J(\mathscr{Y})$, we can then find an idempotent $e \in J(\mathscr{Y})$ with $e \mathrel{\mathscr{R}} z^\omega yf'$. Then $z^\omega e = e$ as required. ∎

The set of idempotents in a profinite semigroup is closed and hence a profinite space. It turns out that the idempotents in $\mathscr{J}$-classes corresponding to irreducible sofic shifts are dense in relatively free profinite semigroups.

Proposition 3.16. *Let $\mathbf{V}$ be a variety of finite semigroups and X a finite set. Let A be the set of idempotents of $\widehat{F}_{\mathbf{V}}(X)$ that belong to a $\mathscr{J}$-class of the form $J(\mathscr{X})$ for some irreducible sofic shift $\mathscr{X} \subseteq X^{\mathbb{Z}}$ with $L(\mathscr{X})$ a $\mathbf{V}$-recognizable set. Then A is dense in $E(\widehat{F}_{\mathbf{V}}(X))$,*

Proof: Let $e \in E(\widehat{F}_{\mathbf{V}}(X))$. Then a basic neighborhood of e is of the form $\pi^{-1}(\pi(e))$ where $\pi\colon \widehat{F}_{\mathbf{V}}(X) \to V$ is a continuous homomorphism to an element V of $\mathbf{V}$. Let J be the $\mathscr{J}$-class of $\pi(e)$ and choose a minimal $\mathscr{J}$-class J' of $\widehat{F}_{\mathbf{V}}(X)$ with $\pi(J') \subseteq J$ as per Lemma 3.7. In particular, J' is regular and $\mathrm{Fact}(J') = \pi^{-1}(\mathrm{Fact}(J))$, and hence is clopen. Proposition 3.13 then implies that $J' = J(\mathscr{X})$ for an irreducible sofic shift $\mathscr{X}$ with $L(\mathscr{X})$ a $\mathbf{V}$-recognizable set. By Lemma 3.7, there is an idempotent $f \in J' = J(\mathscr{X})$ with $\pi(f) = \pi(e)$. Thus $f \in A \cap \pi^{-1}(\pi(e))$, establishing that A is dense. ∎

4. The Schützenberger representation and wreath products

In this section we collect a number of standard facts concerning finite semigroups, which can be found, for instance, in [13, 23, 30].

The Schützenberger representation. Let J be a regular $\mathscr{J}$-class of a finite semigroup S. Fix an $\mathscr{R}$-class R of J. Then S acts on the right of R by partial functions by simply restricting the action of S on the right of itself. More precisely, for $s \in S$ and $x \in R$, define

$$x \cdot s = \begin{cases} xs & xs \in R \\ \text{undefined} & \text{else.} \end{cases}$$

The resulting faithful partial transformation semigroup does not depend on R up to isomorphism [30, Chapter 4, Section 6] and we denote it by

$(R, \mathsf{RM}_J(S))$. We use $\rho_J \colon S \to \mathsf{RM}_J(S)$ for the associated quotient map. The map ρ_J is called the (right) *Schützenberger representation* of S on J. If G is a maximal subgroup contained in R, then the restriction of the action of G to $G \subseteq R$ is the regular representation and hence faithful. Since $\mathsf{RM}_J(S)$ depends only on J and not R, it follows that ρ_J is injective on each maximal subgroup of J. The results of [30, Chapter 4, Section 6] imply that $\rho_J(J)$ is a regular $\mathscr{J}$-class of $\mathsf{RM}_J(S)$ and the Schützenberger representation of $\rho_J(S)$ on it is faithful.

Retaining the above notation, denote by $L(J)$ the set of $\mathscr{L}$-classes of S in J. There is an action of S by partial transformations on $L(J)$ given by

$$L_x s = \begin{cases} L_{xs} & xs \in J \\ \text{undefined} & \text{else.} \end{cases} \tag{4.1}$$

The resulting faithful right partial transformation semigroup is denoted by $(L(J), \mathsf{RLM}_J(S))$ and the quotient map by $\mu_J \colon S \to \mathsf{RLM}_J(S)$. See [30, Chapter 4, Section 6] for details.

Wreath products. Let us briefly recall the wreath product of partial transformation semigroups [18, 30]. In this paper, by a *partial transformation semigroup*, we mean a pair (B, S) where S is a semigroup acting faithfully by partial transformations on the *right* of B. If the maps in S are total, then we use the terminology *transformation semigroup.* In the case that S is a monoid (group) and the identity acts as the identity, then we say it is a *partial transformation monoid (group).* If B is a set, then $\overline{B}$ will denote the semigroup of all constant maps on B.

It will be convenient to use in this paper the formulation of wreath products in terms of row monomial matrices [30, Chapter 5] or [23]. If S is a semigroup, then S^0 is the semigroup obtained by functorially adjoining a multiplicative zero 0 (so a zero is added to S even if it already had one). Let S be a non-empty semigroup and B a set. Then $RM_B(S)$ consists of all $B \times B$-matrices row monomial matrices over S^0 equipped with usual matrix multiplication. Recall that a matrix is *row monomial* if each row contains at most one non-zero entry. The construction $RM_B(-)$ is functorial. Suppose that (B, T) is a partial transformation semigroup. The full partial transformation monoid is easily seen to be isomorphic to $RM_B(\{1\})$ [30, Chapter 5]. Thus we may view T as a subsemigroup of $RM_B(\{1\})$. Let $\pi \colon RM_B(S) \to RM_B(\{1\})$ be the projection. Then we define the *wreath product* $S \wr (B, T) = \pi^{-1}(T)$.

The projection $RM_B(S) \to RM_B(\{1\})$ restricts to a surjective morphism $S \wr (B,T) \to T$. Notice that $(-) \wr (B,T)$ is functorial and preserves surjective morphisms. If S is a group and (B,T) is a transformation group, then $S \wr (B,T)$ is a group.

Let J be a regular $\mathscr{J}$-class of a finite semigroup S with maximal subgroup G. Denote by J^0 the semigroup obtained by adding a multiplicative zero 0 to J and putting

$$x \cdot y = \begin{cases} xy & xy \in J \\ 0 & \text{else.} \end{cases}$$

for $x, y \in J$. Then J^0 is 0-simple and hence isomorphic to a Rees matrix semigroup $\mathscr{M}^0(G,A,B,C)$ where $C\colon B \times A \to G^0$ is the sandwich matrix [13, 23, 30]. Fix $a_0 \in A$ and $b_0 \in B$. Then without loss of generality we may assume that each non-zero entry of row b_0 and of column a_0 of C is the identity of G [23, 30]. We identify G with the maximal subgroup $a_0 \times G \times b_0$.

Recall that B can be identified with the set of $\mathscr{L}$-classes of J [30]. Notice that each element of J acts on B as a rank 1 partial map (cf. (4.1)), where the *rank* of a partial transformation is the size of its image. Moreover, J is transitive on B.

There is a well-known embedding $\mathsf{RM}_J(S) \hookrightarrow G \wr (B, \mathsf{RLM}_J(S))$ such that an element $s = (a,g,b) \in J$ is sent to the matrix $M(s)$ all of whose non-zero entries are in column b and with $M(s)_{b'b} = C_{b'a}g$ [30, Proposition 4.6.42]. In particular, if $s = (a_0, g, b_0)$ is an element of our maximal subgroup, then every non-zero entry of column b_0 of $M(s)$ is g and in particular $M(s)_{b_0b_0} = g$, establishing yet again that the Schützenberger representation is faithful on the maximal subgroup G.

The following well-known lemma elucidates the structure of wreath products. See, for instance, [12, Theorems 9.3.10 and 9.3.15].

Lemma 4.1. *Let $S = G \wr (B,T)$ where G is a non-trivial finite group and T is a finite transitive partial transformation semigroup consisting of maps of rank at most 1 and denote by $\pi\colon G\wr(B,T) \to T$ the wreath product projection. Then S is simple if T consists of total maps and otherwise S is 0-simple. The maximal subgroup of the non-zero $\mathscr{J}$-class of S is isomorphic to G. More precisely, if $e \neq 0$ is an idempotent such that the image of $\pi(e)$ is $\{b\}$, then $\psi\colon G_e \to G$ given by $\psi(s) = s_{bb}$ is an isomorphism.*

Proof: First we claim that T is simple if it consists of total maps and otherwise is 0-simple. If T consists of total maps, it is a right zero semigroup and hence trivially simple. Otherwise, suppose $0 \neq t \in T$ is not total and that b_0 is not in the domain of t. Let $\{b\}$ be the image of t. By transitivity, there is an element $t' \in T$ with $bt' = b_0$. Then $tt't = 0$ so $0 \in T$. To see that T is 0-simple, suppose that $t, t' \in T$ are non-zero. Let $b_t, b_{t'}$ be the unique elements in the image of t, t', respectively. Let b be an element of the domain of t'. By transitivity, we can find $u, v \in T$ with $b_t u = b$ and $b_{t'} v = b_t$. Then $tut'v = t$ and so $t \in Tt'T$. A symmetric argument shows that $t' \in TtT$. Thus T is 0-simple.

Next we verify that $\pi(x) = \pi(y)$ implies $x \mathrel{\mathscr{L}} y$. This will imply the simplicity or 0-simplicity of S (depending on which case we are in). Let $f \in T$ be an idempotent that is $\mathscr{R}$-equivalent to $\pi(x) = t = \pi(y)$ (T is regular). Then f has the same domain as t. Let $z \in S$ be given by putting $z_{i,if} = y_{i,it} x^{-1}_{if,it}$ if if (equivalently, it) is defined and 0 otherwise. Then one immediately verifies that $zx = y$. A symmetric argument establishes that $x \mathrel{\mathscr{L}} y$.

Now suppose that e is an idempotent of S such that $\pi(e)$ has image $\{b\}$. We must show ψ defined as above is an isomorphism. First note that every element s of S that is $\mathscr{L}$-equivalent to e satisfies $B\pi(s) = \{b\}$. Thus each element of G_e has all its non-zero entries in column b. It now follows that if $s, s' \in G_e$, then $(ss')_{bb} = s_{bb} s'_{bb}$, that is, ψ is a homomorphism. In particular, we have $1 = \psi(e) = e_{bb}$.

To see ψ is injective, note that $s \in G_e$ implies $s = es$. Since s, e have all their non-zero entries in column b, it follows that $s_{b'b} = e_{b'b} s_{bb}$ and so s is determined by $\psi(s) = s_{bb}$. Thus ψ is injective. Finally to verify ψ is onto, assume $g \in G$. Let s be the element of S obtained from e by changing e_{bb} to g and leaving all other entries the same. Then $\pi(ese) = \pi(e^3) = \pi(e)$ and so $ese \mathrel{\mathscr{L}} e$ by the above. Hence $ese \mathrel{\mathscr{H}} e$. Since $e_{bb} = 1$, clearly $(ese)_{bb} = e_{bb} s_{bb} e_{bb} = g$. Thus π is onto. ∎

If (A, S) and (B, T) are partial transformation semigroups, then one has that $(A \times B, S \wr (B, T))$ is a partial transformation semigroup, which we denote $(A, S) \wr (B, T)$. Here if $M \in S \wr (B, T)$, then $(a, b)M$ is defined if and only if $M_{bb'} \neq 0$ for some $b' \in B$ and $aM_{bb'}$ is defined. The result is then $(aM_{bb'}, b')$. The wreath product of partial transformation semigroups is known to be associative [18]. We can view an iterated wreath product $S \wr (A, T) \wr (B, U)$ as $|B| \times |B|$ block row monomial matrices where the blocks are $|A| \times |A|$ row monomial matrices over S. The term *block entry* shall refer to a non-zero matrix from $S \wr (A, T)$ while the term *entry* shall always mean an element of the semigroup S^0. In general matrices, and in particular block entries, shall be denoted by capital letters for the remainder of the paper.

5. Statement of the main result and a reduction

In this section, we state our main result and reduce its proof to a technical construction that will be presented in the next section. Recall that a subset Y of a profinite group G *converges to the identity* if each neighborhood of the identity contains all but finitely many elements of Y. A pro-$\mathbf{H}$ group F is *free pro-$\mathbf{H}$ on a subset Y converging to the identity* if given any map $\tau\colon Y \to H$ with H pro-$\mathbf{H}$ and $\tau(Y)$ converging to the identity, there is a unique continuous extension of τ to F. The cardinality of Y is called the *rank* of F. Any free pro-$\mathbf{H}$ group on a profinite space is free on a subset converging to the identity [31].

The following theorem was proved in [10, Theorem 7.5] for the case where $\overline{\mathbf{H}}$ consists of all finite semigroups. We provide here the proof of the general case. Recall that $C \subseteq X^+$ is called a *code* if C^+ is a free semigroup on C. A code is said to have *synchronization delay* at most d, if for all $(c, c') \in C^d \times C^d$ and all $x, y \in X^*$, one has $xcc'y \in C^+$ if and only if $xc, c'y \in C^+$.

Lemma 5.1. *Let $u \in X^+$ be a primitive word. Then, for any $m > 0$ and any $x, y \in X^*$, one has $xu^my \in u^+$ if and only if $x, y \in u^*$.*

Proof: Suppose $xu^my \in u^+$. Then we may write $x = u^kx'$ and $y = y'u^\ell$ so that $|x'|, |y'| < u$. If we can show that $x' = 1 = y'$, we are done. Suppose at least one of x' and y' are non-trivial. Then since $x'u^my' \in u^+$, by length considerations we must have $x'u^my' = u^{m+1}$ and $|x'| + |y'| = |u|$. But then x' is a prefix of u and y' is a suffix of u and so $x'y' = u$ by length considerations. But then $x'u^my' = x'y'u^{m-1}x'y'$ and so $u^m = y'u^{m-1}x'$. Thus y' is a prefix and x' is a suffix of u. Length considerations then yield $y'x' = u = x'y'$. But then x', y' are powers of a word w and hence u is a proper power, contradicting primitivity. Thus $x' = 1 = y'$, as was required. ■

Theorem 5.2. *Suppose that X is a finite set and let $\mathscr{X} \subseteq X^{\mathbb{Z}}$ be a periodic shift. Let $\mathbf{H}$ be a non-trivial variety of finite groups. Then the maximal subgroup $G(\mathscr{X})$ of $J(\mathscr{X}) \subseteq \widehat{F}_{\overline{\mathbf{H}}}(X)$ is a free pro-$\mathbf{H}$ group of rank 1.*

Proof: Let u be a primitive word such that $\mathscr{X}$ is the orbit of $\ldots uuu.uuu\ldots$. We claim that the maximal subgroup K of $J(\mathscr{X})$ containing u^ω is generated by $u^{\omega+1}$. This fact is a special case of [10, Theorem 7.5], but it can proved in an easier way. An elementary result of Restivo [27] shows that if $C \subseteq X^+$ is a code such that C^+ is pure, i.e., closed under extraction of roots, then the syntactic semigroup of C^+ is aperiodic (see also [24, Chapter 7, Exercise 8]). Clearly u^+ is closed under extraction of roots (by primitivity of u) and so its syntactic monoid S is aperiodic and hence belongs to $\overline{\mathbf{H}}$. If $\eta\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to S$ is the canonical extension of the syntactic morphism, then $\eta(K) = \eta(u^\omega) = \eta(u^+)$, where the first equality holds by aperiodicity, whereas the second is immediate from Lemma 5.1. We conclude $K \subseteq \eta^{-1}\eta(u^+) = \overline{u^+}$. Since $\overline{\langle u^{\omega+1}\rangle}$ is the unique maximal subgroup of $\overline{u^+}$, this establishes the claim.

Since K is procyclic, it is free pro-$\mathbf{H}$ if and only if every cyclic group from $\mathbf{H}$ is an image of it. Let n be an integer such that $\mathbf{H}$ contains a cyclic group of order n. Since (u,u) is the unique pair in $\{u\} \times \{u\}$, Lemma 5.1 with $m = 2$ immediately yields that the code $\{u\}$ has synchronizing delay at most 1. Therefore, if T is the syntactic semigroup of $\{u^n\}^+$, then each maximal subgroup of T is in the variety of finite groups generated by $\mathbb{Z}_n$, by [24, Chapter 7, Corollary 2.14] and hence $T \in \overline{\mathbf{H}}$ (this can also be deduced from S being aperiodic and the result of Weil on subgroups of the syntactic semigroup of a composed code [35]). Clearly, a necessary condition for $[u^{n+r}]_T = [u^{n+k}]_T$ is that $r \equiv k \bmod n$. Consequently, $\langle [u]_T^{\omega+1}\rangle$ must in fact be a cyclic group of order n. Putting together what we have just shown, we see that $K = \overline{\langle u^{\omega+1}\rangle}$ maps onto the cyclic group of order n whenever it belongs to $\mathbf{H}$. We conclude that K is a free pro-$\mathbf{H}$ group of rank 1. ∎

A fact that we shall use in the following theorem is that if $\mathbf{V}$ is a variety of finite semigroups containing all finite semilattices such that $\mathbf{V} = \mathbf{V} * \mathbf{D}$ and $\mathscr{X}, \mathscr{Y}$ are conjugate sofic shifts, then the syntactic semigroup of $L(\mathscr{X})$ belongs to $\mathbf{V}$ if and only if the syntactic semigroup of $L(\mathscr{Y})$ does [15].

Theorem 5.3. *Suppose that X is a finite set and let $\mathscr{X} \subseteq X^{\mathbb{Z}}$ be an irreducible sofic shift. Suppose that $\mathbf{H}$ is a variety of finite groups closed under extension such that the syntactic semigroup of $L(\mathscr{X})$ belongs to $\overline{\mathbf{H}}$ and $\mathbb{Z}/p\mathbb{Z} \in \mathbf{H}$ for infinitely many primes p. Then the maximal subgroup $G(\mathscr{X})$ of $J(\mathscr{X}) \subseteq \widehat{F}_{\overline{\mathbf{H}}}(X)$ is a free pro-$\mathbf{H}$ group. If $\mathscr{X}$ is minimal, then $G(\mathscr{X})$ is procyclic; otherwise it is free pro-$\mathbf{H}$ of countable rank.*

Proof: By Theorem 5.2, we may suppose that $\mathscr{X}$ is not minimal. Because $\overline{\mathbf{H}} = \overline{\mathbf{H}}*\mathbf{D}$, the isomorphism class of the maximal subgroup of $J(\mathscr{X})$ depends on $\mathscr{X}$ only up to conjugacy by [14].

Lemma 3.15 and the observation made in the paragraph before the theorem, allow us to assume that there exist an idempotent $e \in J(\mathscr{X})$ and a word $z \in X^+$ so that $e = z^\omega e$ and $\mathsf{alph}(z) \subsetneq \mathsf{alph}(\mathscr{X})$. By possibly shrinking or enlarging the alphabet, we may assume without loss of generality that $X = \{x_1, \ldots, x_{n+1}\}$ where $\mathsf{alph}(\mathscr{X}) = \{x_1, \ldots, x_n\}$ and that we have an idempotent $e \in J(\mathscr{X})$ and a word $z \in \{x_1, \ldots, x_{n-1}\}^+$ so that $z^\omega e = e$ and $x_1 \in \mathsf{alph}(z)$. Doing this lets us avoid treating the full shift as a special case. Instead, we may assume that the syntactic semigroup $S_{\mathscr{X}}$ of $L(\mathscr{X})$ has a zero element 0. Let G_e be the maximal subgroup at e. Our goal is to show that G_e is free pro-$\mathbf{H}$ on a countable set of generators converging to the identity (that is, free of countable rank).

It is well known $\widehat{F}_{\overline{\mathbf{H}}}(X)$ is metrizable [3, 30], and hence so is G_e. Thus the identity e of G_e has a countable basis of neighborhoods. We shall use a well-known criterion, going back to Iwasawa [21], to establish that G_e is free pro-$\mathbf{H}$ of countable rank. An *embedding problem* for G_e is a diagram

$$\begin{tikzcd} & G_e \arrow[d, "\varphi"] \\ H \arrow[r, two heads, "\alpha"] & K \end{tikzcd} \tag{5.1}$$

with $H \in \mathbf{H}$ and φ, α epimorphisms (φ continuous).

A *solution* to the embedding problem (5.1) is a continuous **epimorphism** $\widetilde{\varphi}\colon G_e \to H$ making the diagram

$$\begin{tikzcd} & G_e \arrow[d, "\varphi"] \arrow[dl, dashed, "\widetilde{\varphi}"'] \\ H \arrow[r, two heads, "\alpha"] & K \end{tikzcd}$$

commute. (The terminology "embedding problem" comes from Galois theory.) According to [31, Corollary 3.5.10] to prove G_e is free pro-$\mathbf{H}$ of countable rank it suffices to show that every embedding problem (5.1) for G_e has a solution. We proceed via a series of reductions on the types of embedding problems we need to consider. The initial reductions are nearly identical to those in [29, 33].

So let us suppose that we have an embedding problem for G_e as per (5.1). The reader is referred to [30, Chapter 3, Section 1] for basic properties of profinite semigroups and projective limits; see also [31] for the analogous results in the context of profinite groups. Let $\lambda\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to S_{\mathscr{X}}$ be the continuous extension of the syntactic morphism of $L(\mathscr{X})$; note that $\lambda(x_{n+1}) = 0$. Let $\{S_i\}_{i\in D}$ be the inverse quotient system of all finite continuous images of $\widehat{F}_{\overline{\mathbf{H}}}(X)$ such that λ factors through the projection $\pi_i\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to S_i$. Then $\widehat{F}_{\overline{\mathbf{H}}}(X) = \varprojlim_{i\in D} S_i$. Since G_e is a closed subgroup of $\widehat{F}_{\overline{\mathbf{H}}}(X)$, it follows from basic properties of profinite spaces that $G_e = \varprojlim_{i\in D} \pi_i(G_e)$ (see [31, Corollary 1.1.8]). Since φ is an onto continuous map to a finite group it follows that φ factors through $\pi_i|_{G_i}$ for some $i \in D$ (i.e. $\ker \pi_i|_{G_e} \subseteq \ker\varphi$) [31, Lemma 1.1.16]. Setting $S' = S_i$ and $\varphi' = \pi_i$, we conclude there exists a continuous onto homomorphism $\varphi'\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow S'$ with S' a finite semigroup in $\overline{\mathbf{H}}$ such that $\ker\varphi'|_{G_e} \subseteq \ker\varphi$ and $\ker\varphi' \subseteq \ker\lambda$.

Set $K' = \varphi'(G_e)$ and let $\rho\colon K' \twoheadrightarrow K$ be the canonical projection. Defining H' to be the pullback of α and ρ, that is,

$$H' = \{(h,k') \in H \times K' \mid \alpha(h) = \rho(k')\},$$

yields a commutative diagram

$$\begin{tikzcd} & & G_e \arrow[dl, bend right, "\varphi'"'] \arrow[ddl, bend left, "\varphi"] \\ H' \arrow[r, two heads, "\alpha'"] \arrow[d, "\rho^*"'] & K' \arrow[d, "\rho"] & \\ H \arrow[r, two heads, "\alpha"] & K & \end{tikzcd}$$

where ρ^* is the projection to H and α' is the projection to K'. It is easily verified that all the arrows in the diagram are epimorphisms. So to solve our original embedding problem, it suffices to solve the embedding problem

$$\begin{tikzcd} & G_e \arrow[d, "\varphi'"] \\ H' \arrow[r, two heads, "\alpha'"] & K' \end{tikzcd} \tag{5.2}$$

as the composition of a solution to (5.2) with ρ^* yields a solution to (5.1). In other words, reverting back to our original notation, we may assume in the embedding problem (5.1) that the map φ is the restriction of a continuous onto homomorphism $\varphi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow S$ with $S \in \overline{\mathbf{H}}$ and $\ker\varphi \subseteq \ker\lambda$.

By Lemma 3.14, $J = \varphi(J(\mathscr{X}))$ is a regular $\mathscr{J}$-class of S and the group $K = \varphi(G_e)$ is a maximal subgroup of J. By Section 4, the right Schützenberger representation $\rho_J\colon S \to \mathsf{RM}_J(S)$ of S on J is faithful when restricted to K. Moreover, if $\psi\colon S \to S_{\mathscr{X}}$ is the canonical projection, then $\ker\rho_J \subseteq \ker\psi$ by Lemma 3.14, [30, Proposition 4.6.37] and [30, Equation (4.8)] since $S_{\mathscr{X}}$ is an AGGM-semigroup with distinguished $\mathscr{J}$-class J_0 and J is minimal with $\psi(J) \subseteq J_0$. Possibly replacing S by its image under the Schützenberger representation, we may then assume that the right Schützenberger representation of S on J is faithful (recall that from the results of [30, Chapter 4, Section 6] $\rho_J(J)$ is a regular $\mathscr{J}$-class of $\mathsf{RM}_J(S)$ and the Schützenberger representation of $\rho_J(S)$ on it is faithful). Therefore, we may view S as embedded in the wreath product $K \wr (B, \mathsf{RLM}_J(S))$. Moreover, J is then the unique minimal non-zero $\mathscr{J}$-class of S [30, Proposition 4.6.29]. Consequently, Lemma 3.14 implies the following lemma.

Lemma 5.4. *Let $u \in \widehat{F}_{\overline{\mathbf{H}}}(X)$. Then $u \in \overline{L(\mathscr{X})}$ if and only if $\varphi(u) \neq 0$. In particular, $\varphi(x_{n+1}) = 0$.*

The existence of a solution to (5.1) is then a consequence of the following technical lemma whose proof we defer to Section 6.

Lemma 5.5. *Let $\varphi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow S$ be a continuous surjective morphism with S finite and $\ker\varphi \subseteq \ker\lambda$ such that $\varphi(G_e) = K$ and the Schützenberger representation of S on the $\mathscr{J}$-class $J = \varphi(J(\mathscr{X}))$ is faithful. In particular, J is regular and is the unique minimal non-zero $\mathscr{J}$-class of S. Suppose that $\alpha\colon H \twoheadrightarrow K$ is an epimorphism of finite groups. Then there is an X-generated finite semigroup $S' \in \overline{\mathbf{H}}$ such that if $\eta\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to S'$ is the continuous projection, then:*

1. *there is an isomorphism $\theta\colon G_{\eta(e)} \to H$ where $G_{\eta(e)}$ is the maximal subgroup of S' at $\eta(e)$;*
2. *φ factors through η as $\rho\eta$ where $\rho\colon S' \twoheadrightarrow S$ satisfies $\rho\theta^{-1} = \alpha$.*

Assuming the lemma, our desired solution to the embedding problem (5.1) is $\widetilde{\varphi} = \theta\eta|_{G_e}\colon G_e \to H$. Indeed, $\eta|_{G_e}\colon G_e \to G_{\eta(e)}$ is an epimorphism by Lemma 3.14 (as $\ker\eta \subseteq \ker\varphi \subseteq \ker\lambda$) and hence $\widetilde{\varphi}$ is an epimorphism. Moreover, $\alpha\widetilde{\varphi} = \rho\theta^{-1}\theta\eta|_{G_e} = \varphi|_{G_e}$ and so $\widetilde{\varphi}$ is indeed a solution to the embedding problem (5.1). This completes the proof of Theorem 5.3. ∎

Since the full shift is an irreducible sofic shift, an immediate corollary is the main result of [33] (although the proof of that result is simply a specialization of the current proof).

Corollary 5.6. *Let* $\mathbf{H}$ *be a variety of finite groups closed under extension, which contains* $\mathbb{Z}/p\mathbb{Z}$ *for infinitely may primes* p*. Then the maximal subgroup of the minimal ideal of a finitely generated (but not procyclic) free pro-*$\overline{\mathbf{H}}$ *semigroup is a free pro-*$\mathbf{H}$ *group of countable rank.*

It follows from our main result and Proposition 3.16 that there is a dense set of idempotents in $\widehat{F}_{\overline{\mathbf{H}}}(X)$ whose corresponding maximal subgroups are free pro-$\mathbf{H}$.

6. The proof of Lemma 5.5

We retain the notation of the previous section. In particular, recall that $X = \{x_1, \ldots, x_{n+1}\}$, there is a word $z \in \{x_1, \ldots, x_{n-1}\}^+$ so that $z^\omega e = e$, $x_1 \in \mathsf{alph}(z)$, e is an idempotent of $J(\mathscr{X})$ and $\mathsf{alph}(\mathscr{X}) = \{x_1, \ldots, x_n\}$. Assume that $z = z_1 \cdots z_q$ with $z_i \in \{x_1, \ldots, x_{n-1}\}$ for $i = 1, \ldots, q$.

Proof of Lemma 5.5: Let B be the set of $\mathscr{L}$-classes of J. Since we are assuming the Schützenberger representation of S on J is faithful, we can view S as a subsemigroup of $K \wr (B, \mathsf{RLM}_J(S))$, that is, as a semigroup of $b \times b$ row monomial matrices over K where $b = |B|$. Denote by 1 the $\mathscr{L}$-class of $\varphi(e)$. We order the elements of B with 1 first when we write our matrices. The discussion in Section 4 shows that the embedding can be chosen so that the row monomial matrix associated to an element k of the maximal subgroup K at $\varphi(e)$ has k in every non-zero entry of the first column and 0 in the remaining columns. Moreover, the $1,1$-entry of the row monomial matrix associated to k is k. For $x \in \widehat{F}_{\overline{\mathbf{H}}}(X)$, denote by M_x the row monomial matrix associated to $\varphi(x)$. We shall distinguish formally between M_x and $\varphi(x)$, although $M_x = M_y$ if and only if $\varphi(x) = \varphi(y)$.

Let $N = \ker \alpha$ and choose a set-theoretic section $\sigma\colon K \to H$. Then $H = N\sigma(K)$. For $x \in \widehat{F}_{\overline{\mathbf{H}}}(X)$, denote by M_x^σ the $b \times b$ row monomial matrix over H obtained from M_x by applying σ entry-wise. Let m be a positive integer such that $(M_{z_1}^\sigma \cdots M_{z_q}^\sigma)^m$ is idempotent in $H \wr (B, \mathsf{RLM}_J(S))$. Choose a prime $p > \max\{m, |N|^b, |z|_{x_1}\}$ so that $\mathbb{Z}/p\mathbb{Z} \in \mathbf{H}$; such a prime exists by our assumption on $\mathbf{H}$. Denote by C_p the cyclic group of order p generated by the permutation $(1\,2 \cdots p)$. Our semigroup S' will be a certain subsemigroup of the iterated wreath product

$$Q = H \wr (B, \mathsf{RLM}_J(S)) \wr \overline{([p], C_p)}$$

where $[p] = \{1, \ldots, p\}$. Observe that $Q \in \overline{\mathbf{H}}$ since $\mathbf{H}$ closed under extension implies that $\overline{\mathbf{H}}$ is closed under wreath product [18,30]. The reader is referred to [1] for more on taking a wreath product of a semigroup with a group with constant maps.

We begin our construction of S' by defining

$$\widetilde{x}_1 = \begin{bmatrix} 0 & M^{\sigma}_{x_1} & 0 & \cdots & 0 \\ 0 & 0 & M^{\sigma}_{x_1} & 0 & \vdots \\ \vdots & 0 & 0 & \ddots & 0 \\ 0 & \vdots & 0 & 0 & M^{\sigma}_{x_1} \\ M^{\sigma}_{x_1} & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

In other words $\widetilde{x}_1$ acts on the $[p]$-component by the cyclic permutation $(1\ 2\ \cdots p)$ and each block entry of $\widetilde{x}_1$ from $H \wr (B, \mathsf{RLM}_J(S))$ is $M^{\sigma}_{x_1}$. For $2 \leq i \leq n-1$, we set

$$\widetilde{x}_i = \begin{bmatrix} M^{\sigma}_{x_i} & 0 & \cdots & 0 \\ 0 & M^{\sigma}_{x_i} & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & M^{\sigma}_{x_i} \end{bmatrix}.$$

So $\widetilde{x}_i$ acts on the $[p]$-component as the identity map and each block entry of $\widetilde{x}_i$ from $H \wr (B, \mathsf{RLM}_J(S))$ is $M^{\sigma}_{x_i}$, for $i = 2, \ldots, n-1$.

To define $\widetilde{x}_n$ will require some extra notation. Set $\ell = |N|^b$; so $p > \ell$ by choice of p. Let $1 = N_1, N_2 \ldots, N_\ell$ be the distinct elements of N^b. We identify N^b with the group of diagonal $b \times b$ matrices over N. In particular, N^b is a subgroup of $H \wr (B, \mathsf{RLM}_J(S) \cup \{1_B\})$. In fact, there is a natural onto homomorphism

$$\overline{\alpha}\colon H \wr (B, \mathsf{RLM}_J(S)) \to K \wr (B, \mathsf{RLM}_J(S))$$

induced by $\alpha\colon H \to K$; the map $\overline{\alpha}$ simply applies α entry-wise. Moreover, it is straightforward to verify that $\overline{\alpha}(U) = \overline{\alpha}(V)$ if and only if $U = N_j V$ some $1 \leq j \leq \ell$. Indeed, if we denote by u_i (respectively v_i) the non-zero entry (if there is one) of row i of U (respectively V), then $\overline{\alpha}(U) = \overline{\alpha}(V)$ implies $\alpha(u_i) = \alpha(v_i)$ for all i and so we can find $n_i \in N$ such that $u_i = n_i v_i$ for all i

(where if i is a zero row of u and v, then we may choose n_i arbitrarily). We may then take $N_j = \mathrm{diag}(n_1, n_2, \ldots, n_b)$. Dually, $U = VN_k$, some k.

Next let us define a $p \times p$ block row monomial matrix

$$\widetilde{x}_n = \begin{bmatrix} M^\sigma_{x_n} & 0 & \cdots & 0 \\ N_2 M^\sigma_{x_n} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ N_\ell M^\sigma_{x_n} & 0 & \cdots & 0 \\ M^\sigma_{x_n} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ M^\sigma_{x_n} & 0 & \cdots & 0 \end{bmatrix};$$

so $\widetilde{x}_n$ has all its block entries in the first column. The j^{th} block entry of the first column is $N_j M^\sigma_{x_n}$ if $j \leq \ell$ and otherwise is $M^\sigma_{x_n}$. Finally, let $\widetilde{x}_{n+1} = 0$. Then $\widetilde{x}_1, \ldots, \widetilde{x}_{n+1} \in Q$ and we have a map $X \to Q$ given by $x_i \mapsto \widetilde{x}_i$. Extend this to a continuous morphism $\eta\colon \widehat{F_{\overline{\mathbf{H}}}}(X) \to Q$ and set $S' = \eta(\widehat{F_{\overline{\mathbf{H}}}}(X))$. Our goal is to show S' is the desired semigroup. We begin by verifying that φ factors through η.

Proposition 6.1. *Let $u \in \widehat{F_{\overline{\mathbf{H}}}}(X)$. Then $\eta(u) = 0$ if and only if $\varphi(u) = 0$. Moreover, if $\eta(u) \neq 0$, then $\eta(u)$ is a block $p \times p$-matrix in which each block row contains a (non-zero) block entry $U \in H \wr (B, \mathsf{RLM}_J(S))$, and for every such block entry one has $\overline{\alpha}(U) = M_u$. As a consequence, $\eta(u) = \eta(u')$ implies $\varphi(u) = \varphi(u')$ and so φ factors through η as $\rho\eta$ where $\rho\colon S' \to S$ takes $\eta(u)$ to $\overline{\alpha}(U)$ where U is any block entry of $\eta(u)$.*

Proof: The final statement follows from the previous ones since $\eta(u) = \eta(u')$ then implies $M_u = M_{u'}$ and so $\varphi(u) = \varphi(u')$.

We next prove the remaining part of the statement for words $u \in X^+$ by induction on length, the case $|u| = 1$ being trivial. The result is also trivial for words containing x_{n+1}, so we only deal with words not containing this element. Suppose that $w = x_i u$ with $1 \leq i \leq n$ and $u \in X^+$. By induction $\varphi(u) = 0$ if and only if $\eta(u) = 0$ and so it only remains to deal with the case $\varphi(u) \neq 0$ and $\eta(u) \neq 0$. We recall that since the wreath product consists of row monomial matrices, each block row of an element of Q can have at most one block entry.

Let $1 \leq j \leq p$. By induction, $\eta(u)$ has a unique (non-zero) block entry U_j in the j^{th}-block row. The definition of $\widetilde{x}_i$ implies that the j^{th}-block row of $\eta(w)$ is obtained by multiplying each entry of a certain block row $\xi(j)$ of

$\eta(u)$ on the right by $N_{k_j}M^{\sigma}_{x_i}$ for some $N_{k_j} \in N^b$ (perhaps the identity). So the only candidate to be a block entry of block row j of $\eta(w)$ is $N_{k_j}M^{\sigma}_{x_i}U_{\xi(j)}$. We claim that either $N_{k_j}M^{\sigma}_{x_i}U_{\xi(j)}$ is a (non-zero) block entry in the j^{th}-row of $\eta(w)$ for all $1 \leq j \leq p$, or $\eta(w) = 0 = \varphi(w)$.

By induction, $\overline{\alpha}(U_{\xi(j)}) = \varphi(u)$, thus we have

$$\overline{\alpha}(N_{k_j}M^{\sigma}_{x_i}U_{\xi(j)}) = M_{x_i}\overline{\alpha}(U_{\xi(j)}) = \varphi(x_i)\varphi(u) = \varphi(w) = M_w \tag{6.1}$$

for $j = 1, \dots, p$. Now the diagram

$$\begin{tikzcd} H \wr (B, \mathsf{RLM}_J(S)) \arrow[rr, "\overline{\alpha}"] \arrow[dr] & & K \wr (B, \mathsf{RLM}_J(S)) \arrow[dl] \\ & \mathsf{RLM}_J(S) & \end{tikzcd}$$

commutes, where the bottommost arrows are the wreath product projections. Since an element of a wreath product $L \wr (A, Z)$ is zero if and only if its image under the wreath product projection is zero, it follows from (6.1) that $N_{k_j}M^{\sigma}_{x_i}U_{\xi(j)} = 0$ for some $1 \leq j \leq p$ if and only if $N_{k_j}M^{\sigma}_{x_i}U_{\xi(j)} = 0$ for all $1 \leq j \leq p$, if and only if $\varphi(w) = 0$. Therefore, $\eta(w) = 0$ if and only if $\varphi(w) = 0$, and if neither is 0 then (6.1) implies that, as a block $p \times p$-matrix, each block row of $\eta(w)$ has exactly one (non-zero) block entry, and each block entry is an $\overline{\alpha}$-preimage of M_w.

If $u \in \widehat{F}_{\overline{\mathbf{H}}}(X)$, then since X^+ is dense in $\widehat{F}_{\overline{\mathbf{H}}}(X)$ and $\eta^{-1}\eta(u), \varphi^{-1}\varphi(u)$ are open, there exists a word $w \in X^+$ such that $\eta(u) = \eta(w)$ and $\varphi(u) = \varphi(w)$. The result now follows from the case of words. ■

It now follows that $\ker \eta \subseteq \ker \lambda$ and so Lemma 3.14 yields $J' = \eta(J(\mathscr{X}))$ is an entire regular $\mathscr{J}$-class of S'. Lemma 5.4 established $\varphi(u) = 0$ if and only if $u \notin \overline{L(\mathscr{X})}$. Thus by Proposition 6.1 we conclude $\eta(u) = 0$ if and only if $u \notin \overline{L(\mathscr{X})}$ and hence J' is the unique minimal non-zero $\mathscr{J}$-class of S'. Notice that $\rho(J') = \rho(\eta(J(\mathscr{X}))) = \varphi(J(\mathscr{X})) = J$. In particular, J' is minimal with $\rho(J') \subseteq J$ and so Lemma 3.7 applies.

Our next goal is to show that if $u \in L(\mathscr{X})$ is a word with $x_n \in \mathsf{alph}(u)$, then every preimage of M_u under $\overline{\alpha}$ is a block entry of $\eta(u)$. This will be crucial in showing that the maximal subgroup of $\eta(J)$ is isomorphic to H. To effect this we shall need the following lemma. Notice that if U is any preimage of M_u, then the complete set of preimages of M_u is $\{N_1U, \dots, N_\ell U\} = \{UN_1, \dots, UN_\ell\}$ (note that if M_u has any zero rows, then these elements are not distinct).

Lemma 6.2. *Let $u, w \in \widehat{F}_{\overline{\mathbf{H}}}(X)$ and suppose U is a fixed preimage of M_u under $\overline{\alpha}$. Then every preimage of M_{uw} (respectively, M_{wu}) under $\overline{\alpha}$ is of the form UW (respectively, WU) for some preimage W of M_w under $\overline{\alpha}$.*

Proof: Let M be a preimage of M_{uw} under $\overline{\alpha}$. Since UM_w^σ is a preimage of M_{uw} under $\overline{\alpha}$, it follows that $M = UM_w^\sigma N_i$ for some $1 \le i \le \ell$. But then $W = M_w^\sigma N_i$ is an $\overline{\alpha}$-preimage of M_w and $M = UW$. The statement for M_{wu} is proved dually. ∎

Observe that if $w \in X^+$ and $x_n \in \mathsf{alph}(w)$, then by definition of $\widetilde{x}_1, \dots, \widetilde{x}_n$, the block entries of $\eta(w)$ form a single column, in other words, the $\overline{([p], C_p)}$-component of $\eta(w)$ is a constant map. We can now prove the aforementioned fact concerning preimages.

Proposition 6.3. *Let $w \in L(\mathscr{X})$ with $x_n \in \mathsf{alph}(w)$. Then the set of preimages of M_w under $\overline{\alpha}$ is the set of block entries of $\eta(w)$.*

Proof: Let R be the set of words $w \in L(\mathscr{X})$ with $x_n \in \mathsf{alph}(w)$. We proceed by induction on $|w|$ for $w \in R$. If $|w| = 1$, then the proposition follows from the definition of $\widetilde{x}_n$.

Suppose it is true for words in R of length n and let $w \in R$ have length $n+1$. Let W be a $\overline{\alpha}$-preimage of M_w. If the first letter of w is x_n, then $w = vx_i$ with $v \in R$, some i; else $w = x_i v$ where $v \in R$ and $1 \le i \le n-1$. In the latter case, by Lemma 6.2 we have $W = M_{x_i}^\sigma V$ for some $\overline{\alpha}$-preimage V of M_v. By induction hypothesis, V is a block entry of $\eta(v)$. Then, since $\eta(w) = \eta(x_i)\eta(v)$, it follows from the definition of $\eta(x_i)$ that $M_{x_i}^\sigma V$ is a block entry of $\eta(w)$.

In the case $w = vx_i$ for some $v \in R$ and some i, the block entries of $\eta(v)$ are in a single column, say column j. Let U be the block entry in row j of $\widetilde{x}_i$; by construction it is an $\overline{\alpha}$-preimage of M_{x_i}. By Lemma 6.2 we have $W = VU$ for some $\overline{\alpha}$-preimage V of M_v. By induction hypothesis, V is a block entry of $\eta(v)$, and so it is in column j of $\eta(v)$. Hence VU is a block entry of $\eta(w)$. ∎

A continuity argument allows us to extend the above result beyond words.

Corollary 6.4. *If $w \in J(\mathscr{X})$, then the block entries of $\eta(w)$ are in a single column and the set of preimages under $\overline{\alpha}$ of M_w is the set of block entries of $\eta(w)$.*

Proof: Consider the continuous homomorphism $c\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to (P(X), \cup)$ defined by setting $c(x) = \{x\}$ for $x \in X$. Recall that we are assuming that

$\{x_1, \ldots, x_n\} = \mathsf{alph}(\mathscr{X})$. Since $L(\mathscr{X})$ is irreducible, we can find words $v_1, \ldots, v_{n-1}$ so that $x_1 v_1 x_2 \cdots x_{n-1} v_{n-1} x_n \in L(\mathscr{X})$. It follows that $\mathsf{alph}(\mathscr{X}) \in c(L(\mathscr{X})) = c(\overline{L(\mathscr{X})})$ (the latter by continuity). By minimality of $J(\mathscr{X})$, we conclude that $c(J(\mathscr{X})) = \{\mathsf{alph}(\mathscr{X})\}$. Thus if $\{w_r\}$ is a sequence of words in X^+ converging to w, then there exists $R > 0$ such that, for $r \geq R$, we have $\mathsf{alph}(w_r) = c(w_r) = \mathsf{alph}(\mathscr{X})$. The semigroup S' is finite so there exists $s \geq R$ with $\eta(w) = \eta(w_s)$ by continuity of η. Remembering that $\varphi = \rho\eta$, this implies that $\varphi(w) = \varphi(w_s)$, or equivalently that $M_w = M_{w_s}$. As $\mathsf{alph}(w_s) = \mathsf{alph}(\mathscr{X}) = \{x_1, \ldots, x_n\}$, the corollary now follows from Proposition 6.3 and the remark preceding that proposition applied to w_s. ∎

Recalling that $\mu_J \colon S \to \mathsf{RLM}_J(S)$ denotes the canonical projection, observe that $T = \mu_J(J \cup \{0\})$ is a transitive semigroup of partial transformations of B of rank at most 1 containing the empty map. By Corollary 6.4 if $w \in J(\mathscr{X})$, then the $\overline{([p], C_p)}$-component of $\eta(w)$ is a constant map, that is, the block entries of $\eta(w)$ appear in a single column. Moreover, Proposition 6.1 shows that each block entry of $\eta(w)$ is a preimage of M_w under $\overline{\alpha}$. Hence, $J' \subseteq H \wr (B, T) \wr ([p], \overline{[p]})$. Moreover, $(B, T) \wr ([p], \overline{[p]})$ is easily verified to be a transitive semigroup of partial transformations of rank at most 1. Indeed, each entry of an element of $(B, T) \wr ([p], \overline{[p]})$ has all of its block entries in a single column and each non-zero element of T is a rank 1 partial transformation. The transitivity is immediate from the transitivity of T and $\overline{[p]}$ since if $(b, i), (b', j) \in B \times [p]$ and $bt = b'$ with $t \in T$, then $(b, i)D = (b', j)$ where the block entries of D are all in column j and each block entry of D is t. Lemma 4.1 now implies that $H \wr (B, T) \wr ([p], \overline{[p]})$ is 0-simple.

It remains to construct an isomorphism $\theta \colon G_{\eta(e)} \to H$ such that $\rho\theta^{-1} = \alpha$. Corollary 6.4 yields that all the block entries of $\eta(e)$ belong to a single column. By cyclically permuting the names of the elements of $[p]$, we may assume without loss of generality that $\eta(e)$ is a block matrix with each block entry in the first column. Also, the discussion in Section 4 indicates M_e is a matrix whose only non-zero column is the first column and whose non-zero entries are comprised of the identity of K; moreover, the $1,1$-entry of M_e is the identity of K. Since the block entries of $\eta(e)$ are preimages of M_e under $\overline{\alpha}$ (Proposition 6.1), we deduce that all the non-zero entries of $\eta(e)$ are in the first column and belong to N. Lemma 4.1 says that the map $\Theta \colon H \wr (B, T) \wr ([p], \overline{[p]}) \to H$ selecting the $1,1$-entry of a matrix is an isomorphism from the maximal subgroup at $\eta(e)$ of $H \wr (B, T) \wr ([p], \overline{[p]})$ to H.

In particular, $\eta(e)_{11}$ is the identity of H. We shall show that the restriction θ of Θ to $G_{\eta(e)}$ is onto and $\rho\theta^{-1} = \alpha$. This will require a little preparation.

Proposition 6.5. *If $u \in G_e$, the $\varphi(u) = \alpha(\eta(u)_{11})$.*

Proof: Corollary 6.4 implies that all the block entries of $\eta(u)$ are in a single column. In fact, they are all in the first column since we just saw that this is the case for $\eta(e)$ and $\eta(u) = \eta(u)\eta(e)$. Proposition 6.1 implies that M_u is the matrix obtained by choosing any block entry of $\eta(u)$ and applying $\overline{\alpha}$. In particular, M_u is the result of applying α entry-wise to the $1,1$-block entry of $\eta(u)$ and so $[M_u]_{11} = \alpha(\eta(u)_{11})$.

Now if $k \in K$, then according to first paragraph of the proof of Lemma 5.5 the row monomial matrix associated to k has $1,1$-entry k. In particular, since $\varphi(u) \in K$, it follows that $[M_u]_{11} = \varphi(u)$. The last statement of the previous paragraph then yields $\varphi(u) = \alpha(\eta(u)_{11})$, as required. ∎

The proposition admits the following corollary.

Corollary 6.6. *The equality $\alpha\theta = \rho|_{G_{\eta(e)}}$ holds.*

Proof: Recalling that θ selects the $1,1$-entry of an element of $G_{\eta(e)}$, Proposition 6.5 shows that $\varphi = \alpha\theta\eta$ as maps from G_e to K. By definition of ρ there is a factorization $\varphi = \rho\eta$ and hence, in fact, $\rho\eta = \alpha\theta\eta \colon G_e \to K$. But $\eta(G_e) = G_{\eta(e)}$ by Lemma 3.14, so we conclude that $\rho|_{G_{\eta(e)}} = \alpha\theta$ as was to be proved. ∎

Since θ is injective, being a restriction of the isomorphism Θ, Corollary 6.6 immediately yields that if θ is onto, then $\alpha = \rho\theta^{-1}$. Thus we are left with proving θ is onto. Since J' is the minimal $\mathscr{J}$-class with $\rho(J') \subseteq J$ (as was already observed) ρ must take $G_{\eta(e)}$ onto K by Lemma 3.7. It follows from Corollary 6.6 that α maps $\theta(G_{\eta(e)})$ onto K. Recalling $\ker\alpha = N$, we conclude $H = N\theta(G_{\eta(e)})$ and so to complete the proof it suffices to establish that N is contained in the image of θ.

Recall that we have a word $z = z_1 \cdots z_q$ such that $z_i \in \{x_1, \ldots, x_{n-1}\}^+$, for $i = 1, \ldots, q$, the letter x_1 is a factor of z and $z^\omega e = e$. Set $Z = M^\sigma_{z_1} \cdots M^\sigma_{z_q} \in H \wr (B, \mathsf{RLM}_J(S))$. Let us remind the reader that our prime p was chosen so that $p > m$ where $Z^m = Z^\omega$ and $p > |z|_{x_1}$. Thus, we can find a positive integer r so that $1 \equiv rm|z|_{x_1} \bmod p$. Direct computation shows that

$$\eta(z)^{rm} = \begin{bmatrix} 0 & Z^\omega & 0 & \cdots & 0 \\ 0 & 0 & Z^\omega & 0 & \cdots \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & Z^\omega \\ Z^\omega & 0 & \cdots & 0 & 0 \end{bmatrix}$$

since every block entry of $\eta(z)$ is Z and $\eta(z)$ acts in the $[p]$-component by the permutation $(1\ 2\ \cdots p)^{|z|_{x_1}}$. Set $C = \eta(z)^{rm}$. Then C^j has the block form of the permutation matrix corresponding to $(1\ 2\ \cdots p)^j$ and each block entry of C^j is Z^ω. In particular, the effect of multiplying a matrix D on the left by C^j is to permute the rows of D according to the permutation $(1\ 2\ \cdots p)^{-j}$ and to multiply each row of D on the left by Z^ω.

Notice that $\eta(e) = \eta(z)^\omega \eta(e)$ as $z^\omega e = e$. But $\eta(z)^\omega$ is a $p \times p$-block diagonal matrix with Z^ω as each diagonal block. Thus the set of elements of the form $Z^\omega U$ with U a block entry of $\eta(e)$ is precisely the set of block entries of $\eta(e)$, which is precisely the set of preimages of M_e under $\overline{\alpha}$ by Corollary 6.4. Each preimage of M_e is therefore the $1,1$-block entry of a product $C^j\eta(e)$ for a correctly chosen j as $(1\ 2\ \cdots p)$ acts transitively on $\{1, \ldots, p\}$ and all the block entries of $\eta(e)$ are in the first column.

Now M_e is a matrix all of whose non-zero entries are the identity of K and belong to the first column; moreover, the $1,1$-entry of M_e is the identity of K. It follows that the $\overline{\alpha}$-preimages of M_e are precisely those matrices with first column having entries from $N = \ker \alpha$ in those rows that are non-zero in M_e and whose remaining columns consist of zeroes. Consequently, any element of N can be the $1,1$-entry of an $\overline{\alpha}$-preimage of M_e and so every element $h \in N$ is $[C^j\eta(e)]_{11}$ for some j (as an entry, not a block entry). Since $\eta(e)_{11}$ is the identity of H, it follows $\eta(e)C^j\eta(e)$ has $1,1$-entry h, and in particular is a non-zero element of S'. Thus $\eta(e)C^j\eta(e)$ is an element of $G_{\eta(e)}$ by minimality of J' among non-zero $\mathscr{J}$-classes of S'. By construction, $\theta(\eta(e)C^j\eta(e)) = h$ and so $\theta(G_{\eta(e)})$ contains N as required. This completes the proof of Lemma 5.5, thereby establishing Theorem 5.3. ■

7. Computing idempotents in the $\mathscr{J}$-class of a sofic shift

Let X be a finite alphabet. An element w of $\widehat{X^+}$ is said to be *(polynomial time) computable* if there is an algorithm which on input an X-tuple $(s_x)_{x \in X}$ of elements from a finite semigroup S, computes (in time polynomial in $|S|$)

the value $\varphi(w)$ where $\varphi\colon \widehat{X^+} \to S$ is the canonical extension of the map $x \mapsto s_x$. The existence of a computable idempotent in the minimal ideal of $\widehat{X^+}$ was proved independently by Reilly and Zhang [26] on the one hand, and by Almeida and Volkov [9] on the other. The Reilly-Zhang idempotent was shown to be polynomial time computable in [9].

Let $\mathscr{X}$ be an irreducible sofic shift over an alphabet X. Our goal is to construct a computable idempotent in $J(\mathscr{X})$. In fact, we give an algorithm which is uniform in the sofic shift, given as input via a so-called irreducible presentation. First we need a lemma.

Lemma 7.1. *Let $\mathscr{X} \subseteq X^{\mathbb{Z}}$ be an irreducible sofic shift whose syntactic semigroup is in a variety $\mathbf{V}$ of finite semigroups. Let $\iota\colon X^+ \to \widehat{F}_{\mathbf{V}}(X)$ be the canonical morphism. Then $u \in \overline{\iota(L(\mathscr{X}))}$ belongs to $J(\mathscr{X})$ if and only if each element of $\iota(L(\mathscr{X}))$ is a factor of u.*

Proof: Clearly each element of $\iota(L(\mathscr{X}))$ is a factor of each element of $J(\mathscr{X})$ by minimality of $J(\mathscr{X})$. Suppose conversely, that each element of $\iota(L(\mathscr{X}))$ is a factor of $u \in \overline{\iota(L(\mathscr{X}))}$. Let $v \in J(\mathscr{X})$ and write $v = \lim \iota(v_n)$ with the v_n in X^+. Since $\overline{\iota(L(\mathscr{X}))}$ is clopen, it follows that, for all n sufficiently large, $\iota(v_n) \in \overline{\iota(L(\mathscr{X}))} \cap \iota(X^+) = \iota(L(\mathscr{X}))$ (since $L(\mathscr{X})$ is $\mathbf{V}$-recognizable [3]). Hence we may assume that $v_n \in L(\mathscr{X})$ for all n. By hypothesis on u, we can find, for each n, elements $r_n, s_n \in \widehat{F}_{\mathbf{V}}(X)$ so that $r_n\iota(v_n)s_n = u$. Passing to a subsequence, we may assume that $r_n \to r, s_n \to s$ for some $r, s \in \widehat{F}_{\mathbf{V}}(X)$. Then $u = rvs$ and so $u \in J(\mathscr{X})$ by minimality of $J(\mathscr{X})$. ■

The following can be found in [25, Chapter 3]. For an irreducible sofic shift $\mathscr{X}$ there is a strongly connected graph Γ with non-empty set E of edges, and a map $\pi\colon E \to X$ such that, if P is the set of paths in Γ then, denoting the unique extension of π to a homomorphism $E^+ \to X^+$ also by π, we have $\pi(P) = L(\mathscr{X})$. We say that (Γ, π) is an *irreducible presentation* of $\mathscr{X}$. In other words, an irreducible presentation is a strongly connected non-deterministic automaton, all of whose states are initial and final, recognizing $L(\mathscr{X})$.

We shall reduce our problem to producing a computable idempotent in the kernel of a clopen subsemigroup of $\widehat{X^+}$.

Lemma 7.2. *Let (Γ, π) be an irreducible presentation of a sofic shift $\mathscr{X} \subseteq X^{\mathbb{Z}}$ and let v be a vertex of Γ. Let $T \subseteq X^+$ be the rational subsemigroup of* *all words in* X^+ *reading a loop at* v. *Then each element of the minimal ideal of* $\overline{T} \subseteq \widehat{X^+}$ *belongs to* $J(\mathscr{X})$.

Proof: By construction, $T \subseteq L(\mathscr{X})$ and hence $\overline{T} \subseteq \overline{L(\mathscr{X})}$. Suppose t belongs to the minimal ideal of $\overline{T}$. Then each element of T is a factor of t. But since Γ is strongly connected, each word labeling a path in Γ is a factor of an element of T. Thus $t \in J(\mathscr{X})$ by Lemma 7.1. ∎

In light of Lemma 7.2, to achieve our goal, it suffices to construct a computable idempotent ρ_T in the minimal ideal of $\overline{T}$ for each rational subsemigroup $T \subseteq X^+$. Moreover, our algorithm will be uniform in T (meaning, given an automaton for T and an X-tuple of a finite semigroup S, we can compute the value of ρ_T on this X-tuple).

Lemma 7.3. *Let* $L \subseteq X^+$ *be a rational subset and* $\varphi\colon X^+ \to S$ *a homomorphism. Then each element in* $\varphi(L)$ *can be represented by a word in* L *of length at most* $m(|S|+1)-1$ *where* m *is the number of states of the minimal automaton for* L.

Proof: Let $\mathscr{A} = (Q, X, \delta, q_0, F)$ be the minimal automaton for L and construct an automaton $\mathscr{B} = (Q \times S^1, X, \Delta, (q_0, 1), F \times S)$ where $(q, s)x = (qx, s\varphi(x))$ describes the transition function. Then $s \in \varphi(L)$ if and only if there is a word $w \in X^+$ reading in $\mathscr{B}$ from $(q_0, 1)$ to a state of the form (q, s) with $q \in F$. Since $\mathscr{B}$ has $m(|S|+1)$ states, such a word can always be chosen to have length at most $m(|S|+1)-1$. ∎

We can now construct our idempotent using the 'Zimin word' idea of Reilly and Zhang (see also [9]). We assume that the alphabet X is totally ordered. The *shortlex* order is defined on X^+ by putting $u < v$ if $|u| < |v|$ or $|u| = |v|$ and u lexicographically precedes v.

Theorem 7.4. *Let* $T \subseteq X^+$ *be a rational subsemigroup. Let* $v_1, v_2, \ldots$ *be the elements of* T *in shortlex order and put* $w_1 = v_1$ *and* $w_{n+1} = (w_n v_{n+1} w_n)^{(n+1)!}$ *for* $n \geq 1$. *Then the sequence* $\{w_n\}$ *converges to a computable idempotent* ρ_T *of the minimal ideal of* $\overline{T} \subseteq \widehat{X^+}$.

Proof: First of all, since T has decidable membership and there is a Turing machine that enumerates X^+ in shortlex order, clearly there is a Turing machine that can compute the element w_n of the sequence given n as input. Let $\varphi\colon X^+ \to S$ be a morphism where S is a finite semigroup of order k. Let m be the number of states of the minimal automaton of T. Put $r =$

$m(k+1)-1$ and $N = |X|+|X|^2+\cdots+|X|^r$. We claim that $\varphi(w_N) = \varphi(w_n)$ for all $n \geq N$ and that $\varphi(w_N)$ is an idempotent of the minimal ideal of $\varphi(T)$. It will then follow that $\{w_n\}$ converges to a computable idempotent in the minimal ideal of $\overline{T}$.

First observe that for $n \geq k$, the elements $\varphi(w_n)$ form a descending chain of idempotents. Now, by choice of N, for $n \geq N$, every word in T of length at most r is a factor of w_n. Lemma 7.3 then yields that every element of $\varphi(T)$ is a factor of $\varphi(w_n)$; consequently, $\varphi(w_n)$ is an element of the minimal ideal I of $\varphi(T)$. But I is a completely simple semigroup and so contains no strictly descending chains of idempotents. Thus $\varphi(w_n) = \varphi(w_N)$ for all $n \geq N$. This completes the proof. ■

The proof shows the construction is uniform in T. Applying Lemma 7.2, we obtain:

Corollary 7.5. *If $\mathscr{X} \subseteq X^{\mathbb{Z}}$ is an irreducible sofic shift, then there is a computable idempotent in $J(\mathscr{X})$.*

We leave it as an open question whether the polynomial time algorithm in [9] to compute the Reilly-Zhang idempotent (which is our idempotent for $T = X^+$) can be extended to arbitrary rational subsemigroups.

8. Entropy

Let $\mathscr{X}$ be a shift of $X^{\mathbb{Z}}$. The *complexity function of $\mathscr{X}$* is the map $q_{\mathscr{X}}$ that assigns to each positive integer n the number of elements of $L(\mathscr{X})$ with length n. This map satisfies the property $q_{\mathscr{X}}(n+m) \leq q_{\mathscr{X}}(n) \cdot q_{\mathscr{X}}(m)$. As proved in [25, Lemma 4.1.7], this property implies the convergence of the sequence $\{\frac{1}{n}\log_2 q_{\mathscr{X}}(n)\}$ to its infimum $h(\mathscr{X})$, called the *entropy of $\mathscr{X}$*. Complexity functions and entropy are fundamental notions in symbolic dynamics. In [10] these notions were adapted to the elements of $\widehat{F}_{\mathbf{V}}(X)$, where $\mathbf{V}$ is a variety of finite semigroups containing $\mathbf{LSl}$. More precisely, the *complexity function of an element w of $\widehat{F}_{\mathbf{V}}(X)$* is the map q_w that assigns to each positive integer n the number of finite factors of w with length n; this map also satisfies $q_w(n+m) \leq q_w(n) \cdot q_w(m)$, and so, if $w \notin X^+$, the sequence $\{\frac{1}{n}\log_2 q_w(n)\}$ converges to its infimum $h(w)$, called the *entropy of w*. The entropy of elements of X^* is defined to be 0.

One should be more precise and say that in [10] the entropy of $w \in \widehat{F}_{\mathbf{V}}(X) \setminus X^+$ is defined as the limit of $\{\frac{1}{n}\log_{|X|} q_w(n)\}$, which is $h(w)\log_{|X|} 2$ according to our definition of $h(w)$. The two definitions are essentially the same, but ours does not depend on the alphabet, and it is more consistent with the usual definition of entropy of a shift.

Next we recall from [10] some properties about the entropy of elements of $\widehat{F}_{\mathbf{V}}(X)$, starting with the following:

$$h(uv) = \max\{h(u), h(v)\}. \tag{8.1}$$

In particular, the set S_k of elements with entropy less than k is a subsemigroup of $\widehat{F}_{\mathbf{V}}(X)$. It is well know that the elements of relatively free profinite semigroups have an operational interpretation. Under this interpretation, these elements are called *implicit operations*; see [3] for details. We may compose implicit operations. Then (8.1) has the following generalization: if w is a r-ary implicit operation over $\mathbf{V}$, then

$$h(w(v_1, \ldots, v_r)) \leq \max\{h(w) \cdot \log_{|X|} 2 \cdot \log_{|X|} r, h(v_1), \ldots, h(v_r)\}. \tag{8.2}$$

If S is a finitely generated profinite semigroup, then the monoid $\mathrm{End}(S)$ of continuous endomorphisms of S is a profinite monoid, considered with the pointwise topology, which coincides with the compact-open topology [6]. For each $\varphi \in \mathrm{End}(S)$, elements of the subsemigroup of $\mathrm{End}(S)$ generated by φ are of the form φ^ν, where the exponent ν is an element of the profinite completion $\widehat{\mathbb{N}}$ of $\mathbb{N}$ (details can be found in [10]). It was proved in [10] that

$$\max_{x \in X} h(\varphi^\nu(x)) \leq \max_{x \in X} h(\varphi(x)) \tag{8.3}$$

for every $w \in \widehat{F}_{\mathbf{V}}(X)$ and $\nu \in \widetilde{\mathbb{N}} \setminus \{0\}$. A subset W of $\widehat{F}_{\mathbf{V}}(X)$ is *closed under iterations* if $\varphi(x) \in W$ implies $\varphi^\nu(x) \in W$, for all $\nu \in \widetilde{\mathbb{N}} \setminus \{0\}$ and $x \in X$. Note that by (8.3) the semigroup S_k is closed under iterations.

An important application of these results was given in [10]: it is easy to prove that an element w of $\widehat{F}_{\mathbf{V}}(X)$ belongs to the minimal ideal K_X if and only if $h(w) = \log_2 |X|$, hence one immediately concludes that $\widehat{F}_{\mathbf{V}}(X) \setminus K_X$ is a semigroup closed under iterations and composition with r-ary implicit operations w such that $h(w) < (\log_2 |X|)^2 \cdot \log_r |X|$. The minimal ideal K_X is the $\mathscr{J}$-class associated to the full shift $X^{\mathbb{Z}}$. We are going to prove analogues of these results for sofic shifts.

Let $F(w)$ be the set of finite factors of w. Suppose that $\overline{L(\mathscr{X})}$ is factorial. If $w \in \overline{L(\mathscr{X})}$ then $F(w) \subseteq L(\mathscr{X})$, and so $h(w) \leq h(\mathscr{X})$. Note that $h(w) = h(\mathscr{X})$ if $w \in J(\mathscr{X})$, since $F(w) = L(\mathscr{X})$ if $w \in J(\mathscr{X})$. The following proposition gives a converse. It is an analog of [25, Corollary 4.4.9], stating that if $\mathscr{Y}$ is a subshift strictly contained in a sofic shift $\mathscr{X}$ then $h(\mathscr{Y}) < h(\mathscr{X})$. The proof of the proposition consists in a reduction to this result.

Proposition 8.1. *Let* $\mathbf{V}$ *be a variety of finite semigroups containing* $\mathbf{LSl}$. *Suppose* $\mathscr{X}$ *is a non-periodic irreducible sofic shift such that* $\overline{L(\mathscr{X})}$ *is a factorial subset of* $\widehat{F}_{\mathbf{V}}(X)$. *If* $w \in \overline{L(\mathscr{X})} \setminus J(\mathscr{X})$ *then* $h(w) < h(\mathscr{X})$.

Proof: If $w \in X^+$ then $h(w) = 0$. Since $\mathscr{X}$ is a non-periodic irreducible sofic shift, we have $h(\mathscr{X}) > 0$ [25, Corollary 4.4.9], therefore we may suppose that $w \notin X^+$.

Let $\{w_n\}$ be a sequence of elements of $L(\mathscr{X})$ converging to w. Let $\lambda\colon X^+ \to S_{\mathscr{X}}$ be the syntactic morphism for $L(\mathscr{X})$. Taking subsequences, we may suppose that $|w_n| \geq 2|S_{\mathscr{X}}| + n$ for all n. From the proof of [3, Prop. 3.7.1] we conclude that given a homomorphism $\psi\colon B^+ \to T$ onto a finite semigroup T, then, for every $z \in B^+$ such that $|z| \geq |T|$, there are $z_0, z_2 \in B^*$ and $z_1 \in B^+$ such that $z = z_0 z_1 z_2$, $|z_0 z_1| \leq |T|$ and $\psi(z_1)$ is idempotent. Of course the dual result holds as well. Applying this result to the syntactic morphism λ, and to the prefix and the suffix of length $|S_{\mathscr{X}}|$ of w_n, we conclude that $w_n = w_{n,0}w_{n,1}w_{n,2}w_{n,3}w_{n,4}$ for some $w_{n,i} \in X^*$ such that $|w_{n,0}w_{n,1}| \leq |S_{\mathscr{X}}|$ and $|w_{n,3}w_{n,4}| \leq |S_{\mathscr{X}}|$, $w_{n,1}$ and $w_{n,3}$ are non-empty words whose image under λ is idempotent, and $|w_{n,2}| \geq n$. Taking subsequences, we may suppose that the sequence of tuples $\{(w_{n,0}, w_{n,1}, w_{n,2}, w_{n,3}, w_{n,4})\}$ converges to $(w_0, w_1, w_2, w_3, w_4)$. Then $w = w_0 w_1 w_2 w_3 w_4$. Note that $(w_i)^\omega = \lim_{k\to\infty} \lim_{n\to\infty} (w_{n,i})^{k!}$. Since $\lambda(w_{n,1})$ and $\lambda(w_{n,3})$ are idempotents and $\lambda(w_{n,1}\, w_{n,2}w_{n,3}) \neq 0$, the word $(w_{n,1})^{k!}w_{n,2}(w_{n,3})^{k!}$ belongs to $L(\mathscr{X})$ for all k, n. Therefore, the element $v = (w_1)^\omega w_2 (w_3)^\omega$ belongs to $\overline{L(\mathscr{X})}$.

We have $h(w) = \max\{h(w_0), h(w_1w_2w_3), h(w_4)\}$ by (8.1). But w_0 and w_4 belong to X^+, because the words $w_{n,0}$ and $w_{n,4}$ have bounded length. Therefore $h(w_0) = h(w_4) = 0$, and so $h(w) = h(w_1w_2w_3)$. Let ρ be the ternary implicit operation $x_1^\omega x_2 x_3^\omega$, on the three-letter alphabet $\{x_1, x_1, x_3\}$. Note that $v = \rho(w_1, w_2, w_3)$. Since $h(\rho) = \max\{h(x_1^\omega), h(x_2), h(x_3^\omega)\} = 0$, it follows from (8.2) that

$$h(v) = \max\{h(w_1), h(w_2), h(w_3)\} = h(w_1w_2w_3) = h(w).$$

So, it suffices to prove that $h(v) < h(\mathscr{X})$.

By Lemma 7.1, the hypothesis $w \in \overline{L(\mathscr{X})} \setminus J(\mathscr{X})$ implies the existence of a word $u \in L(\mathscr{X})$ such that u is not a factor of w.

The language $F(v)$ is clearly factorial, and it is prolongable because $v = w_1^\omega v w_3^\omega$ belongs to $\overline{\widehat{F}_{\mathbf{V}}(X)\, v\, \widehat{F}_{\mathbf{V}}(X)}$. Therefore $F(v) = L(\mathscr{Y})$ for some shift $\mathscr{Y}$. Since $v \in \overline{L(\mathscr{X})}$ and $\overline{L(\mathscr{X})}$ is factorial, we know that $F(v) \subseteq L(\mathscr{X})$ and $F(w_1^\omega) \cup F(w_2^\omega) \subseteq L(\mathscr{X})$. The set $F(w_1^\omega) \cup F(w_2^\omega)$ is the language of the union of two periodic shifts, whence $F(w_1^\omega) \cup F(w_2^\omega) \neq L(\mathscr{X})$, else $\mathscr{X}$ would not be irreducible non-periodic. Hence, there is a word u' belonging to $L(\mathscr{X})$ but not to $F(w_1^\omega) \cup F(w_2^\omega)$. Since $\mathscr{X}$ is irreducible, there are x, y such that the word $u'' = uxu'yu$ belongs to $L(\mathscr{X})$.

Suppose that u'' is a factor of $v = w_1^\omega w_2 w_3^\omega$. The word u'' is not a factor of w_1^ω or w_3^ω, (because u' is a factor of u''), nor of w_2 (because u is a factor of u'' and w_2 is a factor of w). By [10, Lemma 8.2] and the fact that $w_2 \in \widehat{F}_{\mathbf{V}}(X) \setminus X^+$, we have $u'' = sp$ for some words s and p such that s is a suffix of w_1^ω and p is a prefix of w_2, or such that s is a suffix of w_2 and p is a prefix of w_3^ω. Suppose the first case occurs. Then s does not have u' as factor, thus s is a strict prefix of uxu'. But then yu is a suffix of p, which is impossible, since u is not a factor of w_2. The first case leads to an absurdity, and similarly so does the second case. Hence u'' is not a factor of v.

Therefore $L(\mathscr{Y}) \subsetneq L(\mathscr{X})$, that is, $\mathscr{Y} \subsetneq \mathscr{X}$. By [25, Corollary 4.4.9], this implies $h(\mathscr{Y}) < h(\mathscr{X})$. Then it follows trivially from equality $F(v) = L(\mathscr{Y})$ that $h(v) < h(\mathscr{X})$. ∎

Proposition 8.1 states that $\overline{L(\mathscr{X})} \setminus J(\mathscr{X})$ is contained in the semigroup $S_{h(\mathscr{X})}$, stable under iterations. In general $\overline{L(\mathscr{X})} \setminus J(\mathscr{X})$ is not stable under iterations, but if we restrict to endomorphisms such that $\varphi(L(\mathscr{X})) \subseteq \overline{L(\mathscr{X})}$ then we obtain a positive result.

Another example in which one obtains a result weaker than in the case of the full shift, is the following: if $I(\mathscr{X})$ is the ideal generated by $J(\mathscr{X})$, then $S_{h(\mathscr{X})} \subseteq \widehat{F}_{\mathbf{V}}(X) \setminus I(\mathscr{X})$, but in general $S_{h(\mathscr{X})} \neq \widehat{F}_{\mathbf{V}}(X) \setminus I(\mathscr{X})$ and $\widehat{F}_{\mathbf{V}}(X) \setminus I(\mathscr{X})$ is not stable under iteration. For example, let $\mathscr{X}$ be a shift such that $\mathsf{alph}(\mathscr{X}) = \{a, b\}$ and let $X = \{a, b, c\}$. Let $u \in J(\mathscr{X})$. Consider the endomorphisms ψ and φ given by

$$\psi(a) = a,\ \psi(b) = c,\ \psi(c) = b, \qquad \varphi(a) = a,\ \varphi(b) = \psi(u),\ \varphi(c) = b.$$

Then $h(\psi(u)) = h(u)$ and $\varphi(\psi(u)) = u$. Since $\psi(u) \notin I(\mathscr{X})$ and $u \in I(\mathscr{X})$, it follows that $S_{h(\mathscr{X})} \neq \widehat{F}_{\mathbf{V}}(X) \setminus I(\mathscr{X})$ and that $\widehat{F}_{\mathbf{V}}(X) \setminus I(\mathscr{X})$ is not stable under iteration. On the other hand, $\widehat{F}_{\mathbf{V}}(X) \setminus I(\mathscr{X})$ is a semigroup whenever $\mathbf{V} = \mathbf{A} ⓜ \mathbf{V}$ [32].

References

[1] D. Allen, Jr. and J. Rhodes. Synthesis of classical and modern theory of finite semigroups. *Advances in Math.*, 11(2):238–266, 1973.

[2] J. Almeida. *Finite and profinite semigroups and symbolic dynamics*. Notes for a course in the Ural State University, first semester of 2005.

[3] J. Almeida. *Finite semigroups and universal algebra*, volume 3 of *Series in Algebra*. World Scientific Publishing Co. Inc., River Edge, NJ, 1994. Translated from the 1992 Portuguese original and revised by the author.

[4] J. Almeida. Profinite structures and dynamics. *CIM Bulletin*, 14:8–18, 2003.

[5] J. Almeida. Profinite groups associated with weakly primitive substitutions. *Fundam. Prikl. Mat.*, 11(3):13–48, 2005. Translation in *J. Math. Sci. (N. Y.)* 144(2):3881–3903, 2007.

[6] J. Almeida. Profinite semigroups and applications. In V. B. Kudryavtsev and I. G. Rosenberg, editors, *Structural Theory of Automata, Semigroups and Universal Algebra*, pages 1–45, New York, 2005. Springer.

[7] J. Almeida and A. Costa. The Schützenberger group associated to the Thue-Morse subshift. In preparation.

[8] J. Almeida and A. Costa. Infinite-vertex free profinite semigroupoids and symbolic dynamics. *J. Pure Appl. Algebra*, 213(5):605–631, 2009.

[9] J. Almeida and M. V. Volkov. Profinite identities for finite semigroups whose subgroups belong to a given pseudovariety. *J. Algebra Appl.*, 2(2):137–163, 2003.

[10] J. Almeida and M. V. Volkov. Subword complexity of profinite words and subgroups of free profinite semigroups. *Internat. J. Algebra Comput.*, 16(2):221–258, 2006.

[11] D. Beauquier. Minimal automaton for a factorial, transitive, and rational language. *Theoret. Comput. Sci.*, 67(1):65–73, 1989.

[12] J. Berstel, D. Perrin, and C. Reutenauer. *Codes and automata*. Cambridge University Press, to appear.

[13] A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups. Vol. I.* Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1961.

[14] A. Costa. Conjugacy invariants of subshifts: an approach from profinite semigroup theory. *Internat. J. Algebra Comput.*, 16(4):629–655, 2006.

[15] A. Costa. Pseudovarieties defining classes of sofic subshifts closed under taking shift equivalent subshifts. *J. Pure Appl. Algebra*, 209(2):517–530, 2007.

[16] A. Costa. *Semigrupos Profinitos e Dinâmica Simbólica*. PhD thesis, Faculdade de Ciências da Universidade do Porto, 2007.

[17] S. Eilenberg. *Automata, languages, and machines. Vol. A*. Academic Press, New York, 1974. Pure and Applied Mathematics, Vol. 58.

[18] S. Eilenberg. *Automata, languages, and machines. Vol. B*. Academic Press, New York, 1976. With two chapters ("Depth decomposition theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

[19] R. Fischer. Sofic systems and graphs. *Monatsh. Math.*, 80(3):179–186, 1975.

[20] P.-A. Grillet. *Semigroups*, volume 193 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1995. An introduction to the structure theory.

[21] K. Iwasawa. On solvable extensions of algebraic number fields. *Ann. of Math (2)*, 58:548–572, 1953.

[22] K. Krohn and J. Rhodes. Complexity of finite semigroups. *Ann. of Math. (2)*, 88:128–160, 1968.

[23] K. Krohn, J. Rhodes, and B. Tilson. *Algebraic theory of machines, languages, and semigroups*. Edited by Michael A. Arbib. With a major contribution by Kenneth Krohn and John L. Rhodes. Academic Press, New York, 1968. Chapters 1, 5–9.

[24] G. Lallement. *Semigroups and combinatorial applications*. John Wiley & Sons, New York-Chichester-Brisbane, 1979. Pure and Applied Mathematics, A Wiley-Interscience Publication.

[25] D. Lind and B. Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.

[26] N. R. Reilly and S. Zhang. Decomposition of the lattice of pseudovarieties of finite semigroups induced by bands. *Algebra Universalis*, 44(3-4):217–239, 2000.

[27] A. Restivo. Codes and aperiodic languages. In *Erste Fachtagung der Gesellschaft für Informatik über Automatentheorie und Formale Sprachen (Bonn, 1973)*, pages 175–181. Lecture Notes in Computer Science, Vol. 2. Springer, Berlin, 1973.

[28] J. Rhodes. Algebraic theory of finite semigroups. Structure numbers and structure theorems for finite semigroups. In K. Folley, editor, *Semigroups (Proc. Sympos., Wayne State Univ., Detroit, Mich., 1968)*, pages 125–162. Academic Press, New York, 1969.

[29] J. Rhodes and B. Steinberg. Closed subgroups of free profinite monoids are projective profinite groups. *Bull. London Math. Soc.*, 40(3):375–383, 2008.

[30] J. Rhodes and B. Steinberg. *The q-theory of finite semigroups*. Springer Monographs in Mathematics. Springer, New York, 2009.

[31] L. Ribes and P. Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, 2000.

[32] B. Steinberg. A combinatorial property of ideals in free profinite monoids. arxiv:0811.1274, 2008.

[33] B. Steinberg. Maximal subgroups of the minimal ideal of a free profinite monoid are free. *Israel J. Math.*, to appear.

[34] B. R. Tilson. Appendix to "Algebraic theory of finite semigroups". On the p-length of p-solvable semigroups: Preliminary results. In K. Folley, editor, *Semigroups (Proc. Sympos., Wayne State Univ., Detroit, Mich., 1968)*, pages 163–208. Academic Press, New York, 1969.

[35] P. Weil. Groups in the syntactic monoid of a composed code. *J. Pure Appl. Algebra*, 42(3):297–319, 1986.

Alfredo Costa
CMUC, Department of Mathematics, University of Coimbra, 3001-454 Coimbra
E-mail address: amgc@mat.uc.pt

Benjamin Steinberg
Carleton University, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada
E-mail address: bsteinbg@math.carleton.ca