Irreducibility of certain pseudovarieties[1]

S. Margolis
Department of Mathematics and Computer Science
Bar Ilan University
52900 Ramat Gan – Israel
margolis@bimacs.cs.biu.ac.il

M. Sapir
Department of Mathematics and Statistics
Center for Communic. and Inform. Science
University of Nebraska-Lincoln
Lincoln, NE 68588 – USA
mvs@unlinfo.unl.edu

P. Weil
LIAFA
Université Paris-VI et CNRS
4 place Jussieu
75252 Paris Cedex 05 – France
Pascal.Weil@litp.ibp.fr

Abstract

We prove that the pseudovarieties of all finite semigroups, and of all aperiodic finite semigroups are irreducible for join, for semidirect product and for Mal'cev product. In particular, these pseudovarieties do not admit maximal proper subpseudovarieties. More generally, analogous results are proved for the pseudovariety of all finite semigroups all of whose subgroups are in a fixed pseudovariety of groups **H**, provided that **H** is closed under semidirect product.

Résumé

Nous prouvons que la pseudovariété de tous les semigroupes finis, et celle de tous les semigroupes apériodiques finis sont irréductibles pour le sup, pour le produit semidirect et pour le produit de Mal'cev. En particulier, ces pseudovariétés n'admettent pas de sous-pseudovariété maximale propre. Des résultats analogues sont établis plus généralement pour la pseudovariété de tous les semigroupes finis dont les sous-groupes sont dans une pseudovariété de groupes fixée **H**, pourvu que **H** soit fermée par produit semidirect.

[1]The two first authors were partially supported by NSF Grant DMS920381. Part of this work was done while the second author was an invited Professor at the Université Paris-VI. All three authors were partially supported by the Center for Communication and Information Science of the University of Nebraska.

Within the context of the general study of the structure of the lattice of pseudovarieties of finite semigroups, the question of describing the irreducible pseudovarieties is both a natural and an old problem. For instance, only a handful of the "classical" pseudovarieties are known to be join-irreducible or join-reducible (see [1, chap. 9]). In particular, the pseudovariety of nilpotent semigroups is join-irreducible, whereas $\mathbf{J}$, the pseudovariety of $\mathcal{J}$-trivial semigroups, is join-*reducible* (Almeida [2]).

In this paper, we show that if $\mathbf{H}$ is a pseudovariety of groups closed under semidirect product, then the pseudovariety of all semigroups all of whose subgroups are in $\mathbf{H}$ is irreducible for join, for semidirect product and for Mal'cev product. The particular cases where $\mathbf{H}$ is the pseudovariety of all groups, and where $\mathbf{H}$ is trivial yield the irreducibility of $\mathbf{S}$, the pseudovariety of all finite semigroups, and of $\mathbf{A}$, the pseudovariety of aperiodic semigroups. As a consequence, it follows that these pseudovarieties do not contain maximal proper subpseudovarieties, a fact which generalizes a result of Margolis [11].

If we consider the analogous problem for $\mathcal{S}$ and $\mathcal{G}$, respectively the variety of all semigroups and the variety of all groups, it is known that $\mathcal{S}$ is join irreducible (Evans [6]) but that $\mathcal{S} = \mathcal{C}om \circledm \mathcal{C}om = \mathcal{C}om * \mathcal{C}om$ where $\mathcal{C}om$ is the variety of all commutative semigroups: the first equality is immediate when one considers the projection from the free semigroup onto the free commutative semigroup; the second one follows from a result of Mal'cev stating that the free semigroup on 2 generators is embedded in the free metabelian group [10]. It is also known that $\mathcal{G}$ is irreducible for join, semidirect product and Mal'cev product [12].

The proof of the join irreducibility of $\mathcal{S}$ is based on the manipulation of identities, and cannot be used directly for pseudovarieties. However, it is known that each subpseudovariety of a pseudovariety $\mathbf{V}$ is defined by a set of formal equalities between elements of certain relatively free profinite structures (Reiterman's theorem, see [1, 17, 20]). We call these formal equalities *pro-$\mathbf{V}$-identities*. They are also called pseudoidentities [1]. Formal definitions are given in Section 1.1.

In order to prove that a pseudovariety $\mathbf{V}$ is join (resp. semidirectly, Mal'cev) irreducible, we use an idea inspired by Evans's proof. It is enough to prove the following:

> From every pair of pro-$\mathbf{V}$-identities $u_1 = v_1$ and $u_2 = v_2$ which are non trivial, i.e. which define proper subpseudovarieties $\mathbf{V}_1$ and $\mathbf{V}_2$ of $\mathbf{V}$, we can construct a non trivial pro-$\mathbf{V}$-identity which holds in $\mathbf{V}_1 \vee \mathbf{V}_2$ (resp. $\mathbf{V}_1 * \mathbf{V}_2$, $\mathbf{V}_1 \circledm \mathbf{V}_2$).

This is done in several steps, each of which consists in constructing non trivial consequences of $u_1 = v_1$ and $u_2 = v_2$ with some special properties. These consequences are obtained by encoding $u_1 = v_1$ and $u_2 = v_2$. That is, we substitute given values for the variables of the given pro-$\mathbf{V}$-identities in such a way that the resulting pro-$\mathbf{V}$-identities are again non trivial. The main result is proved in Section 3.

1 Preliminaries

Here we review some elementary definitions on pseudovarieties, profinite semigroups and pro-identities. We also remind the reader of the definition of unambiguous relation semigroups and of the unambiguous product of semigroups (Sakarovitch [22]). This product will appear in the proof of several of our intermediary results.

1.1 Pro-identities and pseudovarieties

A class $\mathbf{V}$ of finite semigroups is called a *pseudovariety* if it is closed under taking subsemigroups, homomorphic images and finite direct products. The *trivial* pseudovariety consists only of one-element semigroups. For classical results concerning semigroups and pseudovarieties, and in particular for the definitions of the semidirect product $S * T$ and the wreath product $S \circ T$ of semigroups, and of the product $\mathbf{V} * \mathbf{W}$ of pseudovarieties, the reader is referred to [5, 14, 1].

If $\mathbf{V}$ and $\mathbf{W}$ are pseudovarieties, the *Mal'cev product* $\mathbf{V} \textcircled{m} \mathbf{W}$ is the pseudovariety generated by the semigroups S such that there exists a morphism $\pi: S \to T$, with $T \in \mathbf{W}$ and $e\pi^{-1} \in \mathbf{V}$ for each idempotent e of T.

If S is a semigroup, we let S^1 be the monoid equal to S, if S has an identity, and to $S \cup \{1\}$ otherwise. Following Eilenberg, we say that a pseudovariety of semigroups is *monoidal* if it is generated by monoids, or equivalently, if $S^1 \in \mathbf{V}$ for each $S \in \mathbf{V}$ [5, Prop. V.1.2].

If $\mathbf{V}$ is a pseudovariety of semigroups, a semigroup is said to be *pro*-$\mathbf{V}$ if it is a projective limit of semigroups of $\mathbf{V}$. A topological semigroup is pro-$\mathbf{V}$ if and only if it is compact, 0-dimensional and all its finite continuous homomorphic images are in $\mathbf{V}$ [13]. Let A be a finite set, or *alphabet.* We denote by A^+ the free semigroup on A and by $\hat{F}_A(\mathbf{V})$ the projective limit of the A-generated elements of $\mathbf{V}$. The main properties of these semigroups for our purposes are summarized in the next proposition [1, 3]. They will be used freely in the sequel.

Proposition 1.1 *Let A be an alphabet and let $\mathbf{V}$ be a non trivial pseudovariety.*

- *There exists a natural injective mapping $\iota: A \to \hat{F}_A(\mathbf{V})$ such that $A\iota$ generates a dense subsemigroup of $\hat{F}_A(\mathbf{V})$.*
- *$\hat{F}_A(\mathbf{V})$ is the free pro-$\mathbf{V}$ semigroup over A: if σ is a mapping from A into a pro-$\mathbf{V}$ semigroup S, then σ admits a unique continuous extension $\hat{\sigma}: \hat{F}_A(\mathbf{V}) \to S$ such that $\sigma = \iota\hat{\sigma}$.*
- *A finite semigroup is in $\mathbf{V}$ if and only if it is a continuous homomorphic image of $\hat{F}_A(\mathbf{V})$ for some alphabet A.*

Whenever convenient, the mapping $\iota: A \to \hat{F}_A(\mathbf{V})$ is ignored, and A is considered as a subset of $\hat{F}_A(\mathbf{V})$.

Observe that, if $\mathbf{W}$ is a subpseudovariety of $\mathbf{V}$, then every pro-$\mathbf{W}$ semigroup is also pro-$\mathbf{V}$. In particular, the identity on A induces a continuous onto morphism $\pi: \hat{F}_A(\mathbf{V}) \to \hat{F}_A(\mathbf{W})$, called the *natural projection* of $\hat{F}_A(\mathbf{V})$ onto $\hat{F}_A(\mathbf{W})$.

Let us fix some notation. For each alphabet A and for each $x \in \hat{F}_A(\mathbf{V})$, the sequence $(x^{n!})_n$ converges in $\hat{F}_A(\mathbf{V})$, and we denote by x^ω its limit: x^ω is the only idempotent in the topological closure of the subsemigroup generated by x [1]. Let A be a n-letter alphabet, $A = \{a_1, \ldots, a_n\}$, let B be an alphabet, and let $x_1, \ldots, x_n \in \hat{F}_B(\mathbf{V})$. If $u \in \hat{F}_A(\mathbf{V})$, we denote by $u(x_1, \ldots, x_n)$ the image of u under the continuous morphism $\varphi: \hat{F}_A(\mathbf{V}) \to \hat{F}_B(\mathbf{V})$ defined by letting $a_i\varphi = x_i$ for $1 \leq i \leq n$.

A *pro-$\mathbf{V}$-identity on the set of variables A* (or *in $|A|$ variables*) is a pair (u, v) of elements of $\hat{F}_A(\mathbf{V})$. It is usually denoted $u = v$. It is said to be non trivial if the elements u and v are distinct. We say that $u = v$ is an *identity*, or *word identity*, if u and v are words, i.e. finite products of elements of A, or elements of $A^+\iota$. If the pseudovariety $\mathbf{V}$ is understood, we also say *pro-identity* for pro-$\mathbf{V}$-identity.

A semigroup $S \in \mathbf{V}$ *satisfies* the pro-$\mathbf{V}$-identity $u = v$ if, for any continuous morphism $\sigma: \hat{F}_A(\mathbf{V}) \to S$, one has $u\sigma = v\sigma$. Let Σ be a set of pro-$\mathbf{V}$-identities. A subclass $\mathbf{W}$ of $\mathbf{V}$ *satisfies* Σ if each element of $\mathbf{W}$ satisfies each element of Σ. It is *defined by* Σ if it consists of all the elements of $\mathbf{V}$ which satisfy Σ. Reiterman proved the following fundamental theorem [20].

Theorem 1.2 *Let $\mathbf{V}$ be a pseudovariety and let $\mathbf{W}$ be a subclass of $\mathbf{V}$. Then $\mathbf{W}$ is a pseudovariety if and only if it is defined by a set of pro-$\mathbf{V}$-identities. In particular, every proper subpseudovariety of $\mathbf{V}$ satisfies some non trivial pro-$\mathbf{V}$-identity.*

1.2 Unambiguous and wreath products

A *semigroup of relations* is a pair (Q, R) where Q is a finite set and R is a semigroup of $Q \times Q$ Boolean matrices. Let $\mathcal{A}$ be a (possibly non deterministic) automaton over the alphabet A with state set Q and let u be a word in A^+. The transition labeled by u, denoted $u\rho$, is the $Q \times Q$ Boolean matrix whose (p, q)-entry is 1 if there is a path labeled u in $\mathcal{A}$, and 0 otherwise ($p, q \in Q$). The set $A^+\rho$ is a subsemigroup of the set of all $Q \times Q$ Boolean matrices, and $(Q, A^+\rho)$ is called the *transition semigroup* of $\mathcal{A}$. In addition, ρ is a morphism, called the *transition morphism* of $\mathcal{A}$.

A semigroup of relations (Q, R) is said to be *unambiguous* if, for any elements $s, t \in R$ and for any pair (p, q) corresponding to a non-zero entry in st, there exists a unique element $r \in Q$ such that the entries (p, r) of s and (r, q) of t are non zero. The notion of unambiguous relation semigroup is closely associated with that of a *code*, that is, of a free set of generators of a free subsemigroup of the free semigroup. More precisely, let $\mathcal{A}$ be a finite automaton with one initial-terminal vertex 1, and such that each state is visited along some successful path (*trim* automaton). Let us also assume that each word labeling a path from 1 to 1 and not visiting 1 as an internal state of that path, labels exactly one such path. Let C be the set of those words. Then $\mathcal{A}$ recognizes C^+. Moreover the transition semigroup of $\mathcal{A}$ is unambiguous if and only if C is a code [4, Thm IV.2.1].

If (Q, R) is an unambiguous relation semigroup, we can define, for each semigroup S, a semigroup $S \circledast (Q, R)$ by considering the set of all $Q \times Q$ matrices with entries in $S \cup \{0\}$ (with 0 a new zero) obtained from the matrices in R by replacing the non zero entries by arbitrary elements of S. The usual matrix multiplication makes $S \circledast (Q, R)$ into a semigroup, called the *unambiguous product* of S and (Q, R). Note that, in the particular case where (Q, R) is a semigroup of partial functions, $S \circledast (Q, R)$ coincides with the wreath product as it is defined by Eilenberg [5] (see [22]), and $S \circledast (Q, R)$ is a semidirect product of the form $S^k * R$ for some integer k [5, Cor. V.4.3]. Here S^k is the direct product of k copies of S.

If $\mathbf{V}$ and $\mathbf{W}$ are pseudovarieties, we let $\mathbf{V} \circledast \mathbf{W}$ be the pseudovariety generated by the semigroups of the form $V \circledast (Q, W)$ where $V \in \mathbf{V}$ and (Q, W) is a semigroup of unambiguous relations with $W \in \mathbf{W}$.

Let us also note the following result [24, Prop. 3.4].

Lemma 1.3 *Let S be a finite semigroup and let (Q, R) be a semigroup of unambiguous relations, with Q finite. Then every group G in $S \circledast (Q, R)$ admits a normal subgroup K dividing a finite direct product of copies of S, such that G/K divides R.*

1.3 Pseudovarieties of the form $\overline{\mathbf{H}}$

If $\mathbf{H}$ is a pseudovariety of groups, we denote by $\overline{\mathbf{H}}$ the pseudovariety of all semigroups, all of whose subgroups are in $\mathbf{H}$.

It is clear that $\overline{\mathbf{H}}$ is monoidal, and that it contains $\mathbf{A}$, the pseudovariety of aperiodic semigroups. In fact, $\mathbf{A} = \overline{\mathbf{I}}$, where $\mathbf{I}$ is the trivial pseudovariety. Moreover, Lemma 1.3 shows that $\overline{\mathbf{H}} = \overline{\mathbf{H}} \circledast \mathbf{A}$. In addition, if $\mathbf{H}$ is closed under semidirect product, then $\overline{\mathbf{H}}$ is closed under semidirect product, and $\overline{\mathbf{H}} = \overline{\mathbf{H}} \circledast \overline{\mathbf{H}}$.

2 Pro-V codes

Let A and B be alphabets, and for each $a \in A$, let $k_a \in \hat{F}_B(\mathbf{V})$. By Theorem 1.1, there is a unique continuous morphism $\kappa\colon \hat{F}_A(\mathbf{V}) \to \hat{F}_B(\mathbf{V})$ such that $a\kappa = k_a$ for each $a \in A$. It is easy to verify that if a semigroup $S \in \mathbf{V}$ satisfies a pro-$\mathbf{V}$-identity $u = v$ with $u, v \in \hat{F}_A(\mathbf{V})$, then it satisfies the pro-$\mathbf{V}$-identity $u\kappa = v\kappa$.

In analogy with the terminology concerning the free semigroup (see [4]), we say that the morphism κ is a *pro-$\mathbf{V}$ coding morphism* if it is one-to-one. In this case, we call $A\kappa$ a *pro-$\mathbf{V}$ code*. This means exactly that the κ-image of a non trivial pro-$\mathbf{V}$-identity is also non trivial.

2.1 Word codes and pro-V codes

Let A and B be alphabets, and let $\kappa\colon A^+ \to B^+$ be an injective morphism. The morphism κ admits a unique continuous extension to a morphism from $\hat{F}_A(\mathbf{V})$ into $\hat{F}_B(\mathbf{V})$, also denoted by κ. Moreover, the set $C = A\kappa$ is a (word) code, that is C freely generates a free subsemigroup of B^+ (namely C^+). If the syntactic semigroup of C^+ belongs to a pseudovariety $\mathbf{V}$, we say that C is a $\mathbf{V}$*-code*.

In this section, we find a sufficient condition for a word code to be a pro-$\mathbf{V}$ code as well.

Let P be the set of proper prefixes of the words of C, that is,

$$P = \{w \in B^* \mid wx \in C \text{ for some } x \in B^+\}.$$

In particular, $1 \in P$. The *sagittal automaton* of C is the automaton with state set P, initial and terminal state 1, and with transitions defined, for each letter $b \in B$, as follows: there is a b-labeled arrow from p to q ($p, q \in P$) if, either $q = pb$, or $q = 1$ and $pb \in C$. (The sagittal automaton is called the literal automaton of C^* in [4, p. 98].) The transition semigroup of this automaton, denoted $Sag(C)$, is called the *sagittal semigroup* of C. Since C is a code, the sagittal automaton of C is unambiguous, and $(P, Sag(C))$ is a semigroup of unambiguous relations.

In the particular case where C is a prefix code, that is, no word of C is a proper prefix of another word of C, it is easily verified that the sagittal automaton of C is deterministic, so that the relation semigroup $(P, Sag(C))$ is a transformation semigroup.

The sagittal semigroup of C is close to the syntactic semigroup of C^+. In fact, if the syntactic semigroup of C^+ lies in a pseudovariety $\mathbf{V}$, then $Sag(C) \in L\mathbf{I} \circledcirc \mathbf{V}$ where $L\mathbf{I}$ is the pseudovariety of all semigroups S such that $eSe = e$ for each idempotent e of S [9].

By adapting the proof of [16, Prop. 4.3], we get the following encoding result.

Proposition 2.1 *Let A and B be alphabets, let $\kappa: A^+ \to B^+$ be an injective morphism and let $(P, Sag(C))$ be the sagittal relation semigroup of the code $C = A\kappa$. If $\mathbf{V}$ is a monoidal pseudovariety such that $S \circledast (P, Sag(C)) \in \mathbf{V}$ for each $S \in \mathbf{V}$, then the continuous morphism $\kappa: \hat{F}_A(\mathbf{V}) \to \hat{F}_B(\mathbf{V})$ is injective as well, that is, C is a pro-$\mathbf{V}$ code.*

Proof. Let u and v be distinct elements of $\hat{F}_A(\mathbf{V})$. Then, there exists a semigroup $S \in \mathbf{V}$ and a continuous morphism $\sigma: \hat{F}_A(\mathbf{V}) \to S$ such that $u\sigma \neq v\sigma$. Let $\rho: \hat{F}_B(\mathbf{V}) \to Sag(C)$ be the continuous extension of the transition morphism of the sagittal automaton of C. By hypothesis, $S^1 \circledast (P, Sag(C))$ lies in $\mathbf{V}$. We define a continuous morphism τ from $\hat{F}_B(\mathbf{V})$ into $S^1 \circledast (P, Sag(C))$ by letting, for each letter $b \in B$, $b\tau$ be the matrix obtained from $b\rho$ by replacing the non zero entries on pairs of the form (p, pb) ($p, pb \in A\kappa$) by $1 \in S^1$, and the non zero entries on pairs of the form $(p, 1)$ ($p \in P$ and $pb = a\kappa$, $a \in A$) by $a\sigma$. For each word $w = a_1 \cdots a_n \in A^+$, it is easily verified that $w\kappa\tau$ has its $(1,1)$ entry equal to $w\sigma$. By continuity, the same equality holds for all elements $w \in \hat{F}_A(\mathbf{V})$, since they are limits of sequences of words. Therefore $u\kappa\tau \neq v\kappa\tau$, and hence $u\kappa \neq v\kappa$. Thus κ is a pro-$\mathbf{V}$ coding morphism. $\square$

The following consequence of this proposition is easily derived.

Corollary 2.2 *Let $\mathbf{H}$ be a pseudovariety of groups closed under semidirect product. Then every finite $\overline{\mathbf{H}}$-code is a pro-$\overline{\mathbf{H}}$ code. In particular, every finite code is a pro-$\mathbf{S}$ code and every finite aperiodic code is a pro-$\mathbf{A}$ code.*

Note. In [8, Thm. 1], Koryakov shows that the n-element code $C_n = \{y, xy, \ldots, x^{n-1}y\}$ is a pro-$\overline{\mathbf{H}}$ code for any pseudovariety of groups $\mathbf{H}$. It is easily verified that C_n is an aperiodic code for all n, so this result follows from the above corollary. In the same paper, Koryakov uses the resulting continuous one-to-one morphisms from the n-generated free pro-$\overline{\mathbf{H}}$ semigroups $\hat{F}_n(\overline{\mathbf{H}})$ into $\hat{F}_2(\overline{\mathbf{H}})$ to construct a continuous one-to-one morphism from $\tilde{F}_\omega(\overline{\mathbf{H}})$ (the inductive limit of the $\hat{F}_n(\overline{\mathbf{H}})$) into $\hat{F}_2(\overline{\mathbf{H}})$ with open image.

Examples. The sufficient condition in Proposition 2.1 is not necessary. Let indeed $\mathbf{N}$ denote the pseudovariety of nilpotent semigroups, $\mathbf{N} = [\![x^\omega y = yx^\omega = x^\omega]\!]$. Then $\hat{F}_A(\mathbf{N}) = A^+ \cup \{0\}$ (see [1]) and it is easily verified that every word code is a pro-$\mathbf{N}$ code.

Since every one-generated aperiodic semigroup is also nilpotent, for each one-letter alphabet $\{a\}$, we have $\hat{F}_{\{a\}}(\mathbf{A}) = a^+ \cup \{0\}$. It is then also easily verified that each non empty word a^k constitutes a code, whose sagittal semigroup is the k-element cyclic group, and which is also a pro-$\mathbf{A}$ code.

However, not every word code is pro-$\mathbf{A}$. A counterexample is given by the word code $\{aa, ab, ba, bb\}$. Let indeed $B = \{x, y, z, t\}$ and let $\kappa: \hat{F}_B(\mathbf{A}) \to \hat{F}_{\{a,b\}}(\mathbf{A})$ be given by $x\kappa = aa$, $y\kappa = ab$, $z\kappa = ba$ and $t\kappa = bb$. Then

$$\begin{aligned}
(x^\omega y^\omega z^\omega x^\omega)\kappa &= a^\omega (ab)^\omega (ba)^\omega a^\omega \\
&= a^\omega (ba)^\omega bb (ab)^\omega a^\omega \\
&= (x^\omega z^\omega t y^\omega x^\omega)\kappa.
\end{aligned}$$

But $x^\omega y^\omega z^\omega x^\omega \neq x^\omega z^\omega t y^\omega x^\omega$ in $\hat{F}_B(\mathbf{A})$ (since they have distinct alphabetical contents), so κ is not one-to-one, and hence $\{aa, ab, ba, bb\}$ is not a pro-$\mathbf{A}$ code.

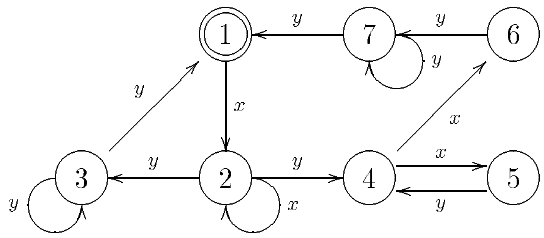
2.2 A coding for 2-variable pro-identities

In this section, we exhibit another, more specific, coding morphism. The reason for considering this particular coding will be made clear in Section 3.

Proposition 2.3 *Let* $\mathbf{V}$ *be a monoidal pseudovariety such that* $\mathbf{V} = \mathbf{V} \circledast \mathbf{A}$. *The continuous morphism* $\kappa\colon \hat{F}_{\{a,b\}}(\mathbf{V}) \to \hat{F}_{\{x,y\}}(\mathbf{V})$ *defined by* $a\kappa = x^\omega y^\omega$ *and* $b\kappa = x^\omega(yx)^\omega y^\omega$, *is a pro-*$\mathbf{V}$ *coding morphism.*

Proof. The proof relies on the same idea as the proof of Proposition 2.1, and makes use of an unambiguous automaton recognizing the subsemigroup generated by a certain infinite (word) code.

Let us consider the 2-letter alphabet $\{x, y\}$ and let $C = x^+yy^+ \cup x^+(yx)^+yy^+$. Then C is a code and the following automaton, $\mathcal{A}$, recognizes C^+ (with initial and terminal state 1).



Let $\rho\colon \{x, y\}^+ \to R$ be the transition morphism of $\mathcal{A}$, and let Q be its set of states, $Q = \{1, \ldots, 7\}$. Since C is a code, (Q, R) is a monoid of unambiguous relations. Moreover, one can verify that R is aperiodic, and hence $R \in \mathbf{V}$. Therefore we may consider the continuous extension $\rho\colon \hat{F}_{\{x,y\}}(\mathbf{V}) \to R$ of the transition morphism of $\mathcal{A}$. Let $\{a, b\}$ be another 2-letter alphabet, and let u, v be distinct elements of $\hat{F}_{\{a,b\}}(\mathbf{V})$: there exists a semigroup S in $\mathbf{V}$ and a continuous morphism $\sigma\colon \hat{F}_{\{a,b\}}(\mathbf{V}) \to S$ such that $u\sigma \neq v\sigma$. By hypothesis, the semigroup $T = S^1 \circledast (Q, R)$ lies in $\mathbf{V}$. Let τ be the continuous morphism from $\hat{F}_{\{x,y\}}(\mathbf{V})$ into T defined by letting $x\tau$ and $y\tau$ be the $Q \times Q$ matrices obtained from $x\rho$ and $y\rho$ respectively in the following fashion:

- for $x\tau$, replace all non-zero entries of $x\rho$ by $1 \in S^1$;
- for $y\tau$, replace the $(3, 1)$ entry of $y\rho$ by $a\sigma$, the $(7, 1)$ entry of $y\rho$ by $b\sigma$ and all other non-zero entries by 1.

Then, for each n, the $(1, 1)$ entry of $(x^ny^n)\tau$ is $a\sigma$, the $(1, 1)$ entry of $(x^n(yx)^ny^n)\tau$ is $b\sigma$, and hence, by continuity, the $(1, 1)$ entry of $(x^\omega y^\omega)\tau$ is $a\sigma$ and the $(1, 1)$ entry of $(x^\omega(yx)^\omega y^\omega)\tau$ is $b\sigma$. More generally, if κ is the continuous morphism from $\hat{F}_A(\mathbf{V})$ into $\hat{F}_B(\mathbf{V})$ defined by $a\kappa = x^\omega y^\omega$ and $b\kappa = x^\omega(yx)^\omega y^\omega$, then for each word $w \in A^+$, the $(1, 1)$ entry of $w\kappa\tau$ is $w\sigma$. By continuity again, the $(1, 1)$ entry of $w\kappa\tau$ is $w\sigma$ for each $w \in \hat{F}_A(\mathbf{V})$. Therefore, the $(1, 1)$ entries of $u\kappa\tau$ and $v\kappa\tau$ are distinct, so $u\kappa \neq v\kappa$. Thus κ is one-to-one, that is, κ is a pro-$\mathbf{V}$ coding morphism. □

Note. In the above proof, one could only require that $\mathbf{V} = \mathbf{V} \circledast \mathbf{W}$, where $\mathbf{W}$ is the pseudovariety generated by R. But R contains the 3-element monoid $U_2 = \{1, g, d\}$ given by $g^2 = dg = g$ and $d^2 = gd = d$. (Say $\{y^2\rho, (y^2xy^2)\rho, (y^2xyxy^2)\rho\}$ is isomorphic to U_2.) Therefore $\mathbf{V} = \mathbf{V} \circledast \mathbf{W}$ implies $\mathbf{V} = \mathbf{V} \circledast (U_2) = \mathbf{V} * (U_2)$. But the semidirect closure of (U_2) is $\mathbf{A}$ (see [5]), so $\mathbf{V} \circledast \mathbf{W} = \mathbf{V}$ is equivalent to $\mathbf{V} \circledast \mathbf{A} = \mathbf{V}$.

2.3 A last coding result

Our last coding result shows how one can use the two members of a non trivial pro-$\overline{\mathbf{H}}$-identity to construct a 2-element pro-$\overline{\mathbf{H}}$-code, when $\mathbf{H}$ is a pseudovariety of groups closed under semidirect product.

Proposition 2.4 *Let* $\mathbf{H}$ *be a pseudovariety of groups closed under semidirect product. Let* $u' = v'$ *be a non trivial pro-*$\overline{\mathbf{H}}$*-identity on some alphabet* B*, and let* z *be a new symbol, not in* B*. Then the continuous morphism* $\kappa\colon \hat{F}_{\{a,b\}}(\overline{\mathbf{H}}) \to \hat{F}_{B\cup\{z\}}(\overline{\mathbf{H}})$ *given by* $a\kappa = u'z$ *and* $b\kappa = v'z$*, is a pro-*$\overline{\mathbf{H}}$ *coding morphism.*

Proof. Let u, v be distinct elements of $\hat{F}_{\{a,b\}}(\overline{\mathbf{H}})$. There exists a semigroup S_1 (resp. S_2) in $\overline{\mathbf{H}}$ in which the pro-$\mathbf{V}$-identity $u = v$ (resp. $u' = v'$) does not hold. Then $S = S_1 \times S_2 \in \overline{\mathbf{H}}$, and S satisfies neither $u = v$ nor $u' = v'$. Since $\overline{\mathbf{H}}$ is monoidal, we may assume that S is a monoid. Let $\mu\colon \hat{F}_{\{a,b\}}(\overline{\mathbf{H}}) \to S$ and $\nu\colon \hat{F}_B(\overline{\mathbf{H}}) \to S$ be continuous morphisms such that $u\mu \neq v\mu$ and $u'\nu \neq v'\nu$. Let $B' = B \cup \{z\}$.

Let $\widetilde{S}$ be the semigroup $\widetilde{S} = S \cup \{\widetilde{s} \mid s \in S\} \cup \{\widetilde{z}\}$ (where z is a new symbol) endowed with the following product:

$$\begin{aligned} s \cdot t &= st \\ x \cdot \widetilde{t} &= \widetilde{t} \\ x \cdot \widetilde{z} &= \widetilde{z} \\ \widetilde{s} \cdot t &= \widetilde{st} \\ \widetilde{z} \cdot t &= \widetilde{t} \end{aligned}$$

for all $s, t \in S$ and $x \in \widetilde{S}$. The elements $\widetilde{s}$ ($s \in S$) and $\widetilde{z}$ form an aperiodic ideal of $\widetilde{S}$, so $\widetilde{S} \in \overline{\mathbf{H}}$, and it follows that the wreath product $S \circ \widetilde{S}$ lies in $\overline{\mathbf{H}}$ as well.

We now define a continuous morphism $\tau\colon \hat{F}_{B'}(\overline{\mathbf{H}}) \to S \circ \widetilde{S}$ by letting:

- for each letter $b \in B$, $b\tau = (f_1, b\nu)$, where $f_1\colon \widetilde{S} \to S$ is the constant function with value 1;
- $z\tau = (f_z, \widetilde{1})$, where $f_z\colon \widetilde{S} \to S$ is given, for each $s \in \widetilde{S}$, by

$$(s)f_z = \begin{cases} a\mu & \text{if } s = u'\nu \text{ or } s = \widetilde{u'\nu}; \\ b\mu & \text{if } s = v'\nu \text{ or } s = \widetilde{v'\nu}; \\ 1 & \text{otherwise.} \end{cases}$$

Then, for each word $w \in B^+$, $w\tau = (f_1, w\nu)$. By continuity, the same equality holds for all $w \in \hat{F}_B(\mathbf{V})$. Moreover, $(wz)\tau = (f_1, w\nu)(f_z, \widetilde{1}) = (g, \widetilde{1})$, with $(s)g = (s)f_1\ (s\,w\nu)f_z = (s\,w\nu)f_z$ for each $s \in \widetilde{S}$. In particular, $(1)g = (w\nu)f_z$ and $(\widetilde{1})g = (\widetilde{w\nu})f_z = (w\nu)f_z = (1)g$.

Let $w' \in \hat{F}_B(\mathbf{V})$ and let $(w'z)\tau = (g', \widetilde{1})$. Then

$$(wzw'z)\tau = (g, \widetilde{1})(g', \widetilde{1}) = (h, \widetilde{1}) \quad \text{with} \quad (s)h = (s)g\ (s\widetilde{1})g' = (s)g\ (\widetilde{1})g' = (s)g\ (1)g'.$$

So $(1)h = (1)g\ (1)g' = (w\nu)f_z\ (w'\nu)f_z$. More generally, if $w \in \{a, b\}^+$, then $w\kappa\tau = (h, \widetilde{1})$ with $(1)h = w\mu$. By continuity, it follows that $u\kappa\tau = (g, \widetilde{1})$ and $v\kappa\tau = (h, \widetilde{1})$ satisfy

$$g(1) = u\mu \quad \text{and} \quad h(1) = v\mu.$$

So $u\kappa\tau \neq v\kappa\tau$, and hence $u\kappa \neq v\kappa$. Thus κ is one-to-one, and hence it is a pro-$\overline{\mathbf{H}}$ coding morphism. $\square$

3 Irreducibility of certain pseudovarieties

In the rest of this article, $\mathbf{H}$ will be a pseudovariety of groups closed under semidirect product. We will prove that $\overline{\mathbf{H}}$ is Mal'cev irreducible. We first prove a weaker result.

Proposition 3.1 *Let* $\mathbf{V}$ *be a monoidal pseudovariety closed under unambiguous product with* $\mathbf{A}$ *and let* $\mathbf{W}$ *be a proper subpseudovariety of* $\mathbf{V}$*. Then* $(\mathbf{W} ⓜ \mathbf{Com}) \cap \mathbf{V}$ *is proper.*

Proof. Let $u = v$ be a non trivial pro-$\mathbf{V}$-identity satisfied by $\mathbf{W}$. Let X be the alphabet of variables of $u = v$, say, $X = \{x_1, \ldots, x_n\}$. Let $A = \{a, b\}$ and let $\kappa: X^+ \to A^+$ be defined by $x_i\kappa = a^i b$ for each $1 \leq i \leq n$. Then $X\kappa$ is a prefix code, and it is easily verified that $Sag(X\kappa)$ is aperiodic. By Proposition 2.1, it follows that $u\kappa = v\kappa$ is a non trivial pro-$\mathbf{V}$-identity. In addition, this pro-identity is satisfied by $\mathbf{W}$, since it is a continuous homomorphic image of a pro-identity which is. So we may assume that $u = v$ was chosen to be a 2-variable pro-$\mathbf{V}$-identity, on the alphabet A.

Let $\mathbf{S}$ be the pseudovariety of all semigroups and let $\pi: \hat{F}_A(\mathbf{S}) \to \hat{F}_A(\mathbf{V})$ be the natural projection. Since π is onto, we may consider elements u' and v' of $\hat{F}_A(\mathbf{S})$ such that $u'\pi = u$ and $v'\pi = v$. In particular, $\mathbf{W}$ satisfies the non trivial pro-identity $u' = v'$.

We now consider the pro-$\mathbf{S}$-identity

$$u'(x^\omega y^\omega, x^\omega (yx)^\omega y^\omega) = v'(x^\omega y^\omega, x^\omega (yx)^\omega y^\omega). \tag{1}$$

Observe that $\mathbf{Com}$ satisfies $(xy)^\omega = x^\omega y^\omega = x^\omega (yx)^\omega y^\omega$. Now [18, Lemma 4.2] states that $\mathbf{W} ⓜ \mathbf{Com}$ is defined by the pro-$\mathbf{S}$-identities of the form $\ell(z_1, \ldots, z_n) = r(z_1, \ldots, z_n)$ where $\ell = r$ is an n-variable pro-$\mathbf{S}$-identity satisfied by $\mathbf{W}$ and where $\mathbf{Com}$ satisfies $z_1 = \cdots = z_n = z_1^2$. Thus $\mathbf{W} ⓜ \mathbf{Com}$ satisfies the pro-identity (1), and hence so does $(\mathbf{W} ⓜ \mathbf{Com}) \cap \mathbf{V}$. Since the latter pseudovariety is contained in $\mathbf{V}$, it also satisfies the pro-$\mathbf{V}$-identity obtained by taking the image under π of the pro-identity (1), namely

$$u(x^\omega y^\omega, x^\omega (yx)^\omega y^\omega) = v(x^\omega y^\omega, x^\omega (yx)^\omega y^\omega). \tag{2}$$

There remains to verify that the pro-$\mathbf{V}$-identity (2) is non trivial, which follows immediately from Proposition 2.3, thus concluding the proof. □

Theorem 3.2 *Let* $\mathbf{H}$ *be a pseudovariety of groups closed under semidirect product. Then* $\overline{\mathbf{H}}$ *is Mal'cev irreducible.*

Proof. Let us first consider a proper subpseudovariety $\mathbf{V}_1$ of $\overline{\mathbf{H}}$. By Proposition 3.1, $(\mathbf{V}_1 ⓜ \mathbf{Com}) \cap \overline{\mathbf{H}}$ is proper as well. As above, we may consider a 2-variable non trivial pro-$\overline{\mathbf{H}}$-identity $u = v$ satisfied by $(\mathbf{V}_1 ⓜ \mathbf{Com}) \cap \overline{\mathbf{H}}$.

Let us now assume that $\overline{\mathbf{H}} = \mathbf{V}_1 ⓜ \mathbf{V}_2$ with $\mathbf{V}_2$ a proper subpseudovariety of $\overline{\mathbf{H}}$ as well, and let $u' = v'$ be a non trivial pro-$\overline{\mathbf{H}}$-identity satisfied by $\mathbf{V}_2$. Let z be a new variable, not in the alphabet of variables of $u' = v'$. Then by Proposition 2.4, the pro-$\overline{\mathbf{H}}$-identity $u(u'z, v'z) = v(u'z, v'z)$ is non trivial. To get a contradiction, it suffices to verify that it is satisfied by a set of generators of $\mathbf{V}_1 ⓜ \mathbf{V}_2$, and hence by the pseudovariety $\mathbf{V}_1 ⓜ \mathbf{V}_2$ itself.

Let C be the alphabet of variables of this pro-identity and let $A = \{a, b\}$ be the alphabet of variables of $u = v$. Let S be a semigroup in $\overline{\mathbf{H}}$ admitting an onto morphism $\pi: S \to T$ such that $T \in \mathbf{V}_2$ and $e\pi^{-1} \in \mathbf{V}_1$ for each idempotent e of T, and let $\varphi: \hat{F}_C(\overline{\mathbf{H}}) \to S$

be a continuous morphism. Let also $\kappa: \hat{F}_A(\overline{\mathbf{H}}) \to \hat{F}_C(\overline{\mathbf{H}})$ be the continuous morphism determined by $a\kappa = u'z$ and $b\kappa = v'z$.

$$\hat{F}_A(\overline{\mathbf{H}}) \xrightarrow{\kappa} \hat{F}_C(\overline{\mathbf{H}}) \xrightarrow{\varphi} S \xrightarrow{\pi} T$$

Since $T \in \mathbf{V}_2$, T satisfies $u'z = v'z$, and so $a\kappa\varphi\pi = b\kappa\varphi\pi = t_0$ for some $t_0 \in T$. Let T_0 be the subsemigroup of T generated by t_0. Then $T_0 \in \mathbf{Com}$. Moreover, if $S_0 = T_0\pi^{-1}$, then $S_0 \in \mathbf{V}_1 \circledm \mathbf{Com}$ and the range of $\kappa\varphi$ is in S_0. But S_0 lies also in $\overline{\mathbf{H}}$, so S_0 satisfies $u = v$, and hence $u\kappa\varphi = v\kappa\varphi$. Therefore, $u(u'z, v'z)\varphi = v(u'z, v'z)\varphi$. This concludes the proof. $\square$

If $\mathbf{V}$ is a pseudovariety, we let $L\mathbf{V}$ be the pseudovariety of semigroups S such that $eSe \in \mathbf{V}$ for each idempotent e of S. Since $\overline{\mathbf{H}}$ is monoidal, it is clear that the only pseudovariety $\mathbf{V}$ such that $\overline{\mathbf{H}} = L\mathbf{V}$ is $\mathbf{V} = \overline{\mathbf{H}}$ itself.

Corollary 3.3 *Let* $\mathbf{H}$ *be a pseudovariety of groups closed under semidirect product. Then* $\overline{\mathbf{H}}$ *is semidirectly irreducible.*

Proof. Let us assume that $\overline{\mathbf{H}} = \mathbf{V}_1 * \mathbf{V}_2$ where $\mathbf{V}_1$ and $\mathbf{V}_2$ are proper subpseudovarieties of $\overline{\mathbf{H}}$. Since $\overline{\mathbf{H}} \circledm \overline{\mathbf{H}} = \overline{\mathbf{H}}$ and $\mathbf{V}_1 * \mathbf{V}_2 \subseteq L\mathbf{V}_1 \circledm \mathbf{V}_2$ (see for instance [25, Lemma 2.2]), it follows that $\overline{\mathbf{H}} = L\mathbf{V}_1 \circledm \mathbf{V}_2$, and by Theorem 3.2, $\overline{\mathbf{H}} = L\mathbf{V}_1$. Therefore $\overline{\mathbf{H}} = \mathbf{V}_1$, a contradiction. $\square$

Corollary 3.4 *Let* $\mathbf{H}$ *be a pseudovariety of groups closed under semidirect product. Then* $\overline{\mathbf{H}}$ *is join irreducible.*

Proof. Let us assume that $\overline{\mathbf{H}} = \mathbf{V}_1 \vee \mathbf{V}_2$ where $\mathbf{V}_1$ and $\mathbf{V}_2$ are proper subpseudovarieties of $\overline{\mathbf{H}}$. Since $\overline{\mathbf{H}} \circledm \overline{\mathbf{H}} = \overline{\mathbf{H}}$, we have $\overline{\mathbf{H}} = \mathbf{V}_1 \circledm \mathbf{V}_2$, in contradiction with Theorem 3.2. So $\overline{\mathbf{H}}$ is $\vee$-irreducible. $\square$

4 Applications

The above results have noteworthy consequences. For instance, we get immediate proofs of the infinity of several well-known hierarchies of pseudovarieties.

First let us observe that, if $\mathbf{V}$ is a pseudovariety of monoids and $\mathbf{V_S}$ is the pseudovariety of semigroups generated by the elements of $\mathbf{V}$, then the join- (resp. semidirect, Mal'cev) irreducibility of $\mathbf{V_S}$ implies that of $\mathbf{V}$ (see [1, Section 7.1]). It follows that, for each pseudovariety of groups $\mathbf{H}$ closed under semidirect product, the pseudovariety of all monoids in which the subgroups are in $\mathbf{H}$, is Mal'cev irreducible, semidirectly irreducible and join irreducible. For convenience, this pseudovariety is also denoted by $\overline{\mathbf{H}}$, and in the case of the trivial pseudovariety of groups, we also denote by $\mathbf{A}$ the pseudovariety of aperiodic monoids.

The Straubing dot-depth hierarchy is a hierarchy of pseudovarieties of monoids within $\mathbf{A}$, with connections with language theory and the theory of complexity for boolean circuits. It is defined by letting $\mathbf{V}_0 = \mathbf{I}$, the trivial pseudovariety, and $\mathbf{V}_{n+1} = \Diamond\mathbf{V}_n$ for all $n \geq 0$. Here $\Diamond$ denotes the Schützenberger operator. For complete definitions and references, see [23, 19]. It is well-known that $\mathbf{A}$ is the union of the increasing sequence of the $\mathbf{V}_n$. In [15], it is proved that for any pseudovariety $\mathbf{V}$, $\Diamond\mathbf{V} \subseteq \mathbf{B}_1 \mathbin{ⓜ} \mathbf{V}$, where $\mathbf{B}_1$ is the pseudovariety of aperiodic semigroups

$$\mathbf{B}_1 = [\![(x^\omega s y^\omega t x^\omega)^\omega s y^\omega v (x^\omega u y^\omega v x^\omega)^\omega = (x^\omega s y^\omega t x^\omega)^\omega (x^\omega u y^\omega v x^\omega)^\omega]\!].$$

Proposition 4.1 *The Straubing dot-depth hierarchy is infinite.*

Proof. Let us assume that $\mathbf{A} = \mathbf{V}_{n+1}$, with n minimal. Then $\mathbf{A} = \Diamond\mathbf{V}_n$, and hence $\mathbf{A} = \mathbf{B}_1 \mathbin{ⓜ} \mathbf{V}_n$. But $\mathbf{A}$ is Mal'cev irreducible and $\mathbf{B}_1$ is proper, and so is $\mathbf{V}_n$ by definition of n, so we get a contradiction. $\square$

The original proof of this statement is due to Straubing [23].

The Krohn-Rhodes theorem [5] states that each finite monoid M divides a wreath product of the form

$$M < M_k \circ M_{k-1} \circ \cdots \circ M_1$$

where the M_i are either groups dividing M or copies of the three element monoid U_2 (see Section 2.2). It follows that each finite monoid M divides a wreath product of the form

$$M < A_n \circ G_n \circ A_{n-1} \circ \cdots \circ G_1 \circ A_0$$

where the A_i are aperiodic and the G_i are groups (more precisely, the G_i are wreath products of copies of groups dividing M). Let us consider the following sequence of pseudovarieties of monoids: $\mathbf{C}_0 = \mathbf{A}$ and $\mathbf{C}_{n+1} = \mathbf{A} * \mathbf{G} * \mathbf{C}_n$ for each $n \geq 0$. By the Krohn-Rhodes theorem, the pseudovariety $\mathbf{M}$ of all finite monoids is the union of the increasing sequence $(\mathbf{C}_n)_n$. The least integer n such that a given finite monoid M lies in $\mathbf{C}_n$ is called the *group complexity* of M. It is an old-standing conjecture whether the group complexity of a finite monoid M is effectively computable [5, 7]. Our results give an immediate proof that the hierarchy given by the $\mathbf{C}_n$ is infinite. This was originally proved by Rhodes [21].

Proposition 4.2 *The group complexity hierarchy is infinite.*

Proof. If $\mathbf{M} = \mathbf{C}_{n+1}$ with n minimal, then $\mathbf{M} = \mathbf{A} * \mathbf{G} * \mathbf{C}_n$. Since $\mathbf{M}$ is semidirectly irreducible and $\mathbf{M} \neq \mathbf{C}_n$ by definition of n, it follows that $\mathbf{M} = \mathbf{A} * \mathbf{G}$, and hence $\mathbf{M} = \mathbf{A}$ or $\mathbf{M} = \mathbf{G}$, a contradiction. $\square$

The Krohn-Rhodes theorem also implies that, if $\mathbf{H}$ is a pseudovariety of groups such that $\mathbf{H} = \mathbf{H} * \mathbf{H}$, then the pseudovariety of monoids $\overline{\mathbf{H}}$ is the union of the increasing sequence of pseudovarieties given by $\mathbf{C}_0(\mathbf{H}) = \mathbf{A}$ and $\mathbf{C}_{n+1}(\mathbf{H}) = \mathbf{A} * \mathbf{G} * \mathbf{C}_n(\mathbf{H})$ for each $n \geq 0$. With the same proof, it can be shown that the resulting hierarchy in $\overline{\mathbf{H}}$ is infinite.

Another consequence of the Krohn-Rhodes theorem is that each aperiodic monoid divides a wreath product of copies of U_2. Let now $\mathbf{V}$ be a subpseudovariety of $\mathbf{A}$ containing U_2 and let $\mathbf{V}^{(1)} = \mathbf{V}$ and $\mathbf{V}^{(n+1)} = \mathbf{V} * \mathbf{V}^{(n)}$. This is an increasing sequence of pseudovarieties of monoids within $\mathbf{A}$, and $\mathbf{A} = \bigcup_n \mathbf{V}^{(n)}$. Then we have the following infinity result[2].

[2]The authors thank P. Higgins for bringing this corollary to their attention.

Proposition 4.3 *Let $\mathbf{V}$ be a subpseudovariety of $\mathbf{A}$ containing U_2 and let $(\mathbf{V}^{(n)})_n$ be the associated increasing sequence of subpseudovarieties of $\mathbf{A}$. If $\mathbf{V} \neq \mathbf{A}$, then $\mathbf{V}^{(n)}$ is strictly contained in $\mathbf{V}^{(n+1)}$ for each $n \geq 1$. That is, the resulting hierarchy within $\mathbf{A}$ is infinite.*

Proof. If $\mathbf{V}^{(n)} = \mathbf{V}^{(n+1)}$ with n minimal, then $\mathbf{A} = \mathbf{V} * \mathbf{V}^{(n)}$. Since $\mathbf{A}$ is semidirectly irreducible, it follows that $\mathbf{A} = \mathbf{V}$ by definition of n, a contradiction. □

We can also extend a result of Margolis on maximal subpseudovarieties [11] (for pseudovarieties of semigroups or of monoids).

Corollary 4.4 *Let $\mathbf{H}$ be a pseudovariety of groups closed under semidirect product. Then $\overline{\mathbf{H}}$ admits no maximal proper subpseudovariety.*

Proof. Let $\mathbf{W}$ be a maximal proper subpseudovariety of $\overline{\mathbf{H}}$, and let $S \in \overline{\mathbf{H}} \setminus \mathbf{W}$. Let $\mathbf{W}'$ be the pseudovariety generated by S. Then $\mathbf{W} \subseteq \mathbf{W} \vee \mathbf{W}' \subseteq \overline{\mathbf{H}}$ and $\mathbf{W} \neq \mathbf{W} \vee \mathbf{W}'$, so $\overline{\mathbf{H}} = \mathbf{W} \vee \mathbf{W}'$. Since $\overline{\mathbf{H}}$ is $\vee$-irreducible, it follows that $\overline{\mathbf{H}} = \mathbf{W}'$. In particular, $\overline{\mathbf{H}}$ admits a finite free object over each finite alphabet. This yields immediately a contradiction, since $\overline{\mathbf{H}}$ admits infinitely many 1-generated elements. □

Finally, let us recall that Eilenberg's theorem [5] shows that varieties of rational languages are in bijective correspondence with pseudovarieties of semigroups. In particular, the varieties of languages associated with $\mathbf{S}$ and $\mathbf{A}$ in this correspondance are respectively the variety of all rational languages and the variety of all star-free languages [14]. The irreducibility results obtained in this paper can be readily translated into analogous results for varieties of rational languages.

5 Conclusion

We have proved that, whenever $\mathbf{H}$ is a pseudovariety of groups closed under extension, then the pseudovariety $\overline{\mathbf{H}}$ of all finite semigroups in which all the subgroups are in $\mathbf{H}$, is irreducible for the three main binary operations on pseudovarieties, the join, the semidirect product and the Mal'cev product.

Our proof relies heavily on coding techniques for identities in relatively free profinite structures (pro-identities). We gave sufficient conditions under which an injective, or coding, morphism between free semigroups extends to an injective continuous morphism between free pro-$\mathbf{V}$ semigroups. We also proved the injectivity of other continuous morphisms between free pro-$\mathbf{V}$ semigroups. This opens up the question of describing as accurately as possible all finite pro-$\mathbf{V}$ codes, that is, all continuous embeddings of a free pro-$\mathbf{V}$ semigroup into another one.

Observe that our method does not apply to other pseudovarieties than those of the form $\overline{\mathbf{H}}$, where $\mathbf{H}$ is a pseudovariety of groups closed under semidirect product. It would be interesting to develop general techniques to prove just, say, the join irreducibility, or the semidirect irreducibility of a pseudovariety.

We can also ask, more specifically, whether all pseudovarieties of the form $\overline{\mathbf{H}}$ (with $\mathbf{H}$ a pseudovariety of groups) are irreducible for join, semidirect product or Mal'cev product. For instance, Margolis [11] shows that $\overline{\mathbf{H}}$ has no maximal proper subpseudovarieties for any $\mathbf{H}$ containing the pseudovariety $\mathbf{Ab}$ of all commutative groups.

Another interesting question is that of the join irreducibility of the complexity classes $\mathbf{C}_n$ introduced in the previous section. We now know that $\mathbf{C}_0$ is join and semidirectly irreducible. The other classes are trivially semidirectly reducible.

References

[1] J. Almeida. *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1994.

[2] J. Almeida. On direct product decompositions of $\mathcal{J}$-trivial semigroups, *Intern. J. Algebra and Comput.* **1** (1991) 329–337.

[3] J. Almeida and P. Weil. Relatively free profinite monoids: an introduction and examples, in J. Fountain ed. *Semigroups, Formal Languages and Groups*, NATO ASI Series C-466, Kluwer Academic, 1995, 73–117.

[4] J. Berstel and D. Perrin. *Theory of Codes*, Academic Press, New York, 1985.

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

[6] T. Evans. The lattice of semigroup varieties, *Semigroup Forum* **2** (1971) 1–43.

[7] K. Henckell, S. W. Margolis, J.-E. Pin and J. Rhodes. Ash's type II theorem, profinite topology and Malcev products, *International Journal of Algebra and Computation* **1** (1991) 411–436.

[8] I. Koryakov. Embedding of pseudofree semigroups, *Izvestiya VUZ Matem.* **39** (1995), 58–64. English translation: *Russian Mathem. (Iz. VUZ)* **39** (1995) 53–69.

[9] E. Le Rest and M. Le Rest. Sur le calcul du monoïde syntaxique d'un sous-monoïde finiment engendré, *Semigroup Forum* **21** (1980) 173–185.

[10] A. Malcev. Nilpotent Semigroups, *Uch. Zap. Ivanovsk. Ped. In-ta* **4** (1953) 107–111.

[11] S. Margolis. On maximal varieties of finite monoids and semigroups, *Izvestiya VUZ Matem.* **39** (1995), 65–70. English translation: *Russian Mathem. (Iz. VUZ)* **39** (1995) 60–64.

[12] H. Neumann. *Varieties of groups*, Springer (1967).

[13] K. Numakura. Theorems on compact, totally disconnected semigroups and lattices, *Proc. Amer. Math. Soc.* **8** (1957) 623–626.

[14] J.-E. Pin. *Variétés de langages formels*, Masson, Paris, 1984. English translation: *Varieties of formal languages*, North Oxford, London and Plenum, New York, 1986.

[15] J.-E. Pin. A property of the Schützenberger product, *Semigroup Forum* **35** (1987) 53–62.

[16] J.-E. Pin and J. Sakarovitch. Une application de la représentation matricielle des transductions, *Theoret. Comp. Science* **35** (1985) 271–293.

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

[18] J.-E. Pin and P. Weil. Profinite semigroups, Mal'cev products and identities, *J. Algebra* **182** (1996) 604–626.

[19] J.-E. Pin and P. Weil. Polynomial closure and unambiguous product, *Theory of Computing Systems*, to appear.

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

[21] J. Rhodes. Some results on finite semigroups, *J. Algebra* **4** (1966) 471–504.

[22] J. Sakarovitch. Sur la définition du produit en couronne, in G. Pirillo ed. *Colloque Codages et Transductions*, Florence, 1981, 285–300.

[23] H. Straubing. A generalization of the Schützenberger product of finite monoids, *Theoret. Comp. Science* **13** (1981) 137–150.

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

[25] P. Weil. Closure of varieties of languages under products with counter, *Journ. Comp. System and Science* **45** (1992) 316–339.