PROFINITE STRUCTURES AND DYNAMICS

JORGE ALMEIDA

Surprising as it may be at first sight, there are a number of connections between the theories of finite semigroups and dynamical systems, both viewed in a broad sense. For instance in symbolic dynamics, ideas or analogies from the theory of finite automata find a natural setting for application in sofic systems [10, 24] and, even though not usually formulated in dynamical terms, the dynamical behavior of various operators on finite groups has been extensively studied. The purpose of this note is to review some further connections that have emerged recently driven mainly by work on finite semigroups and thus perhaps open the path to new investigations in this area.

The main tool underlying our approach is found in profinite constructions, be it semigroups, groups, graphs or categories. Generally speaking, profinite structures are a way of encoding, with the help of an additional topological structure, common properties of a class of finite structures of the same type. This idea can be found in various areas, from Galois theory [17] to finite semigroup theory [6, 35, 4].

Results which are given without reference are announced here for the first time and will be proved elsewhere.

A general framework for dynamics in profinite structures

We start by quickly recalling some terminology from model theory. See [27] for details.

Let $\mathcal{L}$ be a *first-order language* given by a finite set $\mathcal{F}$ of *operation symbols* and a finite set $\mathcal{R}$ of *relation symbols* together with a function α with nonnegative integer values describing the *arity* of each symbol. Let $\mathfrak{A}$ be an $\mathcal{L}$*-structure*, which is determined by a choice of a nonempty set A (the *universe*), for each operation symbol $f \in \mathcal{F}$ an operation $f^{\mathfrak{A}} : A^{\alpha(f)} \to A$, and for each relation symbol $R \in \mathcal{R}$ a relation $R^{\mathfrak{A}} \subseteq A^{\alpha(R)}$. For example, semigroups are structures in the language with one binary operation symbol and ordered semigroups are structures in the language that has an additional binary relation symbol, in both cases with the usual properties bing assumed.

A *homomorphism* of $\mathcal{L}$-structures $\mathfrak{A} \to \mathfrak{B}$ is a function $\gamma : A \to B$ between the corresponding universes such that, for every operation symbol $f \in \mathcal{F}$ with arity m, and all $a_1, \ldots, a_m \in A$,

$$(1) \qquad \gamma\big(f^{\mathfrak{A}}(a_1, \ldots, a_m)\big) = f^{\mathfrak{B}}\big(\gamma(a_1), \ldots, \gamma(a_m)\big)$$

and for every relation symbol $R \in \mathcal{R}$ with arity n and all $a_1, \ldots, a_n$,

$$(2) \quad (a_1, \ldots, a_n) \in R^{\mathfrak{A}} \Rightarrow \big(\gamma(a_1), \ldots, \gamma(a_n)\big) \in R^{\mathfrak{B}}.$$

Note that the reverse implication of (2) is not assumed in our definition of homomorphism. So, for the definition of *isomorphism* we take a bijective homomorphism whose inverse is also a homomorphism.

A *substructure* of a structure $\mathfrak{A}$ is a structure $\mathfrak{B}$ such that the corresponding universes satisfy the inclusion $B \subseteq A$, and each operation $f^{\mathfrak{B}}$ and each relation $R^{\mathfrak{B}}$ is the restriction to the set B of the corresponding operation $f^{\mathfrak{A}}$ and relation $R^{\mathfrak{A}}$ on A. Given a subset X of the universe A of a structure $\mathfrak{A}$, the *substructure generated by* X is the structure $\mathfrak{B}$ with universe B the smallest subset of A that contains X and that is closed under every operation $f^{\mathfrak{A}}$ with $f \in \mathcal{F}$. Direct products of structures are defined by taking the Cartesian product of their universes and interpreting operation and relation symbols component-wise.

From this point on we will abuse notation and talk about structures rather than $\mathcal{L}$-structures and a structure $\mathfrak{A}$ with universe A will be referred simply as 'the structure A' and we will talk of an operation f and a relation R instead of $f^{\mathfrak{A}}$ and $R^{\mathfrak{A}}$, respectively.

We say that a structure A is *finite* if the set A is finite. If the set A is endowed with a topology such that each operation f is continuous and each relation R is closed, then we say that A is a *topological structure*. Finite structures are viewed as topological structures for the discrete topology. For a class $\mathcal{C}$ of topological structures, a topological structure A is said to be *residually in* $\mathcal{C}$ if for any two distinct points $a, b \in A$ there is a continuous homomorphism $\gamma : A \to F$ into some $F \in \mathcal{C}$ such that $\gamma(a) \neq \gamma(b)$. A compact, Hausdorff, residually in $\mathcal{C}$, structure is called a *pro-*$\mathcal{C}$ *structure*. In case $\mathcal{C}$ consists of all finite structures, then we talk respectively of a *residually finite* and a *profinite* structure. Note that a structure is profinite if and only if it embeds as a closed substructure in a product of finite structures.

For instance, profinite groups have been extensively studied in connection with Galois theory, number theory, and model theory [17, 29], and free profinite semigroups play a prominent role in the theory of pseudovarieties of finite semigroups [4, 6, 35], which will be introduced in the next section.

We say that a topological structure A is *finitely generated* if there is a finite subset of A such that the substructure it generates is dense in A.

We denote by $\operatorname{End} A$ the set of continuous endomorphisms of a topological structure A. Note that it is a monoid under the operation of composition. Its group of units is the group $\operatorname{Aut} A$ of continuous automorphisms of A.

For the study of a profinite structure A, it is useful to have at hand a topology on $\operatorname{End} A$ for which $\operatorname{End} A$ is a profinite monoid and the evaluation mapping

$$(3) \qquad \begin{array}{rcl} \operatorname{End} A \times A & \to & A \\ (\gamma, a) & \mapsto & \gamma(a) \end{array}$$

is continuous. Two classical candidates are the pointwise convergence topology, that is the induced topology from the product topology in A^A, and the compact-open topology. These topologies do not always satisfy the above requirements but we do have the following result that extends well-known facts in the theory of profinite groups [29].

Theorem 1. *Let A be a finitely generated profinite structure. Then* End A *is a profinite monoid and* Aut A *is a profinite group under the point-wise convergence topology, which coincides with the compact-open topology, and the evaluation mapping* (3) *is continuous.*

Dynamics of continuous endomorphisms

A *topological dynamical system* (T, f) is a topological structure T for the language with only one operation symbol f, which is unary, and no relation symbols. Two topological dynamical systems (T, f) and (U, g) are said to be *conjugate* if they are isomorphic as topological structures; an isomorphism $\varphi : T \to U$ between them is usually called a *conjugacy*, since it is a homoeomorphism which satisfies $\varphi \circ f = g \circ \varphi$.

For example, if A is a finitely generated profinite structure then, fixing $\gamma \in \operatorname{End} A$, we have a topological dynamical system (A, γ), which just says that A is a topological space and γ is a continuous transformation of A. For the infinite iteration of γ, we use Theorem 1 to introduce an operation that is well-known in finite semigroup theory.

For an element m of a finite monoid M, the sequence $(m^{n!})_n$ becomes constant for $n \geq |M|$, therefore it converges in M, and moreover this eventual constant value is an idempotent. Since a profinite monoid embeds in the product of its finite continuous homomorphic images, if m is an element of a profinite monoid M, then the sequence $(m^{n!})_n$ also converges in M; its limit is denoted m^ω and by the above it is an idempotent. Similarly, we may define $m^{\omega+k}$ to be the limit of the sequence $(m^{n!+k})_{n \geq |k|}$ for any integer k. Note that, if G is a profinite group, then $g^{\omega+k} = g^k$ for every $g \in G$ and integer k.

Going back to our dynamical system (A, γ), we have a very special infinite iterate γ^ω of γ, which is an idempotent, namely the only idempotent in the (closed) subsemigroup of End A generated by γ. We proceed to examine how the dynamics of the system is determined by this particular iterate.

Recall that a point x of a topological dynamical system (X, φ) is *periodic* if there exists k such that $\varphi^k(x) = x$; the point x is *recurrent* if, for every neighborhood U of x and every k, there exists $\ell \geq k$ such that $f^\ell(x) \in U$; and x is *uniformly recurrent* if there exists m such that, for every neighborhood U of x and every k, there exists $\ell \in \{k+1, \ldots, k+m\}$ such that $f^\ell(x) \in U$. Note that periodicity implies uniform recurrence which in turn implies recurrence.

Of course, if X is finite then the above three properties are equivalent and the periodic points are the elements of the image of φ^ω (note that φ is an element of the finite monoid of all transformations of X). So in particular, if A is a finite structure and $\gamma \in \operatorname{End} A$, then the three notions are equivalent for points of the dynamical system (A, γ). For general topological dynamical systems, there are well-known examples in which no two of the three notions are equivalent. But, what about dynamical systems of the form (A, γ) with A a finitely generated profinite structure? It is easy to construct examples in which periodicity and uniform recurrence are inequivalent but it turns out that the two forms of recurrence coincide in such systems. The following result improves [2, Proposition 3.1].

Proposition 1. *Let A be a finitely generated profinite structure and let γ be a continuous endomorphism of A. Then every recurrent point of A under the action of γ is uniformly recurrent and the set of all such points is the image of γ^ω.*

Relatively free structures and implicit operations

We extend the notion of generating set X of a structure A by allowing X to be a topological space for which there is a continuous function $X \to A$ (the generating mapping) whose image generates A in the previous sense. In general we will omit reference to the generating mapping although we always consider a specific one when we talk about a generating space. Note that a generating mapping may not be injective. To avoid degenerate cases, from hereon we will consider only nonempty generating spaces.

We say that a structure A is *weakly free* with respect to a generating mapping $\iota : X \to A$ if every continuous mapping $\varphi : X \to A$ *extends* (uniquely) to a continuous endomorphism $\hat{\varphi}$ of A in the sense that $\hat{\varphi} \circ \iota = \varphi$. There is a related notion of relatively free structure that we proceed to introduce.

By a *pseudovariety* of finite structures (always of a fixed first-order language) we mean a class of such structures that is closed under taking homomorphic images, substructures and finite direct products. Note that, if $\varphi : A \to B$ is an onto homomorphism, then we call B a homomorphic image of A even though relation symbols may be interpreted in B as larger sets than the images of their interpretations in A. Pseudovarieties of finite semigroups and monoids have been extensively studied in connection with applications to automata, formal languages, circuit complexity, and temporal logic [15, 1, 30] and embody at present the most developed part of finite semigroup theory.

Let V be a pseudovariety of finite structures. We say that a pro-V structure A is V-*free* with respect to a generating mapping $\iota : X \to A$ if every continuous mapping $\varphi : X \to B$ into another pro-V structure *extends* (uniquely) to a continuous homomorphism $\hat{\varphi} : A \to B$ in the sense that $\hat{\varphi} \circ \iota = \varphi$. A profinite structure is *relatively free* with respect to a generating mapping ι if it is V-free with respect to ι for some pseudovariety V. Elements of a generating set for a relatively free structure are often called *letters*. In case $|X| = n$, we will usually presume an ordering $x_1, \ldots, x_n$ of the letters.

Proposition 2. *A profinite structure A is relatively free with respect to a generating mapping ι if and only if A is weakly free with respect to ι.*

From the definition of V-free structure A with respect to a generating mapping $\iota : X \to A$ it follows that, for a fixed space X, it is unique up to isomorphism. The existence of such a structure is established by observing that it may be constructed as the projective limit of all X-generated members of V. In general the generating mapping is understood and we talk simply about the relatively V-free structure on the space X. It will be denoted $\overline{\Omega}_X\mathsf{V}$. In case X is a (nonempty) finite set, we sketch an alternative construction of $\overline{\Omega}_X\mathsf{V}$. See [4] for details.

Let $F(X)$ denote the absolutely free structure on the set X, whose algebraic structure is that of the algebra of terms in X in the fixed first-order language $\mathcal{L}$, and where all relational symbols are interpreted as the empty set. The intersection of all kernels of homomorphisms into members of V is a congruence θ on $F(X)$. Endow the quotient $\Omega_X\mathsf{V} = F(X)/\theta$ with the structure in which, for an n-ary relational symbol R in $\mathcal{L}$, and $w_1, \ldots, w_n \in F(X)$, we set $(w_1/\theta, \ldots, w_n/\theta) \in R$ in $\Omega_X\mathsf{V}$ if and only if $(\varphi(w_1), \ldots, \varphi(w_n)) \in R$ in B for every $B \in \mathsf{V}$ and every homomorphism $\varphi : F(X) \to B$. Then, by construction, $\Omega_X\mathsf{V}$ is a minimal V-free abstract structure in the sense that, for the natural mapping $\iota : X \to \Omega_X\mathsf{V}$ and any mapping $\varphi : X \to B$ with $B \in \mathsf{V}$, there is a unique homomorphism $\hat{\varphi} : \Omega_X\mathsf{V} \to B$ such that $\hat{\varphi} \circ \iota = \varphi$ and any homomorphism of $\Omega_X\mathsf{V}$ onto a structure with the same property is an isomorphism. It is an easy exercise to show that $\Omega_X\mathsf{V}$ embeds in $\overline{\Omega}_X\mathsf{V}$ as the substructure generated by X and this partly explains the notation since this substructure is dense. The letter Ω is meant to suggest that the elements of $\Omega_X\mathsf{V}$ may be viewed as polynomial operations over V in the set X of variables. We also give below an interpretation of the elements of $\overline{\Omega}_X\mathsf{V}$ as operations.

We may define a metric structure on $\Omega_X\mathsf{V}$ by setting $d(u, v) = 2^{-r(u,v)}$, for distinct $u, v \in \Omega_X\mathsf{V}$, where $r(u, v)$ denotes the minimum cardinality of $B \in \mathsf{V}$ for which there exists a homomorphism $\varphi : \Omega_X\mathsf{V} \to B$ such that $\varphi(u) \neq \varphi(v)$, and taking $d(u, u) = 0$. Instead of proving the triangle inequality, it is more natural to establish the stronger ultra-metric inequality $d(u, w) \leq \max\{d(u, v), d(v, w)\}$. A sequence in $\Omega_X\mathsf{V}$ is a Cauchy sequence if and only if its image under any homomorphism into a member of V converges. This implies that, in $\Omega_X\mathsf{V}$, $\mathcal{L}$-operations are uniformly continuous with respect to d and that $\mathcal{L}$-relations are closed sets. Hence the completion of $\Omega_X\mathsf{V}$ with respect to the metric d is a topological structure and one can show that it is isomorphic with $\overline{\Omega}_X\mathsf{V}$.

The elements of $\overline{\Omega}_X\mathsf{V}$ may also be viewed as operations as follows. Let A be a pro-V structure. For $w \in \overline{\Omega}_X\mathsf{V}$, we define an operation $w_A : A^X \to A$ by letting, for a function $\varphi : X \to A$, $w_A(\varphi) = \hat{\varphi}(w)$ where $\hat{\varphi} : \overline{\Omega}_X\mathsf{V} \to A$ is the unique continuous homomorphism such that $\hat{\varphi} \circ \iota = \varphi$. Thus w becomes an $|X|$-ary operation with a 'natural' interpretation on every pro-V structure, and it is an easy exercise to show that this interpretation commutes with continuous homomorphisms between pro-V structures; such an operation is said to be an *implicit operation* (on the class of pro-V structures). We say w 'becomes' an operation since the fact that $\overline{\Omega}_X\mathsf{V}$ is residually in V implies that already the natural interpretations of w as an operation in the members of V completely determine w. Moreover, one can show that every implicit operation on V arises in this way. In other words, the natural interpretation determines a bijection between $\overline{\Omega}_X\mathsf{V}$ and the set of $|X|$-ary implicit operations on V and therefore we may think of the elements of $\overline{\Omega}_X\mathsf{V}$ themselves as implicit operations.

Since, up to isomorphism, $\overline{\Omega}_X\mathsf{V}$ depends only on $n = |X|$ and V, we may write $\overline{\Omega}_n\mathsf{V}$ instead of $\overline{\Omega}_X\mathsf{V}$.

Sometimes it is also useful to consider some structure on the generating set X. Usually this is done by reducing the first-order language by dropping some operation or relation symbols. The case described above in some detail corresponds to dropping all such symbols, so that structures are plain sets. Of course then, rather than considering functions from X into structures of the given language, one takes homomorphisms in the reduced language. The above may be carried out in this context, *mutatis mutandis*. A further restriction which is sometimes useful is to assume that X is a topological structure of the reduced language, in which case homomorphisms from X are also assumed to be continuous, as we already did in the definition of relatively free profinite structure.

Dynamics of implicit operators

The implicit operation point of view is particularly suited for iteration, and thus for a dynamical study. It was basically as a result of this observation that the author started getting involved with dynamical systems [3].

Let us concentrate on the case of a finite generating set $X = \{x_1, \ldots, x_n\}$. Since $\overline{\Omega}_X\mathsf{V}$ is weakly free, a continuous endomorphism γ of $\overline{\Omega}_X\mathsf{V}$ is completely determined by the n-tuple $(\gamma(x_1), \ldots, \gamma(x_n))$. Thus, giving an element of $\gamma \in \operatorname{End}\overline{\Omega}_X\mathsf{V}$ is equivalent to choosing an n-tuple $(w_1, \ldots, w_n)$ of n-ary implicit operations on V. We will abuse notation and write $\gamma = (w_1, \ldots, w_n)$. Moreover, for any pro-$\mathsf{V}$ structure A, we have an associated transformation $\gamma_A : A^n \to A^n$ defined by the natural interpretations of the w_i as follows:

$$v \in A^n \mapsto ((w_1)_A(v), \ldots, (w_n)_A(v)).$$

Such a transformation of A^n is called an *n-ary implicit operator on A*, as in [3] from where the following result can be derived.

Proposition 3. *The set of n-ary implicit operators on a profinite structure A is a profinite monoid with respect to the component-wise point-wise convergence topology and the evaluation mapping is continuous. Moreover, in case A is weakly free on n generators, this profinite monoid is isomorphic with* $\operatorname{End} A$ *via the correspondence described above.*

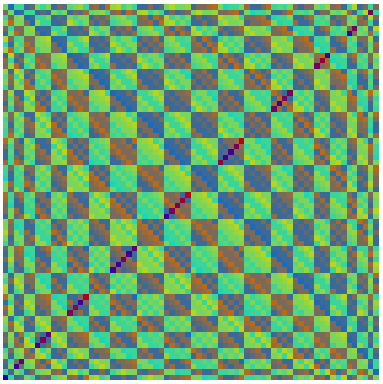

FIGURE 1. The Thuë-Morse operator on $\mathbb{Z}/70\mathbb{Z}$

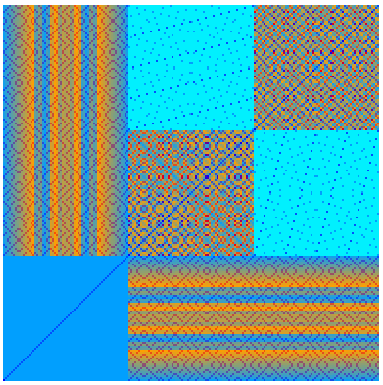

FIGURE 2. The Thuë-Morse operator on $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}/3\mathbb{Z}$

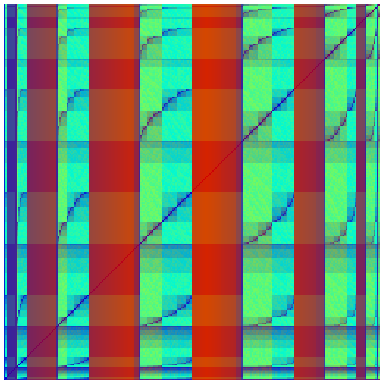

FIGURE 3. Action of the operator $(y^{\omega-1}xy, x)$ on D_{256}

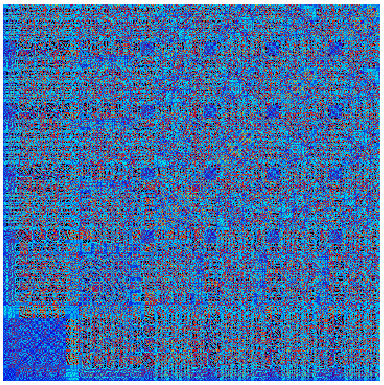

FIGURE 4. Action of the Thuë-Morse operator on A_6

One may thus consider an arbitrary pro-V structure A and implicit operations $w_1, \ldots, w_n \in \overline{\Omega}_n\mathsf{V}$ and the idempotent infinite iterate $(w_1, \ldots, w_n)^\omega$ on A^n. The behavior of this operator may be closely linked with structural properties of A. Examples of this situation are explored in [2] for pseudovarieties of finite groups. We present next a few examples of this phenomenon.

Denote by S the pseudovariety of all finite semigroups. Note that the subclass G consisting of all finite groups is also a pseudovariety. Define the *commutator* of x and y to be $[x, y] = x^{\omega-1}y^{\omega-1}xy$, which determines a binary implicit operation on finite semigroups that coincides with the usual commutator on finite groups.

Example 2. Note that, on finite groups, the first component of $([x, y], y)^n$ is the usual iterated commutator $[x, {}_n y]$. Similarly, for an integer k, denote by $[x, {}_{\omega+k}y]$ the binary implicit operation defined by taking the first component of $([x, y], y)^{\omega+k}$. Then, by a theorem of Zorn [37], a finite group G is nilpotent if and only if G satisfies the operation equation $[x, {}_\omega y] = 1$.

In the preceding example, strictly speaking 1 is not an operation in our chosen language but we could take any idempotent like x^ω in its place. Or we could take, for an implicit operation w, $w = 1$ to be an abbreviation of the equations $wy = yw = w$ where y is a new variable. In general, an equation whose sides are implicit operations on V (which can always be viewed as being of the same arity) is called a *pseudoidentity*. It is said to be *valid* in a pro-V structure A if the natural interpretations in A of both sides coincide. For a set Σ of pseudoidentities, the class of all structures from V that satisfy all pseudoidentities from Σ is denoted $[\![\Sigma]\!]$. It is a pseudovariety and every pseudovariety W contained in V is of the form $\mathsf{W} = [\![\Sigma]\!]$ for some set Σ of pseudoidentities, in which case we also say that Σ is a *basis of pseudoidentities* of W or that W *is defined by* Σ. This is an extension of Reiterman's Theorem [28] that has been independently established in [26, 27].

Example 3. Let w denote the ternary operation defined by $(w, y, z) = ([[x, y], [x, z]], y, z)^\omega$. B. Plotkin has proposed a conjecture that translates into saying that the pseudovariety of all finite solvable groups is defined by the pseudoidentity $w([x, y], x, y) = 1$ [18]. In the same vein the author [2] has proposed the following alternative pseudoidentity: $u = v$ where $(u, v) = ([x, y], [x^{\omega-1}, y^{\omega-1}])^\omega$. The proof that such characterizations of solvability for finite groups hold is not likely to be very simple since one consequence of them is that a finite group is solvable if and only if all its 2-generated subgroups are solvable. This property was first established by Thompson [32] as a consequence of his monumental classification of finite

simple groups whose proper subgroups are solvable, whose proof extends over 400 printed pages and which earned J. G. Thompson the Fields Medal in 1970. A much shorter yet rather involved proof of the 2-generator characterization of finite solvable groups has been given by Flavell [16].

One may try to visualize the dynamical behavior of an implicit operator on a finite structure. The examples in Figures 1 through 4 were calculated using GAP [31] for the group calculations and Mathematica [36] for converting them into a picture of the action of a binary implicit operator on a finite group G. The method used was to draw a square grid of pixels, each pixel representing a point in $G \times G$. Each pixel is colored with the three basic colors green, red and blue. The intensity of green represents the distance of the point to the cycle in its orbit so that, in particular, pixels corresponding to periodic points get no green color component. By taking a total ordering of the cycles and associating to each cycle an increasing intensity of blue and a decreasing intensity of red, according to its position in the ordering, each pixel gets the blue and red tonality determined by the cycle in its orbit. Of course, the final picture will depend on the ordering of the elements of the group G and the ordering of the cycles. We just took the ordering of the groups given by GAP and the ordering of cycles is by first appearance as the cycle in the orbit of the successive elements of G.

The picture for the *Thuë-Morse* implicit operator $(x, y) \mapsto (xy, yx)$ acting on the cyclic group $\mathbb{Z}/70\mathbb{Z}$ is shown on Figure 1, where the intensities of the basic colors have been weighted to increase the spatial visual effect. Figure 2 represents the action of the same operator on the wreath product of the Klein 4-group by the group of order 3. The fractal-like Figure 3 portrays the action of the iterated conjugation operator $(x, y) \mapsto (y^{\omega-1}xy, x)$ on the dihedral group D_{256} of order 256. Finally, in contrast, with the above examples, where one immediately recognizes patterns, the much more "chaotic" Figure 4 represents the action of the Thuë-Morse operator on the alternating group A_6.

So far these examples have only been used to experimentally explore the behavior of operators or simply for their aesthetic appeal. They may be viewed as approximations or as representing a small portion of the pictures of the action of the same operators on profinite groups, which seems to explain their fractal-like appearance.

Here is a small sample of other results concerning the action of implicit operators on finite groups.

Theorem 4 (Širšov [34])**.** *Consider the binary implicit operations u and v defined by $(u, v) = (xy, yx)^\omega$, the idempotent iterate of the Thuë-Morse operator. Then a finite group satisfies the pseudoidentity $u = v$ if and only if it is an extension of a nilpotent group by a 2-group.*

Theorem 5. *Let $(u, v) = (y^{\omega-1}xy, x)^\omega$. Then the pseudoidentity $u = 1$ defines the pseudovariety of all finite nilpotent groups.*

The following result provides partial information on finite groups for which the iterated commutator has period 1. A structure A is said to *divide* a structure B if A is a homomorphic image of a substructure of B.

Theorem 6. *Let G be a finite group satisfying the pseudoidentity $[x, {}_{\omega+1}y] = [x, {}_{\omega}y]$. Then*

(a) *G is supersolvable and G is a direct product of a group of order relatively prime to 6 with a group of order 2^m3^n which has a normal Sylow 3-subgroup (Brandl [11]) ;*
(b) *G is either nilpotent or divisible by the symmetric group S_3 (A. Costa [13]).*

Dynamics of implicit operators on free profinite semigroups

We first introduce briefly the most basic tools in semigroup theory. Readers interested in more details might wish to consult a book in the area such as [23].

In a semigroup S, say that an element s is a *factor* of (or *lies $\mathcal{J}$-below*) another element t if t can be written as a product $t = t_1 \cdots t_r$ with $r \geq 1$ and some $t_i = s$. Two elements are *associates* if they are factors of each other. This defines an equivalence relation on S which is one of *Green's relations*, denoted $\mathcal{J}$. Similarly, one may consider left factors or *prefixes*, with corresponding equivalence relation $\mathcal{R}$, and right factors or *suffixes*, with corresponding equivalence relation $\mathcal{L}$. For a compact semigroup, the smallest equivalence relation, denoted $\mathcal{D}$, containing both $\mathcal{R}$ and $\mathcal{L}$ is precisely $\mathcal{J}$. The intersection $\mathcal{R} \cap \mathcal{L}$ provides the last of Green's relations, denoted $\mathcal{H}$. The maximal subgroups of S are precisely the $\mathcal{H}$-classes that contain idempotents and any two of them contained in the same $\mathcal{D}$-class are isomorphic.

An element s of a semigroup S is *regular* if there exists $t \in S$ such that $sts = s$. All or none of the elements in a $\mathcal{D}$-class are regular, and the former condition holds if and only if the $\mathcal{D}$-class contains an idempotent.

Free pro-V semigroups have been computed for some very special examples of pseudovarieties of semigroups, often with numerous applications as in the case of the pseudovariety

$$\mathsf{J} = [\![(xy)^\omega = (yx)^\omega, x^{\omega+1} = x^\omega]\!]$$

which consists of all finite semigroups in which the $\mathcal{J}$-classes are singletons. It turns out that $\overline{\Omega}_n\mathsf{J}$ is a relatively free structure in the language with a symbol added for the ω-power operation, and a finite basis of equations (that is, a finite presentation consisting of universal relations) has been given and the word problem has been solved for this structure [1].

But for instance very little is known about the free profinite semigroups $\overline{\Omega}_n\mathsf{S}$. As in the previous section, we may use infinite iteration of implicit operators to define complex implicit operations from simple ones. This has been recently used as a tool to study the semigroups $\overline{\Omega}_n\mathsf{S}$ in [8]. We proceed to review a sample of results from that paper.

The semigroup $\Omega_n\mathsf{S}$ is the free semigroup on n letters and so its elements may be viewed as words on

the letters, for which an appropriate model is the sequence of letters in the unique factorization into letters. Since implicit operations are limits of sequences of finite words, we may also call them *profinite words*. So, of course, a profinite word $w \in \overline{\Omega}_n\mathsf{S}$ is said to be *finite* if it belongs to $\Omega_n\mathsf{S}$ and we will say it is *infinite* otherwise. The *length* of a finite word is the length of the sequence of letters that compose it.

An infinite profinite word w is said to be *recurrent* if every finite factor of w is also a factor of every infinite factor of w; and we say that w is *uniformly recurrent* if every finite factor of w is also a factor of every sufficiently long finite factor of w. One can easily show that these two notions are equivalent. We prefer to refer to uniformly recurrent profinite words for reasons that will be made clear in the next section.

An implicit operator $\varphi = (w_1, \ldots, w_n)$ ($w_i \in \overline{\Omega}_n\mathsf{S}$) is *finite* if its components are finite words; we say that φ is *primitive* if, for some finite exponent k, all components of φ^k admit all letters as factors; and φ is G-*invertible* if the induced operator on $(\overline{\Omega}_n\mathsf{G})^n$ is invertible. These notions are carried to continuous endomorphisms of $\overline{\Omega}_n\mathsf{S}$ via the isomorphism of Proposition 3. One can easily show that, for a primitive implicit operator $(w_1, \ldots, w_n)$, all components of the idempotent iterate $(v_1, \ldots, v_n) = (w_1, \ldots, w_n)^\omega$ are $\mathcal{J}$-equivalent [8]. Moreover, in case the w_i are finite, then the v_i are uniformly recurrent.

Theorem 7. [8] *Let $(w_1, \ldots, w_n)$ be a primitive, G-invertible, implicit operator all of whose components start with the same letter and end with the same letter. Let $(v_1, \ldots, v_n) = (w_1, \ldots, w_n)^\omega$. Then $\{v_1, \ldots, v_n\}$ freely generates a profinite subgroup of $\overline{\Omega}_n\mathsf{S}$ which is a retract of $\overline{\Omega}_n\mathsf{S}$. Moreover, every retract subgroup isomorphic with $\overline{\Omega}_n\mathsf{G}$ is obtained in this way.*

For example, the components of $(xyx, x)^\omega$ freely generate a profinite subgroup of $\overline{\Omega}_2\mathsf{S}$ but those of the operator $(xy, yx)^\omega$ do not even belong to the same $\mathcal{H}$-class although they are $\mathcal{J}$-equivalent.

The interest in finding n-tuples $(v_1, \ldots, v_n)$ of profinite words which freely generate profinite retract subgroups of $\overline{\Omega}_n\mathsf{S}$, which are called *group-generic*, stands from the fact that such n-tuples may be used to construct bases of pseudoidentities for pseudovarieties of semigroups which are derived from pseudovarieties of groups as follows. Let H be a pseudovariety of groups. Then the class $\overline{\mathsf{H}}$ of all finite semigroups whose subgroups belong to H is a pseudovariety. To obtain a basis of pseudoidentities for $\overline{\mathsf{H}}$ from a given basis for H simply transform each pseudoidentity $u(x_1, \ldots, x_n) = w(x_1, \ldots, x_n)$ into $u(v_1, \ldots, v_n) = w(v_1, \ldots, v_n)$ where $(v_1, \ldots, v_n)$ is a group-generic n-ary implicit operator. As an example, if Ab is the pseudovariety of all finite Abelian groups and $(v_1, v_2) = (xyx, x)^\omega$, then $\overline{\mathsf{Ab}} = [\![v_1v_2 = v_2v_1]\!]$. An alternative approach for the construction of group-generic n-tuples of profinite words which involves idempotents from the minimal ideal of $\overline{\Omega}_n\mathsf{S}$ is presented in [7].

The iteration φ^ω of finite implicit operators $\varphi = (w_1, \ldots, w_n)$ is of special interest because the elements of $\overline{\Omega}_n\mathsf{S}$ with which we start are particularly simple and because similar iterations take place in other areas of Mathematics, from symbolic dynamics to the theory of computation. In the case of a finite, primitive, G-invertible, implicit operator, we have the following improvement of Theorem 7.

Theorem 8. *Let φ be a finite, primitive, n-ary, implicit operator and let J be the $\mathcal{J}$-class of $\overline{\Omega}_n\mathsf{S}$ containing the $\varphi^\omega(x_i)$ ($i = 1, \ldots, n$). If φ is G-invertible then there is at least one maximal subgroup H of $\overline{\Omega}_n\mathsf{S}$ contained in J which satisfies $H = \varphi^\omega(H)$. Moreover, H is a free profinite group on n generators of the form $\varphi^\omega(u)$ with $u \in \Omega_n\mathsf{S}$.*

For example, taking $\varphi = (xy, zx, yzx)$, with a little additional calculation one can show that the profinite words $\varphi^\omega(x), \varphi^{\omega+1}(x), \varphi^{\omega+2}(x)$ freely generate a maximal subgroup of $\overline{\Omega}_3\mathsf{S}$. We do not know if this subgroup is a retract of $\overline{\Omega}_3\mathsf{S}$ although we conjecture it is not.

In general one cannot expect the retract subgroups of $\overline{\Omega}_n\mathsf{S}$ isomorphic with $\overline{\Omega}_n\mathsf{G}$ to be maximal subgroups. Indeed, by [7, 8] one can find such subgroups in the minimal ideal and there one can show that maximal subgroups are not n-generated for $n > 1$.

To show more generally that, for $n > 1$, the minimal ideal of $\overline{\Omega}_n\mathsf{S}$ cannot be reached through iteration of finite n-ary implicit operators, we introduce some numerical parameters. We first consider the *factor complexity* of a profinite word $w \in \overline{\Omega}_n\mathsf{S}$ which is given by a function q_w that associates to a positive integer k the number of factors of w of length k. One can easily show that the limit

$$h(w) = \lim_{k\to\infty} \frac{1}{k} \log_n q_w(k)$$

exists for every infinite $w \in \overline{\Omega}_n\mathsf{S}$ with $n > 1$ and we call it the *entropy* of w. Note that $\mathcal{J}$-equivalent infinite elements of $\overline{\Omega}_n\mathsf{S}$ have the same complexity and entropy.

Theorem 9. [8] *Entropy does not increase by applying an implicit operation nor by iteration. More precisely:*

(a) *if $u \in \overline{\Omega}_m\mathsf{S}$ and $v_1, \ldots, v_m \in \overline{\Omega}_n\mathsf{S}$, then*

$$\begin{aligned} &h(u(v_1, \ldots, v_m)) \\ &\quad \leq \max\{h(u)\log_n m, h(v_1), ..., h(v_m)\}; \end{aligned}$$

(b) *if $w_1, \ldots, w_n \in \overline{\Omega}_n\mathsf{S}$ and $z_1, \ldots, z_n$ are the components of the iterate $(w_1, \ldots, w_n)^\omega$, then*

$$\max_{1\leq i\leq n} h(z_i) \leq \max_{1\leq i\leq n} h(w_i).$$

We say that a subset X of $\overline{\Omega}_n\mathsf{S}$ is *closed under iteration* if, whenever $w_1, \ldots, w_n \in X$, the components of $(w_1, \ldots, w_n)^\omega$ also belong to X.

Consider the minimal ideal I of $\overline{\Omega}_n\mathsf{S}$. It is a $\mathcal{J}$-class and every element of I admits every element of $\overline{\Omega}_n\mathsf{S}$ as a factor. Hence elements of I have entropy 1 and, conversely, one can show that every profinite word of entropy 1 belongs to I. We thus obtain the following corollary of Theorem 9 which in particular states that the minimal ideal is inaccessible by iteration for $n > 1$.

Corollary 1. [8] *For $n > 1$, the complement of the minimal ideal I of $\overline{\Omega}_n\mathsf{S}$ is closed under iteration and under the application of implicit operations $w \in \overline{\Omega}_m\mathsf{S}$ with $h(w) < \frac{1}{\log_n m}$.*

Symbolic dynamics

We proceed to relate more closely free profinite semigroups with symbolic dynamics. Consider the pseudovarieties defined by the following pseudoidentities:

$$\begin{aligned} \mathsf{K} &= [\![x^\omega y = x^\omega]\!] \\ \mathsf{D} &= [\![yx^\omega = x^\omega]\!] \\ \mathsf{LI} &= [\![x^\omega y x^\omega = x^\omega]\!] \end{aligned}$$

In words: K consists of all finite semigroups in which idempotents are left zeros; D is the left-right dual of K; LI consists of all *locally trivial* finite semigroups in which every submonoid is trivial and it is the smallest pseudovariety containing both K and D.

The free pro-K semigroup $\overline{\Omega}_n\mathsf{K}$ on n letters is the completion of $\Omega_n\mathsf{K} = \Omega_n\mathsf{S}$ with respect to the metric d defined by $d(u,v) = 2^{-p(u,v)}$ where $p(u,v)$ is the length of the longest common prefix of u and v. A sequence of words which is not eventually constant is a Cauchy sequence if and only if prefixes of any given length stabilize for sufficiently large indices and the limit is completely determined by these successive prefixes, or in other words it may be identified with a right infinite word $x_{i_0}x_{i_1}\ldots x_{i_r}\ldots$. Such infinite words are one of the objects studied in symbolic dynamics, precisely under the metric resulting from d. Multiplication in $\overline{\Omega}_n\mathsf{K}$ is by concatenation of words except that right infinite words are declared to be left zeros.

Dually, $\overline{\Omega}_n\mathsf{D}$ is a compactification of $\Omega_n\mathsf{D} = \Omega_n\mathsf{S}$ by adding all left infinite words $\ldots x_{i_r}\ldots x_{j_2}x_{j_1}$ and declaring words (finite or infinite) to be close if they have a long common suffix. As for $\overline{\Omega}_n\mathsf{LI}$, it embeds naturally in the product $\overline{\Omega}_n\mathsf{D} \times \overline{\Omega}_n\mathsf{K}$ as follows: add to $\Omega_n\mathsf{LI} = \Omega_n\mathsf{S}$ points at infinity consisting of pairs $(\ldots x_{j_2}x_{j_1}, x_{i_0}x_{i_1}\ldots)$ of a left infinite and a right infinite word, which may also be identified with a doubly infinite word $\ldots x_{j_2}x_{j_1}x_{i_0}x_{i_1}\ldots$ with a marked origin, that is a function $w \in X^{\mathbb{Z}}$ defined on the integers with values in $X = \{x_1, \ldots, x_n\}$. Two doubly infinite words with marked origins are close if they coincide in a large factor centered at the origin, which induces the product topology on $X^{\mathbb{Z}}$.

The *shift* transformation sending $w \in X^{\mathbb{Z}}$ to the function $\sigma(w) : n \mapsto w(n+1)$ corresponds to a letter conjugation $v \mapsto a^{-1}va$ in $\overline{\Omega}_n\mathsf{LI}$ where $a = w(0)$. The shift defines the natural action of the cyclic group $\mathbb{Z}$ on $X^{\mathbb{Z}}$. A *symbolic dynamical system* or *subshift*, is a closed subset $\mathcal{S}$ of $X^{\mathbb{Z}}$ which is stable under the group action. It is easy to see that a subshift $\mathcal{S}$ is completely determined by the language $L(\mathcal{S}) \subseteq \Omega_n\mathsf{S}$ of its finite factors and that the languages that arise in this way are precisely the subsets L of $\Omega_n\mathsf{S}$ which are *factorial*, that is they are closed under taking factors, and *extendable*, that is for any $w \in L$ there are $a, b \in X$ such that $aw, wb \in L$. A subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ is viewed as a topological dynamical system $(\mathcal{S}, \sigma|\mathcal{S})$.

A subshift whose factors are the factors of the powers of a finite word is said to be *periodic*. The subshift $\mathcal{S}$ is said to be *sofic* if the language $L = L(\mathcal{S})$ can be recognized by a homomorphism $\varphi : \Omega_n\mathsf{S} \to S$ into a finite semigroup S in the sense that $L = \varphi^{-1}\varphi(L)$. If, moreover, $S \in \mathsf{LI}$ then L is said to be *locally testable* and $\mathcal{S}$ is called a subshift *of finite type*. Equivalently, a subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ is of finite type if and only if there is a finite set W of words such that $L(\mathcal{S})$ consists of the finite words over X which do not admit any word from W as a factor. A subshift $\mathcal{S}$ is *irreducible* if, for all $u, v \in L(\mathcal{S})$, there exists $w \in \Omega_n\mathsf{S}$ such that $uwv \in L(\mathcal{S})$. A *minimal subshift* is a nonempty subshift which does not properly contain any other nonempty subshift. It is well known that a subshift is minimal if and only if its language consists of all finite factors of a uniformly recurrent doubly infinite word.

A major open problem in symbolic dynamics is whether conjugacy is decidable for sofic subshifts, or even just for subshifts of finite type. There is a coarser equivalence relation, the *eventual conjugacy* or *shift-equivalence*, for which complete invariants are given by dimension groups [24]. These are ordered Abelian groups which are effectively computable and so eventual conjugacy is decidable. To define eventual conjugacy, one considers first the power $\mathcal{S}^n$ of a subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ whose alphabet is the set X^n of all length n words over X. Elements of $\mathcal{S}$ are considered as words over X^n by scanning the successive factors of length n that compose them. The so-called *eventual conjugacy* of subshifts $\mathcal{S}$ and $\mathcal{T}$ means that their powers $\mathcal{S}^n$ and $\mathcal{T}^n$ are conjugate for all sufficiently large n. Eventual conjugacy is known to be strictly coarser than conjugacy even for irreducible subshifts of finite type [21, 22].

Given a subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$, we may consider the closure $\overline{L(\mathcal{S})}$ of its language of finite factors in $\overline{\Omega}_n\mathsf{S}$. The set $\overline{L(\mathcal{S})}$ completely determines $\mathcal{S}$ since the language of its finite factors is precisely $L(\mathcal{S})$. This suggests doing symbolic dynamics in $\overline{\Omega}_n\mathsf{S}$, an object that has a much richer structure than $X^{\mathbb{Z}}$. The question that immediately comes to mind is what transformation of $\overline{\Omega}_n\mathsf{S}$ should we consider. The shift transformation corresponds to the conjugation $\chi : w \mapsto a^{-1}wa$, where a is the first letter of w, which means sending $w = av$ to va. However, a finite iterate of this transformation conjugates by a finite factor and coinciding in finite factors corresponds to the completion $\overline{\Omega}_n\mathsf{LI}$ of the free semigroup $\Omega_n\mathsf{S}$ rather than the much richer structure $\overline{\Omega}_n\mathsf{S}$ which really interests us here. We do not know of any single transformation which plays for $\overline{\Omega}_n\mathsf{S}$ the role the shift plays in the case of $\overline{\Omega}_n\mathsf{LI}$. Our connection between $\overline{\Omega}_n\mathsf{S}$ and subshifts proceeds in a different direction.

By Zorn's Lemma and compactness, the closed set $\overline{L(\mathcal{S})}$ must contain elements which are $\mathcal{J}$-equivalent to all other elements of $\overline{L(\mathcal{S})}$ of which they are factors. This suggests studying the $\mathcal{J}$-classes of such elements,

which we will call the *minimal $\mathcal{J}$-classes* of $\mathcal{S}$. The following results provide the basis for this study.

Proposition 4. *Let $\mathcal{S} \subseteq X^{\mathbb{Z}}$ be a subshift and let w be a regular element of $\overline{\Omega}_n\mathsf{S}$. Then the following conditions are equivalent:*

(a) *$w \in \overline{L(\mathcal{S})}$;*
(b) *w is $\mathcal{J}$-equivalent to some element of $\overline{L(\mathcal{S})}$;*
(c) *all finite factors of w belong to $L(\mathcal{S})$.*

Theorem 10. *Let $\mathcal{S} \subseteq X^{\mathbb{Z}}$ be a subshift.*

(a) *If $\mathcal{S}$ is sofic, then there are only finitely minimal $\mathcal{J}$-classes of $\mathcal{S}$ and $\overline{L(\mathcal{S})}$ is a union of $\mathcal{J}$-classes.*
(b) *The subshift $\mathcal{S}$ is irreducible if and only if $\mathcal{S}$ has only one minimal $\mathcal{J}$-class and it is regular. The regular $\mathcal{J}$-classes that appear in this way are those that contain profinite words which are limits of sequences of finite factors.*
(c) *The subshift $\mathcal{S}$ is minimal if and only if $\mathcal{S}$ has only one minimal $\mathcal{J}$-class J and J contains all its regular factors. The $\mathcal{J}$-classes that appear in this way are those that contain uniformly recurrent profinite words or, equivalently the $\mathcal{J}$-classes which contain infinite profinite words and all their regular factors.*

In terms of the factor ($\mathcal{J}$-)ordering, minimal subshifts are thus in bijective correspondence with $\mathcal{J}$-maximal regular $\mathcal{J}$-classes. One might expect such $\mathcal{J}$-classes to have low entropy since they are far from the minimal ideal, provided the alphabet has more than one letter. However, it has been recently shown that there are uniformly recurrent doubly infinite words with arbitrarily large entropy $h < 1$ [14].

Corollary 2. *For $n \geq 2$, there are $\mathcal{J}$-maximal regular $\mathcal{J}$-classes in $\overline{\Omega}_n\mathsf{S}$ of arbitrarily large entropy $h < 1$.*

At the other end, we already know that there are $\mathcal{J}$-maximal regular $\mathcal{J}$-classes of $\overline{\Omega}_n\mathsf{S}$ with zero entropy, such as the $\mathcal{J}$-class containing the $\varphi^\omega(x_i)$ for any finite primitive continuous endomorphism φ of $\overline{\Omega}_n\mathsf{S}$.

The study of sofic subshifts and of minimal subshifts correspond to major subareas of symbolic dynamics. In general, the dynamics of a sofic subshift is determined by that of certain irreducible sofic subshifts associated with it. Since minimal subshifts are irreducible (but not sofic, unless they are periodic), irreducibility is usually assumed and it is therefore not a serious restriction, which we will assume from hereon.

In semigroup theory, when a semigroup has a nontrivial minimal ideal, a lot of its structural properties are reflected in the minimal ideal and in the action of the semigroup on this ideal. Although $\overline{L(\mathcal{S})}$ is not in general a subsemigroup of $\overline{\Omega}_n\mathsf{S}$, it does have a minimal $\mathcal{J}$-class J, which is regular, and so one may view it as a partial semigroup, for which J plays the role of the minimal ideal. One way to formalize this idea is to consider a profinite category associated with $\mathcal{S}$ as follows.

By the transition graph $\Gamma(\mathcal{S})$ of a subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ we mean the (directed) graph with vertex set $\mathcal{S}$ and an edge $v \to \sigma(v)$ for each vertex v. As a purely combinatorial graph, this is a rather uninteresting graph in which every vertex has in-degree and out-degree 1 and, for instance, all (nonempty) subshifts without periodic points over finite alphabets have isomorphic graphs. But both the sets of vertices $\mathcal{S}$ and edges $\{(v, \sigma(v)) : v \in \mathcal{S}\} \subseteq \mathcal{S} \times \mathcal{S}$ have a topological structure induced from $X^{\mathbb{Z}}$ and the partial operations of taking the beginning and end vertices of an edge are continuous.

This suggests coming back to the general framework of structures of first-order languages at the beginning of the paper. However, the treatment of partial operations, which has important applications for instance in computer science, is much more delicate and apparently has only be done in special cases in the sense of obtaining Birkhoff/Reiterman-type theorems characterizing certain classes of structures by means of equations [12]. One of the difficulties lies in the definition of a suitable notion of substructure and homomorphic image. For (small) categories, this has been done by Tilson [33] with the profinite approach added in [20, 9].

For our present purposes we do not need Birkhoff/Reiterman-type theorems, but rather just free profinite constructions. This does carry through from the discussion in earlier sections of this paper with a few minor adjustments. For substructures we take subsets such that whenever an operation is defined on elements of the subset then the resulting value is also in the subset. For a homomorphism, whenever an operation is defined on elements of the domain, the corresponding operation should also be defined on their images and the usual relation (1) should hold. We assume further that there are unary relations in the language which are interpreted in structures so as to form partitions of their universes (into *sorts* in the language of computer science) and so that all operations take their arguments in one sort and all their values are also of a single sort. Note that this is a nontrivial restriction. It allows us to define products of structures as subsets of the Cartesian product consisting of elements in which all components have the same sort, and then define operations and relations componentwise. Profinite structures are defined as in the case of fully-defined operations and free profinite structures may be constructed by taking projective limits, which in turn are realized as appropriate substructures of products of finite structures.

In our case, we may view (small) categories as structures of a suitable first-order language, namely the language with unary relation symbols V and E, unary operation symbols α, ω and I, and binary operation symbol π. Their interpretation in a category C is the following: V is the set (sort) of vertices (or objects); E is the set (sort) of edges (or morphisms); α is the partial operation defined on edges where $\alpha(e)$ is the vertex where the edge starts; ω is the partial operation defined on edges where $\omega(e)$ is the vertex where the edge ends; I is the partial operation defined on vertices where $I(v)$ is the identity at v; π is the partial

associative operation defined on edges e, f such that $\omega(e) = \alpha(f)$ and the edge $\pi(e, f)$ starts at $\alpha(e)$ and ends at $\omega(f)$.

Graphs may be viewed as structures of the reduced language in which the symbols I and π are dropped. *Semigroupoids* are structures of the language with the symbol I dropped. The general framework gives us the right notions of graph homomorphism, category homomorphism (or functor), topological graph, profinite category, and so on.

Back to subshifts, with the above topology, not only $\Gamma(\mathcal{S})$ is a topological graph but, more precisely, we have the following expected result.

Proposition 5. *The graph $\Gamma(\mathcal{S})$ is profinite.*

Recall that a homomorphism (or functor) $\varphi : C \to D$ between two categories is *faithful* if its restriction to every set of edges of C with fixed beginning and end is injective. We say that a graph is *strongly connected* if, for all vertices v and w, there is an edge $v \to w$. *Groupoids* are strongly connected categories in which all morphisms are isomorphisms.

Note that the class Cat of all finite categories is a pseudovariety. The free structure $\Omega_\Gamma\mathsf{Cat}$ on a graph Γ is then the free category on Γ, whose edges are the finite paths in Γ. In case Γ is a profinite graph, $\overline{\Omega}_\Gamma\mathsf{Cat}$ may be constructed as in an earlier section as the completion of $\Omega_\Gamma\mathsf{Cat}$ with respect to a suitable metric. We call the edges of $\overline{\Omega}_\Gamma\mathsf{Cat}$ *profinite edges* and we say they are *infinite* if they do not lie in $\Omega_\Gamma\mathsf{Cat}$.

Note that from the free profinite category $\overline{\Omega}_{\Gamma(\mathcal{S})}\mathsf{Cat}$ one can reconstruct the subshift $\mathcal{S}$ as a topological dynamical system: the space $\mathcal{S}$ is the closed subspace V of vertices and the shift transformation $v \to \sigma(v)$ is characterized by the edges which are not local identities and which cannot be factorized nontrivially. In particular, two subshifts are conjugate if and only if their associated profinite graphs (respectively categories) are isomorphic.

A subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ further determines a labeling of its associated profinite graph $\Gamma(\mathcal{S})$: label the edge $v \to \sigma(v)$ with the letter $v(0)$ across which the shift moves the origin of the doubly infinite word v. This labeling extends uniquely to a continuous homomorphism $\lambda : \overline{\Omega}_{\Gamma(\mathcal{S})}\mathsf{Cat} \to \overline{\Omega}_X\mathsf{M}$ to the free profinite monoid on X, which is obtained from $\overline{\Omega}_X\mathsf{S}$ by adding an identity as an isolated point, where monoids are seen as one (virtual) vertex categories.

Proposition 6. *The mapping λ is faithful.*

We thus have another strong, "geometrical", connection between subshifts and free profinite semigroups. The next result summarizes some relationships between the profinite constructions associated with a subshift.

Theorem 11. *Let $\mathcal{S} \subseteq X^{\mathbb{Z}}$ be a subshift.*

(a) *The subshift $\mathcal{S}$ is irreducible if and only if the category $\overline{\Omega}_{\Gamma(\mathcal{S})}\mathsf{Cat}$ is strongly connected. In this case, the labeling λ embeds the minimal ideal of each local monoid of $\overline{\Omega}_{\Gamma(\mathcal{S})}\mathsf{Cat}$ in the minimal $\mathcal{J}$-class of $\mathcal{S}$ as a union of maximal subgroups of $\overline{\Omega}_n\mathsf{S}$.*

(b) *The subshift $\mathcal{S}$ is minimal if and only if the category $\overline{\Omega}_{\Gamma(\mathcal{S})}\mathsf{Cat}$ is strongly connected and its subsemigroupoid whose edges are the infinite profinite paths of $\Gamma(\mathcal{S})$ is a groupoid.*

In particular, for an irreducible subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$, the maximal subgroups of the minimal ideals of local monoids of the profinite category $\overline{\Omega}_{\Gamma(\mathcal{S})}\mathsf{Cat}$ are mutually isomorphic and they are isomorphic to the maximal subgroups of the minimal $\mathcal{J}$-class of $\mathcal{S}$. This gives a geometrical meaning to the groups computed in the preceding section. We also obtain the following result. For shortness, let us denote $G(\mathcal{S})$ any of the maximal subgroups of the minimal $\mathcal{J}$-class of an irreducible subshift $\mathcal{S}$.

Corollary 3. *The group $G(\mathcal{S})$ is a conjugacy invariant of $\mathcal{S}$.*

A subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ is said to be *generated* by a finite primitive endomorphism φ of $\overline{\Omega}_n\mathsf{S}$ if $L(\mathcal{S})$ is the set of factors of the words of the form $\varphi^n(x_i)$ or, equivalently, the finite factors of the profinite words $\varphi^\omega(x_i)$. Since for such φ, $\varphi^\omega(x_i)$ is uniformly recurrent, we do always generate a subshift in this way. The subshifts thus obtained are also called *substitution subshifts*.

As a consequence of Theorem 8 we should note that $G(\mathcal{S})$ is a very rough conjugacy invariant. However, it is easy to see that the action of the alphabet on the minimal $\mathcal{J}$-class of an irreducible subshift $\mathcal{S}$ is sufficient to allow us to recover $\mathcal{S}$. Hence, one should be able to extract from this action enough information to characterize the conjugacy class of $\mathcal{S}$. At present it remains an open problem how to do it and whether that may lead to a solution of the conjugacy problem for subshifts of finite type or even for sofic subshifts.

We end this section with a partial extension of Theorem 8 to non-substitution subshifts. A subshift $\mathcal{S}$ is said to be *Sturmian* if $L(\mathcal{S})$ has exactly $n+1$ elements of length n for every $n \geq 1$. It is well known that this is the minimum possible value for a non-periodic subshift and that Sturmian subshifts are minimal [19]. Taking $n = 1$, we see that a Sturmian subshift involves only two letters and so it may be considered as a subshift over a two-letter alphabet.

The following result has also been announced in [5].

Theorem 12. *Let $\mathcal{S}$ be a Sturmian subshift. Then the group $G(\mathcal{S})$ is a free profinite group on two generators.*

For example, the continuous endomorphism of $\overline{\Omega}_2\mathsf{S}$ defined by $\varphi = (xy, x)$ generates the so-called *Fibonacci subshift*, which has many remarkable properties [25]. The name is justified since the number of occurrences of y in $\varphi^n(x)$ is the nth term of the Fibonacci sequence $1, 1, 2, 3, 5, 8, 13, \ldots$ The associated group is a free profinite group on two generators by Theorem 12.

Sturmian substitution subshifts have been characterized as those subshifts on two-letter alphabets which are generated by finite primitive G-invertible continuous endomorphisms of $\overline{\Omega}_2\mathsf{S}$ [25, Chapter 2]. Hence

Theorem 12 is indeed an extension of Theorem 8 for two-letter alphabets. The following partial extension to larger alphabets has also been announced in [5].

We say that a word w is *right special* for a subshift $\mathcal{S}$, if there are at least two letters a, b such that $wa, wb \in L(\mathcal{S})$. In this case, the number of such letters is called the *right-degree* of w. The left analogues of this notion are defined dually. A subshift $\mathcal{S} \subseteq X^{\mathbb{Z}}$ is said to be an *Arnoux-Rauzy subshift* if, for every positive integer n, there is exactly one right special word of length n, which is of right-degree $|X|$, and one left special word of length n, which is of left-degree $|X|$. One can easily show that an Arnoux-Rauzy subshift is minimal.

Theorem 13. *Let $\mathcal{S}$ be an Arnoux-Rauzy subshift over an alphabet with m letters. Then the group $G(\mathcal{S})$ is a free profinite group on m generators.*

Acknowledgments. This work was supported, in part, by *Fundação para a Ciência e a Tecnologia* (FCT) through the *Centro de Matemática da Universidade do Porto*, by the FCT project POCTI/32817/MAT/2000, which is partially funded by the European Community Fund FEDER, and by the INTAS grant #99-1224. The author is indebted to Alfredo Costa for his comments on a preliminary version of this paper.

References

[1] J. Almeida, *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1995. English translation.

[2] ————, *Dynamics of finite semigroups*, in Semigroups, Algorithms, Automata and Languages, G. M. S. Gomes, J.-E. Pin, and P. V. Silva, eds., Singapore, 2002, World Scientific, 269–292.

[3] ————, *Dynamics of implicit operations and tameness of pseudovarieties of groups*, Trans. Amer. Math. Soc. **354** (2002) 387–411.

[4] ————, *Finite semigroups: an introduction to a unified theory of pseudovarieties*, in Semigroups, Algorithms, Automata and Languages, G. M. S. Gomes, J.-E. Pin, and P. V. Silva, eds., Singapore, 2002, World Scientific, 3–64.

[5] ————, *Symbolic dynamics in free profinite semigroups*, Tech. Rep. CMUP 2003-05, Univ. Porto, 2003.

[6] J. Almeida and M. V. Volkov, *Profinite methods in finite semigroup theory*, in Proceedings of International Conference "Logic and applications" honoring Yu. L. Ershov on his 60-th birthday anniversary and of International Conference on mathematical logic, honoring A. I. Mal'tsev on his 90-th birthday anniversary and 275-th anniversary of the Russian Academy of Sciences, S. S. Goncharov, ed., Novosibirsk, Russia, 2002, 3–28.

[7] ————, *Profinite identities for finite semigroups whose subgroups belong to a given pseudovariety*, J. Algebra & Applications **2** (2003). To appear.

[8] ————, *Subword complexity of profinite words and subgroups of free profinite semigroups*, Tech. Rep. CMUP 2003-10, Univ. Porto, 2003.

[9] J. Almeida and P. Weil, *Profinite categories and semidirect products*, J. Pure Appl. Algebra **123** (1998) 1–50.

[10] M.-P. Béal, *Codage Symbolique*, Masson, Paris, 1993.

[11] R. Brandl, *Engel cycles in finite groups*, Arch. Math. (Basel) **41** (1983) 97–102.

[12] P. Burmeister, *Partial algebras – An introductory survey*, in Algebras and orders. Proceedings of the NATO Advanced Study Institute and Séminaire de mathématiques supérieures, Montréal, Canada, July 29 - August 9, 1991, I. Rosenberg and G. Sabidussi, eds., no. 389 in NATO ASI Ser., Ser. C, Math. Phys. Sci., Dordrecht, 1993, Kluwer Academic Publishers, 1–70.

[13] A. Costa, *Relações entre a dinâmica de operadores implícitos e a estrutura de grupos finitos*, Master's thesis, Univ. Porto, 2003.

[14] D. Damanik and B. Solomyak, *Some high-complexity Hamiltonians with purely singular continuous spectrum*, Ann. Henri Poincare **3** (2002) 99–105.

[15] S. Eilenberg, *Automata, Languages and Machines*, vol. B, Academic Press, New York, 1976.

[16] P. Flavell, *Finite groups in which every two elements generate a soluble group*, Invent. Math. **121** (1995) 279–285.

[17] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer, Berlin, 1986.

[18] F. Grunewald, B. Kuniavskii, D. Nikolova, and E. Plotkin, *Two-variable identities in groups and Lie algebras*, Zapiski Nauch. Seminarov POMI **272** (2000) 161–176. To appear also in J. Math. Sciences.

[19] G. A. Hedlund and M. Morse, *Symbolic dynamics II. Sturmian trajectories*, Amer. J. Math. **62** (1940) 1–42.

[20] P. R. Jones, *Profinite categories, implicit operations and pseudovarieties of categories*, J. Pure Appl. Algebra **109** (1996) 61–95.

[21] K. H. Kim and F. W. Roush, *The Williams conjecture is false for irreducible subshifts*, Ann. of Math. (2) **149** (1999) 545–558.

[22] K. H. Kim, F. W. Roush, and J. Wagoner, *The shift equivalence problem*, Math. Intelligencer **21** (1999) 18–29.

[23] G. Lallement, *Semigroups and Combinatorial Applications*, Wiley, New York, 1979.

[24] D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, Cambridge, 1996.

[25] M. Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press, Cambridge, UK, 2002.

[26] V. A. Molchanov, *Nonstandard characterization of pseudovarieties*, Algebra Universalis **33** (1995) 533–547.

[27] J.-E. Pin and P. Weil, *A Reiterman theorem for pseudovarieties of finite first-order structures*, Algebra Universalis **35** (1996) 577–595.

[28] J. Reiterman, *The Birkhoff theorem for finite algebras*, Algebra Universalis **14** (1982) 1–10.

[29] L. Ribes and P. A. Zalesskiĭ, *Profinite Groups*, no. 40 in Ergeb. Math. Grenzgebiete 3, Springer, Berlin, 2000.

[30] H. Straubing, *Finite automata, formal logic and circuit complexity*, Birkhäuser, Basel, 1994.

[31] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.1*, Aachen, St Andrews, 1999. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[32] J. G. Thompson, *Non-solvable groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968) 383–437.

[33] B. Tilson, *Categories as algebra: an essential ingredient in the theory of monoids*, J. Pure Appl. Algebra **48** (1987) 83–198.

[34] A. I. Širšov, *On certain near-Engel groups*, Algebra i Logika **2** (1963) 5–18.

[35] P. Weil, *Profinite methods in semigroup theory*, Int. J. Algebra Comput. **12** (2002) 137–178.

[36] S. Wolfram, *Mathematica: a system for doing Mathematics by computer*, Addison-Wesley, Reading, Mass., second ed., 1991.

[37] M. Zorn, *Nilpotency of finite groups (abstract)*, Bull. Amer. Math. Soc. **42** (1936) 485–486.