

ON THE DECIDABILITY OF THE MEMBERSHIP PROBLEM OF THE PSEUDOVARIETY $\mathbf{J} \vee \mathbf{B}$

MARC ZEITOUN

LITP

Institut Blaise Pascal

4 Place Jussieu

75252 Paris Cedex 05 – France

e-mail: mz@litp.ibp.fr

AMS Mathematics Subject Classification: 20M07, 20M05

The aim of this article is to prove that the pseudovariety generated by $\mathbf{J} \vee \mathbf{B}$, that is to say, the join of the pseudovariety of \mathcal{J} -trivial semigroups and of the pseudovariety of idempotents semigroups, is decidable. The techniques used were developed by Almeida and are based on the study of the topological semigroup of implicit operations.

1. Introduction

Eilenberg's theorem on varieties [21] states that some classes of rational languages, called varieties, are in one-to-one correspondence with some classes of finite semigroups, the pseudovarieties, also called varieties of finite semigroups. These classes play a central role in the theory of rational languages and finite semigroups, and numerous works have been devoted to their study. Like in other domains of computer science, decision problems are frequently proposed. In particular, a crucial question is to determine an algorithm for checking whether a given recognizable language (resp. a given finite semigroup) belongs to a fixed class of languages (resp. of semigroups). If such an algorithm exists, then the membership problem for this class is said to be *decidable*.

The theories of rational languages and of finite semigroups motivate a systematic study of some fundamental operators on pseudovarieties. Researchers have concentrated their attention on the following ones:

- The unary operator \mathbf{P}_- that associates to each pseudovariety \mathbf{V} the

pseudovariety \mathbf{PV} generated by the power semigroups of all semigroups of \mathbf{V} . It is related to several problems in language theory ([4,5,27]).

- The semidirect product $\mathbf{V} * \mathbf{W}$ of two pseudovarieties \mathbf{V} and \mathbf{W} , which is connected to the Rhodes' theory of semigroups complexity.
- The Mal'cev product $\mathbf{V} \circledast \mathbf{W}$ of two pseudovarieties \mathbf{V} and \mathbf{W} that occurs also frequently in language theory and in semigroup theory ([22]).
- The join $\mathbf{V} \vee \mathbf{W}$ of two pseudovarieties \mathbf{V} and \mathbf{W} , whose definition is probably the most natural: the pseudovariety $\mathbf{V} \vee \mathbf{W}$ is the *smallest pseudovariety* that contains \mathbf{V} and \mathbf{W} . It leads to the study of lattice properties. It corresponds to the parallel computation of automata.

This last operator is the central subject of this paper. More precisely, we are interested in the decidability problem for $\mathbf{V} \vee \mathbf{W}$.

Despite the elementary nature of its construction, the join of two decidable pseudovarieties might not be decidable. A very surprising example was given by Albert, Baldinger and Rhodes [1]: there exists a finite set of identities in two variables Σ such that $[\Sigma] \vee \mathbf{Com}$ is undecidable, where $[\Sigma]$ denotes the (decidable) class of all finite semigroups satisfying the identities of Σ and \mathbf{Com} denotes the class of finite commutative semigroups. Actually, no general method to solve the membership problem of a pseudovariety is known as yet.

Rhodes [29], Almeida [2] and Kharlampovich and Sapir [24] proposed a list of problems on pseudovarieties, most of which are still open. The aim of this article is to give an answer to problem **22** of [2]: “Compute $\mathbf{J} \vee \mathbf{B}$ ”, where \mathbf{J} denotes the pseudovariety of \mathcal{J} -trivial semigroups and \mathbf{B} the pseudovariety of idempotents semigroups. The word “compute” may be understood as:

- find a finite basis, or prove that the pseudovariety is not finitely based;
- solve the membership problem for the pseudovariety.

On the positive side, we show here that the pseudovariety $\mathbf{J} \vee \mathbf{B}$ is decidable. On the negative side, we will show elsewhere that this pseudovariety is not finitely based ([33]).

Most of the few known results concerning calculations of joins of pseudovarieties are due to Almeida, Azevedo and Weil. Almeida [2] introduced a technique based on the theory of implicit operations that he developed. It requires some *ad hoc* arguments, but is successful to compute some non trivial joins: amongst them $\mathbf{R} \vee \mathbf{L}$ ([11]), where \mathbf{R} (resp. \mathbf{L}) denotes the pseudovariety of \mathcal{R} -trivial (resp. \mathcal{L} -trivial) semigroups, $\mathbf{G} \vee \mathbf{Com}$ ([6]),

where \mathbf{G} is the pseudovariety of finite groups, $\mathbf{Perm} \vee \mathbf{J}$ ([15]) where \mathbf{Perm} is the pseudovariety of all semigroups satisfying a non-trivial permutation identity, $\mathbf{G} \vee \mathbf{B}$ ([16]), and more recently, $\mathbf{G} \vee (\mathbf{J} \cap \mathbf{Inv})$ ([13]) where \mathbf{Inv} is the pseudovariety of all semigroups whose idempotents commute. See [2,32] for a more complete list of results.

The idea is the following: to prove the equality $\mathbf{V} = \mathbf{W}_1 \vee \mathbf{W}_2$ where \mathbf{V} is the candidate, one checks first that \mathbf{W}_1 and \mathbf{W}_2 are contained in \mathbf{V} . These inclusions are in general easy because \mathbf{V} is precisely chosen to contain \mathbf{W}_1 and \mathbf{W}_2 . This gives the inclusion $\mathbf{W}_1 \vee \mathbf{W}_2 \subset \mathbf{V}$. In the opposite direction, Reiterman's theorem (theorem 2.2.1 below) states that $\mathbf{W}_1 \vee \mathbf{W}_2$ can be written $[[\Sigma]]_{\mathbf{V}}$, where Σ is a set of pseudoidentities for \mathbf{V} . Therefore, it suffices to show that for every pseudoidentity (π, ρ) of Σ (and such pseudoidentities are satisfied by \mathbf{W}_1 and \mathbf{W}_2), π and ρ are identical.

The paper is organized as follows. Section 2 contains basic facts about pseudovarieties and implicit operations. In section 3, we guess and study a natural candidate for $\mathbf{J} \vee \mathbf{B}$ and its implicit operations. This gives an infinite basis for $\mathbf{J} \vee \mathbf{B}$ (sections 3.1 and 3.2). The proof of the decidability of $\mathbf{J} \vee \mathbf{B}$ is based on the above technique, but also requires some arguments of automata theory. It is given in section 3.3.

2. Background

We briefly review the main definitions and some useful facts about semigroups, pseudovarieties and implicit operations. The reader who wants more details is referred to the books of Almeida [2], Pin [26], the article of Almeida [7] or for a brief introduction, to the surveys of Almeida and Weil [8], [13], [14], and [31]. We assume the reader to be familiar with some basic notions of topology, universal algebra and semigroup theory (see [19], [20], [26]).

2.1. Semigroups and pseudovarieties

In the sequel, A_n denotes the finite alphabet $\{x_1, \dots, x_n\}$ and A the countable alphabet $\bigcup_{n>0} A_n$. For a word $u \in A_n^+$, the content $c(u)$ of u is the set of all letters appearing in u .

A *pseudovariety* of semigroups is a class of finite semigroups closed under formation of finitary product, homomorphic image and subsemigroup. The pseudovariety of all finite semigroups is denoted by \mathbf{S} , and

the one of all finite aperiodic (or group-free) semigroups is denoted by **A**. For any pseudovariety **V**, **DV** is the pseudovariety of all semigroups whose regular \mathcal{D} -classes are semigroups of **V**. An idempotent semigroup is called a *band*. The pseudovariety of finite bands is denoted by **B**. The pseudovariety of finite commutative bands (that is, of finite semilattices) is denoted by **Sl**. Finally, **J** denotes the pseudovariety of all \mathcal{J} -trivial semigroups.

The free band is a finite semigroup, quotient of the free semigroup A_n^+ by the congruence generated by $x = x^2$ (see [23,25]). We denote this congruence over A_n^+ by \equiv_n . Notice that one can define the content of an element of the free band, since two \equiv_n -congruent words have the same content.

The only fact on bands we will require is the following basic proposition. It is the key lemma for solving the word problem in the free band:

Proposition 2.1.1. ([23,25]) *Let u, v , and w be words of A_n^+ such that $c(v) \subseteq c(u) = c(w)$. Then $uvw \equiv_n uw$.*

2.2. Implicit operations

Given a pseudovariety **V**, an *implicit operation* for **V** is a family $(\pi_S)_{S \in \mathbf{V}}$ such that

- (i) for every $S \in \mathbf{V}$, π_S is a function from S^n into S ;
- (ii) for every morphism $\varphi : S \rightarrow T$ between members of **V**, the diagram

$$\begin{array}{ccc} S^n & \xrightarrow{\pi_S} & S \\ \downarrow \varphi^n & & \downarrow \varphi \\ T^n & \xrightarrow{\pi_T} & T \end{array}$$

commutes.

The set of all implicit operations for **V** is denoted by $\overline{F}_n(\mathbf{V})$. Notice that a word u defines an implicit operation $(u_S)_{S \in \mathbf{V}}$: one evaluates u over the semigroup S . An implicit operation that can be defined by a word is said to be *explicit*. The set of all explicit operations is denoted by $F_n(\mathbf{V})$. The set of all implicit operations is equipped with the product topology.

If the multiplication of $\pi, \rho \in \overline{\mathbf{F}}_n(\mathbf{V})$ is defined by

$$(\pi\rho)_S(x_1, \dots, x_n) = \pi_S(x_1, \dots, x_n)\rho_S(x_1, \dots, x_n)$$

then $\overline{\mathbf{F}}_n(\mathbf{V})$ is a compact totally disconnected topological semigroup. A pair $(\pi, \rho) \in \overline{\mathbf{F}}_n(\mathbf{V}) \times \overline{\mathbf{F}}_n(\mathbf{V})$ is called a *pseudoidentity*. Let (π, ρ) be a pseudoidentity. A semigroup $S \in \mathbf{V}$ *satisfies* (π, ρ) if and only if $\pi_S = \rho_S$. We will then write $S \models \pi = \rho$. If Σ is a set of pseudoidentities for a pseudovariety \mathbf{V} , S satisfies Σ if S satisfies every pseudoidentity of Σ , and a class \mathcal{C} of semigroups satisfies Σ if every semigroup of \mathcal{C} satisfies Σ . The class $[\Sigma]_{\mathbf{V}}$ of all semigroups of \mathbf{V} satisfying Σ is a pseudovariety.

Given an implicit operation π , one can define another implicit operation π^ω as the limit of the sequence $\pi^{n!}$. If x is a letter, it is easy to see that the evaluation of x^ω over an element s of a semigroup is the idempotent of the subsemigroup generated by s . The notation $x^{\omega+1}$ is an abbreviation for xx^ω . It is well known that the function $\pi \mapsto \pi^\omega$ is continuous.

The following characterization of pseudovarieties is fundamental:

Theorem 2.2.1. (Reiterman, [28]) *Let \mathbf{V} be a pseudovariety of semigroups and let \mathbf{W} be a subclass of \mathbf{V} . Then, \mathbf{W} is a pseudovariety if and only if there exists a set of pseudoidentities $\Sigma \subset \overline{\mathbf{F}}_n(\mathbf{V}) \times \overline{\mathbf{F}}_n(\mathbf{V})$ such that $\mathbf{W} = [\Sigma]_{\mathbf{V}}$.*

For example, \mathbf{J} is defined by $(xy)^\omega = (yx)^\omega$, $x^\omega = x^{\omega+1}$.

In the sequel, we will write $[\Sigma]$ instead of $[\Sigma]_{\mathbf{S}}$. We will say that the pseudoidentities of a set Σ *imply* those of a set Σ' if every semigroup that satisfies Σ also satisfies Σ' . Notice that Birkhoff's completeness theorem doesn't hold for pseudovarieties, and there are no rules to *derive* pseudoidentities of Σ' from pseudoidentities of Σ (see [2,9]).

The notion of content can be generalized for implicit operations as follows:

Theorem 2.2.2. (Almeida, Azevedo, [2,16]) *Let \mathbf{V} be a pseudovariety containing \mathbf{SI} . Then*

$$\begin{aligned} c : \overline{\mathbf{F}}_n(\mathbf{V}) &\longrightarrow \overline{\mathbf{F}}_n(\mathbf{SI}) \\ \pi &\longmapsto (\pi_S)_{S \in \mathbf{SI}} \end{aligned}$$

is a continuous homomorphism.

The study of implicit operations for \mathbf{DS} was done by Almeida and Azevedo:

Theorem 2.2.3. (Almeida, Azevedo, [2,12,16,17]) *Every implicit operation $\pi \in \overline{\mathbf{F}}_n(\mathbf{S})$ admits a factorization of the form $\pi = \pi_1 \dots \pi_k$ where π_i is either explicit or its restriction to \mathbf{DS} is regular.*

Finally, the knowledge of implicit operations for \mathbf{J} will be very useful:

Theorem 2.2.4. (Almeida, [10]) *Every implicit operation $\pi \in \overline{\mathbf{F}}_n(\mathbf{J})$ has a canonical factorization $\pi = \pi_1 \dots \pi_k$ where:*

1. *Every π_i is either explicit or of the form u_i^ω with u_i explicit.*
2. *If π_i is idempotent, then every letter of u_i appears only once and if $j < k$, then x_j appears before x_k .*
3. *Two consecutive factors cannot both be explicit.*
4. *Two consecutive idempotent factors have incomparable contents.*
5. *If π_i is explicit and π_{i+1} idempotent, then the last letter of π_i doesn't appear in π_{i+1} .*
6. *If π_i is idempotent and π_{i+1} explicit, then the first letter of π_{i+1} doesn't appear in π_i .*

If $\pi, \rho \in \overline{\mathbf{F}}_n(\mathbf{J})$, where $\pi = \pi_1 \dots \pi_k$ and $\rho = \rho_1 \dots \rho_l$ are the canonical factorizations, then $\pi = \rho$ if and only if $k = l$ and for every $i = 1, \dots, k$, $\pi_i = \rho_i$.

3. The pseudovariety $\mathbf{J} \vee \mathbf{B}$

It is clear that the pseudoidentities satisfied by $\mathbf{W}_1 \vee \mathbf{W}_2$ are those satisfied by both \mathbf{W}_1 and \mathbf{W}_2 . We will start from a finite set of simple pseudoidentities satisfied by \mathbf{J} and \mathbf{B} . A natural approach is to find pseudoidentities of $\mathbf{J} \vee \mathbf{B}$ are implied from them: if all the pseudoidentities of $\mathbf{J} \vee \mathbf{B}$ are implied from them, to try to find a finite basis. We will find however a semigroup that satisfies our first pseudoidentities but that doesn't belong to $\mathbf{J} \vee \mathbf{B}$. Nevertheless, the knowledge of the pseudoidentities satisfied by \mathbf{J} and by \mathbf{B} gives a description of an (infinite) basis of $\mathbf{J} \vee \mathbf{B}$. The regularities of this basis lead to the main result:

Theorem 3.1. *The pseudovariety $\mathbf{J} \vee \mathbf{B}$ is decidable.*

Using Eilenberg's theorem on varieties ([21]) and Simon's characterization of the languages recognized by \mathcal{J} -trivial semigroups ([30]), one gets another formulation of this theorem:

Theorem 3.2. *One can decide whether a rational language of A_n^+ is a boolean combination of piecewise testable languages and of \equiv_n -classes.*

3.1. A natural upper bound of $\mathbf{J} \vee \mathbf{B}$

There are several choices for an upper bound of $\mathbf{J} \vee \mathbf{B}$. Three natural candidates are:

$$\begin{aligned}\mathbf{V} &= \llbracket x(xy)^\omega = (xy)^\omega = (xy)^\omega y \rrbracket \\ \mathbf{V}' &= \llbracket (x^\omega y^\omega)^\omega = (xy)^\omega, x^\omega = x^{\omega+1} \rrbracket \\ \mathbf{V}'' &= \llbracket \{(x_1^\omega \dots x_n^\omega)^\omega = (x_1 \dots x_n)^\omega \mid n \in \mathbb{N}\}, x^\omega = x^{\omega+1} \rrbracket\end{aligned}$$

We denote by (1) (resp. (2), (3)) the pseudoidentities defining \mathbf{V} (resp. \mathbf{V}' , \mathbf{V}''). Let us first verify that \mathbf{V} , for instance, is not too large:

Proposition 3.1.1. *\mathbf{V} is a subpseudovariety of \mathbf{DA} .*

Proof. Note that (1) implies aperiodicity (take $x = y$). It remains to show that \mathbf{V} satisfies $(xy)^\omega (yx)^\omega (xy)^\omega = (xy)^\omega$. Let S be a semigroup satisfying (1) and $x, y \in S$. Then the following equalities hold in S :

$$\begin{aligned}(xy)^\omega (yx)^\omega (xy)^\omega &= (xy)^{\omega+1} (yx)^\omega (xy)^{\omega+1} && \text{by aperiodicity} \\ &= (xy)^\omega x.y (yx)^\omega x.y (xy)^\omega \\ &= (xy)^\omega x.(yx)^\omega .y (xy)^\omega && \text{by (1)} \\ &= (xy)^\omega && \text{by aperiodicity}\end{aligned}$$

One could check that the inclusion $\mathbf{V} \subset \mathbf{DA}$ is strict, by noting that $\overline{F}_n(\llbracket x_1 x_2 y z_1 z_2 = x_1 x_2 z_1 z_2 \rrbracket)$ is a finite semigroup of \mathbf{DA} which doesn't belong to \mathbf{V} .

It is natural to ask which of the pseudoidentities \mathbf{V} , \mathbf{V}' and \mathbf{V}'' is the smallest. In fact, they are equal:

Proposition 3.1.2. *The pseudovarieties \mathbf{V} , \mathbf{V}' , and \mathbf{V}'' are equal:*

$$\begin{aligned}\llbracket x(xy)^\omega = (xy)^\omega = (xy)^\omega y \rrbracket &= \llbracket x^\omega = x^{\omega+1}, (x^\omega y^\omega)^\omega = (xy)^\omega \rrbracket \\ &= \llbracket \{(x_1^\omega \dots x_n^\omega)^\omega = (x_1 \dots x_n)^\omega \mid n \in \mathbb{N}\} \rrbracket_{\mathbf{A}}\end{aligned}$$

The inclusion $\mathbf{V}'' \subseteq \mathbf{V}'$ is clear since the pseudoidentities of \mathbf{V}' are also pseudoidentities of \mathbf{V}'' . The remaining inclusions $\mathbf{V} \subset \mathbf{V}'$, $\mathbf{V} \subset \mathbf{V}''$ and $\mathbf{V}' \subset \mathbf{V}$ are proved separately in lemmas **3.1.3**, **3.1.4** and **3.1.5**.

Lemma 3.1.3. *The pseudoidentities (1) imply*

$$(xy^2)^\omega = (xy)^\omega = (x^2y)^\omega$$

and the pseudoidentities (2). Therefore, $\mathbf{V} \subseteq \mathbf{V}'$.

Proof. Let S be a semigroup satisfying the pseudoidentities (1) and let $x, y \in S$. Then the following equalities hold in S :

$$\begin{aligned} (xy)^\omega &= (xy)^\omega(xy)^\omega \\ &= (xy)^\omega(xy)^\omega y && \text{by (1)} \\ &= (xy)^{\omega-1}(xy)^\omega(xy^2) \\ &= (xy)^{\omega-2}(xy)^\omega(xy^2)^2 && \text{in the same way} \\ &= \dots \\ &= (xy)^\omega(xy^2)^\omega \\ &= x(yx)^{\omega-1}(y.xy)^\omega y \\ &= x(yx)^{\omega-1}y(yxy)^\omega y && \text{by (1)} \\ &= (xy)^{\omega-1}(xy^2)^{\omega+1} \\ &= (xy)^{\omega-2}(xy^2)^{\omega+2} && \text{in the same way} \\ &= \dots \\ &= (xy^2)^{2\omega} \\ &= (xy^2)^\omega \end{aligned}$$

One could show in the same way that S satisfies $(xy)^\omega = (x^2y)^\omega$. It follows that for each pair $(r, s) \in \mathbb{N}^2$:

$$(x^r y^s)^\omega = (x^{2r} y^{2s})^\omega = \dots = (x^\omega y^\omega)^\omega$$

and in particular $(xy)^\omega = (x^\omega y^\omega)^\omega$.

The following lemma is obtained in a similar way:

Lemma 3.1.4. *The pseudoidentities (1) imply the pseudoidentities (3). Therefore, $\mathbf{V} \subseteq \mathbf{V}''$.*

Proof. Let S be a semigroup satisfying the pseudoidentities (1) and let $x, y, z \in S$. Then the following equalities hold in S :

$$\begin{aligned} (xyz)^\omega &= (xyz)^\omega(xyz)^\omega \\ &= x(y.zx)^\omega yz(xyz)^{\omega-1} \\ &= x(y^2zx)^\omega yz(xyz)^{\omega-1} && \text{by lemma 3.1.3} \\ &= (xy^2z)^\omega(xyz)^\omega \end{aligned}$$

Similarly, $(xy^2z)^\omega = (xyz)^\omega(xy^2z)^\omega$. Hence $(xyz)^\omega \mathcal{R} (xy^2z)^\omega$. By duality, $(xyz)^\omega \mathcal{L} (xy^2z)^\omega$, and finally $(xyz)^\omega = (xy^2z)^\omega$. Therefore, S satisfies: $(xyz)^\omega = (xy^2z)^\omega = (xy^\omega z)^\omega$, and in particular, for $r \geq 1$: $(xy^r z)^\omega = (x(y^r)^\omega z)^\omega = (xy^\omega z)^\omega = (xyz)^\omega$. Now, since (1) implies (2) by lemma **3.1.3**, one gets:

$$(x_1 x_2 \dots x_n)^\omega = (x_1^\omega x_2^\omega \dots x_n^\omega)^\omega$$

using n times (2) or $(xy^r z)^\omega = (xyz)^\omega$.

Lemma 3.1.5. *The pseudoidentities (2) and aperiodicity imply the pseudoidentities (1). Therefore, $\mathbf{V}' \subseteq \mathbf{V}$.*

Proof. First, the pseudoidentities (2) imply $(x^2y)^\omega = ((x^2)^\omega y^\omega)^\omega = (x^\omega y^\omega)^\omega = (xy)^\omega$. Therefore, the following pseudoidentities are satisfied in \mathbf{V}' :

$$\begin{aligned} (xy)^\omega &= (xy)^\omega xy && \text{by aperiodicity} \\ &= (x^2y)^\omega xy && \text{by (2)} \\ &= x^2y(x^2y)^\omega xy && \text{by aperiodicity} \\ &= x^2y(xy)^\omega xy && \text{by (2)} \\ &= x(xy)^\omega && \text{by aperiodicity} \end{aligned}$$

One proves in the same way that $(xy)^\omega = (xy)^\omega y$. This concludes the proof of lemma **3.1.5** and of proposition **3.1.2**.

Corollary 3.1.6. *The following pseudovarieties are equal:*

$$\llbracket x(xy)^\omega = (xy)^\omega = (xy)^\omega y \rrbracket = \llbracket x^{\omega+1} = x^\omega, \{u^\omega = v^\omega \mid u \equiv_n v\} \rrbracket$$

Proof. One first proves the inclusion from left to right. Aperiodicity follows from (1). Next, the above proof of proposition **3.1.2** shows that \mathbf{V} satisfies the pseudoidentities of the form $(rst)^\omega = (rs^2t)^\omega$ where s denotes a letter and r and t denote either a letter or the empty word. The inclusion from right to left also follows from proposition **3.1.2** and corollary **3.1.6** since $\llbracket \{u^\omega = v^\omega \mid u \equiv_n v\} \rrbracket_{\mathbf{A}} \subseteq \llbracket (x^2y)^\omega = (xy)^\omega = (xy^2)^\omega \rrbracket_{\mathbf{A}} = \mathbf{V}' = \mathbf{V}$.

3.2. Implicit operations of \mathbf{V}

Now, we want to have some information about implicit operations of \mathbf{V} . Notice that although they have a very simple form, we won't find any canonical form ("canonical" means that if two implicit operations for $\mathbf{J} \vee \mathbf{B}$ coincide over \mathbf{J} and over \mathbf{B} , then they have the same canonical form).

Lemma 3.2.1. *The idempotents of $\overline{F}_n(\mathbf{V})$ are of the form u^ω where u is an explicit operation of $F_n(\mathbf{V})$. Furthermore, the idempotent u^ω is determined by the natural projection of u over $F_n(\mathbf{B})$.*

Proof. The second part of this lemma has already been mentioned: if u and v are two words such that $u \equiv_n v$, then \mathbf{V} satisfies the pseudo-identity $u^\omega = v^\omega$ (corollary 3.1.6).

Let now $\pi = \pi^\omega$ in $\overline{F}_n(\mathbf{V})$. The implicit operation π is the limit of a sequence of explicit operations $\pi_k \in F_n(\mathbf{V})$. But $\overline{F}_n(\mathbf{B})$ is a finite semigroup of \mathbf{V} . Therefore, there exists $i \in \mathbb{N}$ such that:

$$\forall k \in \mathbb{N}, k > i \implies \overline{F}_n(\mathbf{B}) \models \pi = \pi_k$$

By the second part of this lemma, π_l^ω and π_k^ω coincide in \mathbf{V} if $l, k \geq i$. Since $\overline{F}_n(\mathbf{B})$ is a finite band, π coincides with an explicit operation u over \mathbf{B} . Thus, the sequence $(\pi_k^\omega)_{k > i}$ is constant, say of value u^ω . By continuity of $\pi \mapsto \pi^\omega$, it follows that $\pi = \pi^\omega = \lim_{n \rightarrow \infty} \pi_n^\omega = u^\omega$.

This lemma provides a nice decomposition of implicit operations of $\overline{F}_n(\mathbf{V})$:

Proposition 3.2.2. *Every implicit operation π of the pseudovariety \mathbf{V} admits a decomposition as a product of the form $\pi_1 \dots \pi_k$ where the π_i are either explicit or of the form u_i^ω with $u_i \in F_n(\mathbf{V})$.*

Proof. It is sufficient to apply theorem 2.2.3, and to notice that in $\overline{F}_n(\mathbf{V})$, the regular elements are idempotent since \mathbf{V} is contained in \mathbf{DA} . The result follows then from the preceding lemma.

In fact, we are trying to have something approximating a canonical form for the implicit operations for \mathbf{V} .

Lemma 3.2.3. *If u and v are two words such that $c(u) \subseteq c(v)$, then \mathbf{V} satisfies $uv^\omega = (uv)^\omega = u^\omega v^\omega$ and $v^\omega u = (vu)^\omega = v^\omega u^\omega$.*

Proof. It suffices to show each of the three following pseudoidentities:

$$x(xy)^\omega = (xy)^\omega, x(yx)^\omega = (xyx)^\omega, x(yxz)^\omega = (xyxz)^\omega$$

and the desired ones follow by induction on the length of u . The first one of these pseudoidentities is straightforward. For the second one, if $S \in \mathbf{V}$ and $x, y \in S$, one can write:

$$\begin{aligned}
(xy x)^\omega &= (xy x)^\omega y x && \text{by (1)} \\
&= (xy x)^\omega (y x)^{\omega-1} && \text{in the same way} \\
&= (xy x)^{\omega-1} (xy)^\omega x \\
&= (xy x)^{\omega-2} xy x (xy)^\omega x \\
&= (xy x)^{\omega-2} xy (xy)^\omega x && \text{by (1)} \\
&= (xy x)^{\omega-2} (xy)^\omega x && \text{by aperiodicity} \\
&= (xy x)^{\omega-3} (xy)^\omega x && \text{in the same way} \\
&= \dots \\
&= (xy)^\omega x \\
&= x (yx)^\omega
\end{aligned}$$

Finally, we have:

$$\begin{aligned}
x(yxz)^\omega &= x(yxzxyxz)^\omega && \text{as } yxz \equiv_3 yxzxyxz \text{ (by 2.1.1)} \\
&= x.yxz x(yxz.x.yxz)^\omega && \text{by (1)} \\
&= x.(yxzx)^\omega (yxzxxyxz)^\omega && \text{in the same way} \\
&= (xyxz)^\omega x(yxz)^\omega \\
&= (xyxz)^\omega xyxz(yxz)^\omega && \text{by aperiodicity} \\
&= (x.yxz)^\omega (yxz)^\omega && \text{by aperiodicity} \\
&= (xyxz)^\omega && \text{by (1)}
\end{aligned}$$

This gives the result.

To shorten the notations, we adopt the following conventions:

(1) Given a finite sequence of words of A_n^* : (u_0, \dots, u_{2k}) , we write $[u, 2k]$ for the implicit operation $\left(\prod_{i=0}^{k-1} u_{2i} u_{2i+1}^\omega\right) u_{2k}$. Frequently, the existence of the sequence (u_0, \dots, u_{2k}) will be understood.

(2) Given two finite sequences of words of A_n^* $(u) = (u_0, \dots, u_{2k})$ and $(v) = (v_0, \dots, v_{2l})$, we say that the pair $((u), (v))$ satisfies:

- \mathcal{P}_0 if $[u, 2k]$ and $[v, 2l]$ satisfy condition \mathfrak{B} . of theorem **2.2.4**.
- \mathcal{P}_1 if $\prod_i u_i \equiv_n \prod_i v_i$.
- \mathcal{P}_2 if $k = l$ and if for every integer i , $0 \leq i \leq k - 1$ implies $c(u_{2i+1}) =$

$c(v_{2i+1})$ and $0 \leq i \leq k$ implies $u_{2i} = v_{2i}$.

• \mathcal{P}_3 if $[u, 2k]$ and $[v, 2l]$ satisfy conditions 4., 5. and 6. of theorem 2.2.4.

The next proposition describes some sets of pseudoidentities defining $\mathbf{J} \vee \mathbf{B}$:

Theorem 3.2.4. *Consider the following sets of pseudoidentities:*

$$\begin{aligned}\Sigma_0^{(n)} &= \left\{ (\pi, \rho) \in \overline{\mathbf{F}}_n(\mathbf{V})^2 \mid \mathbf{J} \models \pi = \rho \text{ and } \mathbf{B} \models \pi = \rho \right\} \\ \Sigma_1^{(n)} &= \left\{ ([u, 2k], [v, 2l]) \in \overline{\mathbf{F}}_n(\mathbf{V})^2 \mid ((u), (v)) \text{ satisfies } \mathcal{P}_0, \mathcal{P}_1 \text{ and } \mathcal{P}_2 \right\} \\ \Sigma_2^{(n)} &= \left\{ ([u, 2k], [v, 2l]) \in \overline{\mathbf{F}}_n(\mathbf{V})^2 \mid ((u), (v)) \text{ satisfies } \mathcal{P}_i, 0 \leq i \leq 3 \right\}\end{aligned}$$

and, for $i = 0, 1, 2$, we set $\Sigma_i = \bigcup_{n \geq 0} \Sigma_i^{(n)}$.

Then, $\mathbf{J} \vee \mathbf{B} = \llbracket \Sigma_0 \rrbracket_{\mathbf{A}} = \llbracket \Sigma_1 \rrbracket_{\mathbf{A}} = \llbracket \Sigma_2 \rrbracket_{\mathbf{A}}$.

Proof. From the inclusions between sets of pseudoidentities $\Sigma_2 \subset \Sigma_1 \subset \Sigma_0$, one deduces the inclusions between pseudovarieties $\llbracket \Sigma_0 \rrbracket_{\mathbf{A}} \subset \llbracket \Sigma_1 \rrbracket_{\mathbf{A}} \subset \llbracket \Sigma_2 \rrbracket_{\mathbf{A}}$.

It remains to show that $\llbracket \Sigma_2 \rrbracket_{\mathbf{A}}$ satisfies Σ_0 . First, $\llbracket \Sigma_2 \rrbracket_{\mathbf{A}}$ satisfies $(x^2y)^\omega = (xy)^\omega = (xy^2)^\omega$. Therefore, it is included in \mathbf{V} by proposition 3.1.2 and for $i = 0, 1, 2$, $\llbracket \Sigma_i \rrbracket_{\mathbf{A}} = \llbracket \Sigma_i \rrbracket_{\mathbf{V}}$. Let then $(\pi, \rho) \in \Sigma_0$. From proposition 3.2.2, each of π and ρ has a factorization as a product of explicit operations and of ω -powers of explicit ones. As $\llbracket \Sigma_2 \rrbracket_{\mathbf{A}} \subseteq \mathbf{V}$, proposition 3.1.2 and lemma 3.2.3 imply that $\llbracket \Sigma_2 \rrbracket_{\mathbf{A}}$ satisfies the pseudoidentities $\pi = \pi'$ and $\rho = \rho'$, where π' (resp. ρ') is obtained from π (resp. from ρ) using, until a reduced element is obtained, the following confluent rewriting rules: $(x_1 \dots x_{k-1} x_k^\omega x_{k+1} \dots x_r)^\omega \longrightarrow (x_1 \dots x_r)^\omega$, and if $c(u) \subseteq c(v)$, $v^\omega u^\omega \longrightarrow (vu)^\omega$, $u^\omega v^\omega \longrightarrow (uv)^\omega$, $v^\omega u \longrightarrow (vu)^\omega$ and $uv^\omega \longrightarrow (uv)^\omega$. In fact, π and ρ have been replaced by two implicit operations of the form $\pi' = [u, 2p]$ and $\rho' = [v, 2q]$ such that $((u), (v))$ satisfies the conditions of \mathcal{P}_3 . As \mathbf{J} satisfies by hypothesis $\pi = \rho$, and as the two members of every rewriting rule are equal in $\overline{\mathbf{F}}_n(\mathbf{J})$, \mathbf{J} satisfies $\pi' = \rho'$ too. From theorem 2.2.4, it follows that $((u), (v))$ satisfies also \mathcal{P}_2 . Therefore, $(\pi', \rho') \in \Sigma_2$, and Σ_2 satisfies finally $\pi = \pi' = \rho' = \rho$.

We can now show that $\mathbf{V} \neq \mathbf{J} \vee \mathbf{B}$:

Proposition 3.2.5. *The inclusion $\mathbf{J} \vee \mathbf{B} \subset \mathbf{V}$ is strict.*

Proof. It suffices to find a semigroup of \mathbf{V} that doesn't satisfy a pseudoidentity of $\mathbf{J} \vee \mathbf{B}$. Consider the pseudoidentity

$$xyz(xy)^\omega zyx = xyz(yx)^\omega zyx$$

It is clear that it is satisfied by $\mathbf{J} \vee \mathbf{B}$.

Let S be the transition monoid of the following automaton:

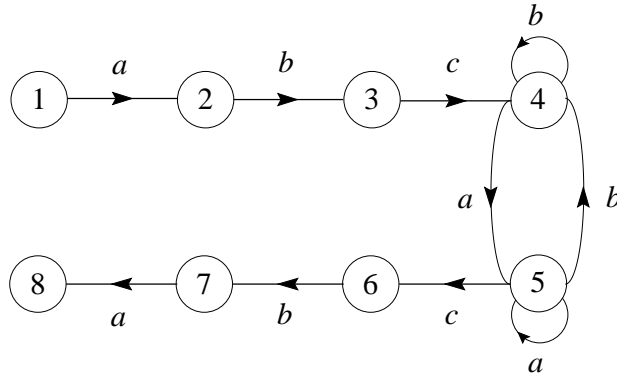


Figure 3.2.1. The automaton \mathcal{A}

Then $S \in \mathbf{V}$ and $S \notin \mathbf{J} \vee \mathbf{B}$.

Let us call *exponent* of a finite semigroup the smallest integer k such that s^k is idempotent for every element s of the semigroup.

First, S is aperiodic of exponent 3. Indeed, its exponent cannot be less than 3 since $3 \cdot (cba)^2 \neq 3 \cdot (cba)^3$. As a, b and c generate S , it suffices to check that $q \cdot u^3 = q \cdot u^4$ for every word $u \in \{a, b, c\}^+$ and for every state q . If u contains the letter c , then $q \cdot u^3$ and $q \cdot u^4$ are undefined for every state q since u^3 and u^4 contain at least three occurrences of the letter c and there is no such path that stays in \mathcal{A} . If $u \in \{a, b\}^+$, $q \cdot u^3$ and $q \cdot u^4$ are again undefined for $q \in \{1, 2, 3, 6, 7, 8\}$, since u^3 and u^4 are of length at least 3 and one cannot read from these states a word of length at least 3 over $\{a, b\}$. It remains to see that $q \cdot u^3 = q \cdot u^4$ for $q \in \{4, 5\}$ and $u \in \{a, b\}^+$, but this is immediate because the final state only depends of the last letter of u . In the sequel, we write $q \cdot u^\omega$ instead of $q \cdot u^3$.

It is easy to see that $S \notin \mathbf{J} \vee \mathbf{B}$, since precisely S doesn't satisfy the pseudoidentity $xyz(xy)^\omega zyx = xyz(yx)^\omega zyx$. Indeed, $1 \cdot abc(ab)^\omega cab$ is not defined when $1 \cdot abc(ba)^\omega cab = 8$.

Let us check that the pseudoidentities $x(xy)^\omega = (xy)^\omega = (xy)^\omega y$ hold in S . Again, it suffices to check the equality $q \cdot [u(uv)^\omega] = q \cdot [(uv)^\omega] = q \cdot [(uv)^\omega v]$ for all words u and v constructed over the three letters a , b , and c and for every state q of the preceding automaton. Since there is no cycle with the letter c in the automaton, if c appears in u or v , then $q \cdot [u(uv)^\omega]$, $q \cdot [(uv)^\omega]$ and $q \cdot [(uv)^\omega v]$ are both undefined since c appears in uv . Assume now that c doesn't appear in uv . In this case, if $q \in \{1, 2, 3, 6, 7, 8\}$, then $q \cdot [u(uv)^\omega]$, $q \cdot [(uv)^\omega]$ and $q \cdot [(uv)^\omega v]$ are once again undefined. Indeed, from one of the states $\{6, 7, 8\}$, one cannot read in \mathcal{A} a word with more than three letters; from one of the states $\{1, 2, 3\}$, the words with more than three letters that one can read staying in \mathcal{A} have to contain the letter c , to have access to the cycle of \mathcal{A} .

It remains to treat the case $q \in \{4, 5\}$, $u, v \in \{a, b\}^*$. But for every word $w \in \{a, b\}^*$ and $q \in \{4, 5\}$, $q \cdot w$ stays in $\{4, 5\}$. Therefore we have to show that the syntactic semigroup of the automaton deduced from \mathcal{A} by keeping only the states 4 and 5 is in \mathbf{V} . But this syntactic semigroup only contains the elements 1, a and b which are both idempotents. Thus, it is in \mathbf{B} , and therefore in \mathbf{V} .

Remark This proves once again that $\mathbf{J} \vee \mathbf{B}$ is a strict pseudovariety of \mathbf{DA} by giving a semigroup that separates \mathbf{DA} and $\mathbf{J} \vee \mathbf{B}$ (this semigroup contains 28 elements).

3.3. The pseudovariety $\mathbf{J} \vee \mathbf{B}$ is decidable

This section is devoted to the proof of the decidability of $\mathbf{J} \vee \mathbf{B}$.

If a recognizable subset R of a semigroup S is recognized by (M, η, P) , where M is a finite semigroup, $\eta : S \rightarrow M$ a morphism and P a subset of M such that $\eta^{-1}(P) = R$, then (M, η, P) will be called a recognizing triple, the recognized subset R as well as the semigroup S being sometimes understood.

The idea of the proof is roughly the following: a semigroup has to be aperiodic to belong to $\mathbf{J} \vee \mathbf{B}$, and that is easy to check. The other pseudoidentities to verify are, for instance, those of the set Σ_1 of theorem 3.2.4. The number of such pseudoidentities is infinite. However, one can prove the decidability using some arguments explained by Berstel in [18]. More precisely, one can:

a) reduce the problem to the membership to a pseudovariety given by a set of *identities* in a *finite number of variables*, and then find an effective algorithm that furnishes a rational expression of this set of identities.

b) find an algorithm whose input is a finite semigroup S and an integer m and whose output is a semigroup M , a morphism $\varphi : A_m^* \times A_m^* \longrightarrow M$ and a subset P of M recognizing exactly the set of all identities in m variables or less satisfied by S .

c) show that given a rational expression $\Gamma \subseteq X^* \times Y^*$ where X and Y are finite alphabets, and a set Θ of identities recognized by a given semigroup M , a given morphism $\varphi : A_m^* \times A_m^* \longrightarrow M$ and a given subset P of M , there exists an effective algorithm to decide whether Θ contains Γ .

Then, one gets the desired algorithm: to decide whether S belongs to $\mathbf{J} \vee \mathbf{B}$, it suffices to see whether the set of identities given as output of the second algorithm contains the one described by the rational expression given as output of the first algorithm.

Point c) being used in the proof of point a), we will show c), then b), and finally a).

We begin by a straightforward lemma that proves in particular that \mathbf{A} is decidable:

Lemma 3.3.1. *There exists an algorithm whose input is*

- (1) *a finite semigroup S .*
- (2) *a finite set Σ of pseudoidentities, each of them having its members described by an expression built from letters of A_n using a finite number of times the concatenation and the operation $x \mapsto x^\omega$.*

and whose output is 1 if S is in the pseudovariety $[[\Sigma]]$ and 0 otherwise. In particular, \mathbf{A} is decidable.

Proof. For every $s \in S$, s^{n_S} is idempotent where n_S is the exponent of S . One can therefore formally replace ω by n_S , that one can compute, in every pseudoidentity of Σ . Thus, we obtain a finite set of identities Σ' such that $S \in [[\Sigma]] \Leftrightarrow S \in [[\Sigma']]$, and the problem is reduced to the membership problem for a finitely based equational pseudovariety (that is, a pseudovariety defined by *identities*), which is well known to be decidable.

We can now begin the proof of point c):

Lemma 3.3.2. *Let X and Y be two finite disjoint alphabets. There exists an algorithm whose input is*

- (1) *a rational expression of a subset Γ of $X^* \times Y^*$.*
- (2) *a triple (M, η, P) where M is a semigroup, η a morphism of $X^* \times Y^*$ in M and P a subset of M recognizing a subset Θ of $X^* \times Y^*$.*

and whose output is a rational expression of $\Gamma \cap \Theta$. In particular, one can compute effectively a rational expression for such a recognizable subset Θ , and one can decide whether $\Gamma \cap \Theta = \emptyset$ and whether $\Gamma \subseteq \Theta$.

Proof. Let Z be $X \cup Y$ and $\varphi : Z^* \rightarrow X^* \times Y^*$ the morphism defined over Z by:

$$\varphi(z) = \begin{cases} (z, 1) & \text{if } z \in X \\ (1, z) & \text{if } z \in Y \end{cases}$$

Note that for every $C, D \subseteq Z^*$:

$$\varphi(C \cup D) = \varphi(C) \cup \varphi(D), \quad \varphi(C \cdot D) = \varphi(C) \cdot \varphi(D), \quad \varphi(C^*) = (\varphi(C))^*$$

- One can compute a rational subset G of Z^* such that $\varphi(G) = \Gamma$. Indeed, if $\Gamma = \{(x, y)\}$, choose $G = \{xy\}$; if $\Gamma = \Lambda \cup \Delta$, the preceding remark shows that if C and D are found such that $\varphi(C) = \Lambda$, $\varphi(D) = \Delta$, then one can choose $G = C \cup D$. In the same way, if $\Gamma = \Lambda \cdot \Delta$, take $G = C \cdot D$. Finally, if $\Gamma = \Lambda^*$, choose $G = C^*$.

- One can compute a rational expression for $\varphi^{-1}(\Theta) = (\eta \circ \varphi)^{-1}(P)$. To do this, just build the automaton whose set of states is M , whose initial state is 1 and whose final states is P , the transitions being given by $m \cdot z = m(\eta \circ \varphi(z))$. Therefore, one can compute a rational expression for $G \cap \varphi^{-1}(\Theta)$, by building once again the automaton for instance.

- Since $\varphi(G \cap \varphi^{-1}(\Theta)) = \Gamma \cap \Theta$, one can find an algorithm that gives a rational expression for $\Gamma \cap \Theta$. Indeed, let $E = G \cap \varphi^{-1}(\Theta)$. If $E = \{z\}$, one chooses $\{(z_X, z_Y)\}$ as rational expression for $\varphi(E)$, where z_X and z_Y are the projections of z over X^* and Y^* respectively. In the same way, by the former remark, if E is of the form $K \cup L$, and if one can find a rational expression for $\varphi(K)$ and $\varphi(L)$, one will choose $\varphi(K) \cup \varphi(L)$ as a rational expression for $\varphi(E)$. If $E = K \cdot L$, one will take $\varphi(E) = \varphi(K) \cdot \varphi(L)$, and finally if $E = K^*$, one will choose $\varphi(E) = (\varphi(K))^*$.

In particular, since a rational expression of $X^* \times Y^*$ is known, namely $(\bigcup_X (x, 1))^* \cdot (\bigcup_Y (1, y))^*$, we are able to compute effectively a rational

expression for $\Theta = \Theta \cap (X^* \times Y^*)$. Moreover, one can decide whether a rational subset of $X^* \times Y^*$ is empty or not given a rational expression that describes it. One can therefore decide whether $\Gamma \cap \Theta$ is empty. Finally, $\Gamma \subseteq \Theta$ is equivalent to $\Gamma \cap \Theta^c = \emptyset$. But, given a triple (M, η, P) recognizing Θ , the triple (M, η, P^c) recognizes Θ^c , and one can apply the preceding result to conclude.

The proof of c) being finished, we prove b). The following lemma says that one can effectively compute a recognizing triple for the set of identities in a finite given number of variables satisfied by a finite semigroup.

Lemma 3.3.3. *For every semigroup S and every integer m , let us call $\Sigma_m(S)$ the set*

$$\{(u, v) \in A_m^* \times A_m^* \mid \text{for every morphism } \varphi : A_m^* \longrightarrow S, u\varphi = v\varphi\}$$

of all identities in at most m variables satisfied by S . Then, there exists an algorithm whose input is:

- (1) *a finite semigroup S .*
- (2) *an integer $m \in \mathbb{N}$.*

and whose output is a triple (M, φ, P) recognizing $\Sigma_m(S)$.

Proof. By definition, one can write $\Sigma_m(S) = \bigcap_{\varphi: A_m^* \longrightarrow S} \varphi^{-1}(\Delta)$ with $\Delta = \{(x, x) \mid x \in S\}$. Now, there is a finite number of morphisms of A_m^* in S and one can compute them by giving the images of letters. As $S \times S$ is finite, one can compute effectively a recognizing triple for every $\varphi^{-1}(\Delta)$. But if the sets E_i , $i = 1, \dots, k$, are recognized by (M_i, η_i, P_i) , then their intersection is recognized by $(\prod_i M_i, (\eta_1 \times \dots \times \eta_k), \prod_i P_i)$.

The next lemma says that to check whether a semigroup S is in a given equational pseudovariety, it suffices to check that it satisfies every identity in $|S|$ variables of the pseudovariety (a more general result is that the membership of a semigroup S to a pseudovariety can be tested by checking every pseudoidentity in $|S|$ variables only).

Lemma 3.3.4. *Let Σ be a set of identities. Let*

$$\Sigma^{(|S|)} = \{(u\varphi, v\varphi) \in A_p^* \times A_p^* \mid \text{there exist } n, p, p \leq |S|, p \leq n, \text{ and } \varphi : A_n^* \rightarrow A_p^* \text{ semigroup morphism such that } (u, v) \in \Sigma \cap A_n^* \times A_n^*\}$$

Then, $S \in \llbracket \Sigma \rrbracket$ if and only if $S \in \llbracket \Sigma^{(|S|)} \rrbracket$.

Proof. The implication from left to right is clear because the identities of $\Sigma^{(|S|)}$ are deduced from those of Σ by semigroup morphism. Let then S be a semigroup that satisfies $\Sigma^{(|S|)}$. Taking $n = p \leq |S|$ and the identity for φ , one sees that S satisfies every identity of Σ with less than $|S|$ variables. Let $(u, v) \in \Sigma \cap A_n^* \times A_n^*$, with $n > |S|$. One has to show that if $s_i, i = 1, \dots, n$ are in S , then $u_S(s_1, \dots, s_n) = v_S(s_1, \dots, s_n)$. Let p be the number of distinct s_i . Thus, $p \leq n$. It suffices then to choose a morphism $\varphi : A_n^* \rightarrow A_p^*$ such that $\varphi(x_i) = s_i$, and this is possible. As $S \in \Sigma^{(|S|)}$, S satisfies $u_S(\varphi(x_1), \dots, \varphi(x_n)) = v_S(\varphi(x_1), \dots, \varphi(x_n))$ and therefore, $u_S(s_1, \dots, s_n) = v_S(s_1, \dots, s_n)$.

We can now prove a).

Notation For a semigroup S whose cardinality is $|S|$ and whose exponent is $\exp(S)$, we set $n_S = \text{lcm}(|S|, \exp(S))$. Furthermore, for $n, N \in \mathbb{N}$, we denote by $\Sigma_{1,N}^{(n)}$ the set of identities of the form $(u, v) \in A_n^{*2}$ with

$$u = \left(\prod_{i=0}^{k-1} u_{2i}(u_{2i+1,1} \dots u_{2i+1,N}) \right) \cdot u_{2k}$$

$$v = \left(\prod_{i=0}^{k-1} v_{2i}(v_{2i+1,1} \dots v_{2i+1,N}) \right) \cdot v_{2k}$$

such that

- (4) if $0 \leq i \leq k$, then $u_{2i} \neq 1 \neq v_{2i}$.
- (5) if $0 \leq i \leq k$, then $u_{2i} = v_{2i}$.
- (6) if $0 \leq r \leq k-1$ and $1 \leq i, j \leq N$, then $c(u_{2r+1,i}) = c(v_{2r+1,j})$.
- (7) $u \equiv_n v$.

Let us begin by an elementary and very classical lemma:

Lemma 3.3.5. *Let S be a finite semigroup of cardinality n and $a_1, \dots, a_n \in S$. Then, there exists a non empty factor $a_i \dots a_j$ of $a_1 \dots a_n$ such that $a_1 \dots a_n = a_1 \dots a_{i-1} (a_i \dots a_j)^2 a_{j+1} \dots a_n$.*

Proof. Just notice that either there exist i and j such that $i \leq j$ and

$$a_1 \dots a_{i-1} = a_1 \dots a_j = a_1 \dots a_{i-1} (a_i \dots a_j) = a_1 \dots a_{i-1} (a_i \dots a_j)^2$$

or the n prefixes $a_1 \dots a_i$, $1 \leq i \leq n$ are pairwise distinct. The first case immediately leads to the desired result, when in the second case, one of the $a_1 \dots a_i$ is idempotent. This gives again the result.

Lemma 3.3.6. *Let S be a semigroup of cardinality at least 2. Then,*

$$S \in \mathbf{J} \vee \mathbf{B} \iff S \models \Sigma_{1,n_S}^{(|S|)} \text{ and } S \in \mathbf{A}$$

Proof. Assume S in $\mathbf{J} \vee \mathbf{B}$, let (u, v) be an identity of $\Sigma_{1,n_S}^{(|S|)}$ and φ a morphism from $A_{|S|}^*$ into S . Let us show that $\varphi(u) = \varphi(v)$. One writes

$$\begin{aligned} \varphi(u) &= \left(\prod_{i=0}^{k-1} \varphi(u_{2i}) \varphi(u_{2i+1,1} \dots u_{2i+1,n_S}) \right) \cdot \varphi(u_{2k}) \\ \varphi(v) &= \left(\prod_{i=0}^{k-1} \varphi(v_{2i}) \varphi(v_{2i+1,1} \dots v_{2i+1,n_S}) \right) \cdot \varphi(v_{2k}) \end{aligned}$$

By lemma 3.3.5, there exist for every $0 \leq i \leq k-1$ some integers m_i, m'_i, n_i and n'_i such that

$$\begin{aligned} \varphi(u_{2i+1,1} \dots u_{2i+1,n_S}) &= \varphi(u_{2i+1,1} \dots (u_{2i+1,m_i} \dots u_{2i+1,m'_i})^\omega \dots u_{2i+1,n_S}) \\ \varphi(v_{2i+1,1} \dots v_{2i+1,n_S}) &= \varphi(v_{2i+1,1} \dots (v_{2i+1,n_i} \dots v_{2i+1,n'_i})^\omega \dots v_{2i+1,n_S}) \end{aligned}$$

But since S lies in $\mathbf{J} \vee \mathbf{B}$, it satisfies in particular the pseudoidentity (π, ρ) where π (resp. ρ) is obtained from of u (resp. of v) by changing $u_{2i+1,m_i} \dots u_{2i+1,m'_i}$ by $(u_{2i+1,m_i} \dots u_{2i+1,m'_i})^\omega$ (resp. $v_{2i+1,n_i} \dots v_{2i+1,n'_i}$ by $(v_{2i+1,n_i} \dots v_{2i+1,n'_i})^\omega$). That is to say $\varphi(u) = \varphi(v)$.

Conversely, if S is an aperiodic semigroup of cardinality at least 2 of $\llbracket \Sigma_{1,n_S}^{(|S|)} \rrbracket$, S satisfies in particular $(x^2y)^\omega = (x^2y)^{n_S} = (xy)^{n_S} = (xy^2)^{n_S} = (xy^2)^\omega$, hence S is in \mathbf{V} . Moreover, S satisfies also every identity of $\Sigma_{1,n_S}^{(|S|)}$ in which one takes $u_{2r+1,i} = u_{2r+1,j}$ and $v_{2r+1,i} = v_{2r+1,j}$ for every $(i, j) \in [1, N]^2$. Since n_S divides the exponent of S , S satisfies all the pseudoidentities of $\Sigma_1^{(|S|)}$, and $S \in \llbracket \Sigma_1 \rrbracket$ by lemma 3.3.4. The theorem 3.2.4 implies then $S \in \mathbf{J} \vee \mathbf{B}$.

Lemma 3.3.7. *There exists an algorithm taking two integers N and n as input and whose output is a rational expression of $\Sigma_{1,N}^{(n)}$.*

Proof. Let

$$\begin{aligned}\Delta_n &= \{(u, u) \mid u \in A_n^+\} \\ \Delta_{F_n(\mathbf{S1})} &= \{(u, u) \mid u \in F_n(\mathbf{S1})\} \\ \Delta_{F_n(\mathbf{B})} &= \{(u, u) \mid u \in F_n(\mathbf{B})\}\end{aligned}$$

and β the canonical morphism of A_n^+ in $F_n(\mathbf{B})$. Thus, one can summarize the conditions (4) to (7) that $\Sigma_{1,N}^{(n)}$ has to verify as follows:

$$\Sigma_{1,N}^{(n)} = (\Delta_n \cdot (c^{-1}(\Delta_{F_n(\mathbf{S1})}))^N)^* \Delta_n \cap \beta^{-1}(\Delta_{F_n(\mathbf{B})})$$

Now, we know a rational expression of $\Delta_n = (\bigcup_{x \in A_n} (x, x))^*$. Furthermore, the sets $\Delta_{F_n(\mathbf{S1})}$ and $\Delta_{F_n(\mathbf{B})}$ are finite and we are able to enumerate them (using the word problem for the free band). Therefore, one knows a triple recognizing $c^{-1}(\Delta_{F_n(\mathbf{S1})})$ and another one recognizing $\beta^{-1}(\Delta_{F_n(\mathbf{B})})$. By lemma 3.3.2, there exists an effective algorithm to compute a rational expression for $(c^{-1}(\Delta_{F_n(\mathbf{S1})}))^N$, and finally for $\Sigma_{1,N}^{(n)}$.

We conclude the proof of the main theorem:

Proof of 3.1: if the cardinality of S is 1, the problem is trivial. Otherwise, one checks whether S is aperiodic, and that is decidable by lemma 3.3.1. If S is not aperiodic, it is not in $\mathbf{J} \vee \mathbf{B}$. Otherwise, it suffices to check by lemma 3.3.6 that it is in $\llbracket \Sigma_{1,n_S}^{(|S|)} \rrbracket$. Therefore, one has to see whether $\Sigma_{1,n_S}^{(|S|)} \subseteq \Sigma_{|S|}(S)$. But lemma 3.3.3 gives an effective algorithm to compute a triple (M, φ, P) recognizing $\Sigma_{|S|}(S)$, and the last lemma gives a rational expression for $\Sigma_{1,n_S}^{(|S|)}$. The conclusion follows from lemma 3.3.2.

Acknowledgments

I am grateful to Jean-Éric Pin who read many times the manuscript and made many valuable comments, and to Jorge Almeida and Pascal Weil for the attention they paid to this work and for their patient explanations and constructive remarks.

References

1. Albert D., Baldinger R., Rhodes J., *Undecidability of the identity problem for finite semigroups*, J. Symbolic Logic, **57,1**, (1992), pp 179-192.
2. Almeida J., *Semigrupos Finitos e Álgebra Universal*, Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, (1992).
3. _____, *Finite Semigroups and Universal Algebra (english trans.)*, (to appear).
4. _____, *Power pseudovarieties of semigroups I*, Semigroup Forum, **33**, (1986), pp 357-373.
5. _____, *Power pseudovarieties of semigroups II*, Semigroup Forum, **33**, (1986), pp 375-390.
6. _____, *Some pseudovariety joins involving the pseudovariety of finite groups*, Semigroup Forum, **37**, (1988), pp 53-57.
7. _____, *The algebra of implicit operations*, Algebra Universalis, **26**, (1989), pp 16-32.
8. _____, *Equations for pseudovarieties*, in J.E. Pin (Ed.) *Formal properties of Finite Automata and Applications*, Springer, Berlin, Lect. Notes in Computer Science, **386**, (1989), pp 148-164.
9. _____, *On pseudovarieties, varieties of languages, filters of congruences, pseudoidentities and related topics*, Algebra Universalis, **27**, (1990), pp 333-350.
10. _____, *Implicit operations on finite \mathcal{J} -trivial semigroups and a conjecture of I. Simon*, J. Pure and Applied Algebra, **69**, (1990), pp 205-218.
11. Almeida J., Azevedo A., *The join of the pseudovarieties of \mathcal{R} -trivial and \mathcal{L} -trivial monoids*, J. Pure and Applied Algebra, **60**, (1989), pp 129-137.
12. _____, *On regular implicit operations*, (to appear in *Portugaliæ Mathematica*).

13. Almeida J., Weil P., *Reduced factorisations in free profinite groups and join decomposition of pseudovarieties*, Int. J. Algebra and Computation, (to appear).
14. _____, *Relatively free profinite monoids: an introduction and examples*, in J.B. Fountain and V.A.R. Gould (Eds.), Semigroups, Formal Languages and Groups, (to appear).
15. Azevedo A., *The join of the pseudovariety \mathbf{J} with permutative pseudovarieties*, in J. Almeida et al (Eds.) Lattices, Semigroups and Universal Algebra, Plenum, London, (1990).
16. _____, *Operações Implícitas sobre Pseudovariiedades de Semigrupos. Aplicações*, Universidade do Porto, Doctoral dissertation, (1989).
17. _____, *Operações que preservam homomorfismos sobre a classe de semigrupos finitos \mathbf{DS}* , Universidade do Porto, Acta do II Encontro de Algebristas Portugueses, (1987), pp 33-34.
18. Berstel J., *Transductions and Context-Free Languages*, B.G. Teubner, Stuttgart, (1979).
19. Bourbaki N., *Éléments de mathématiques*, Hermann, Paris, Topologie générale, **I-IV**, (1971).
20. Burris S., Sankappanavar H.P., *A Course in Universal Algebra*, Springer, Berlin, (1981).
21. Eilenberg S., *Automata, Languages and Machines*, Academic Press, New York, **A** :1974, **B** :1976.
22. Henckell K., Margolis S.W., Pin J.E., Rhodes J., *Ash's type II theorem, profinite topology and Malcev products, Part I*, International Journal of Algebra and Computation, **I-4**, (1991), pp 411-436.
23. Howie J.M., *An Introduction to Semigroup Theory*, Academic Press, London, (1976).
24. Kharlampovich O.G., Sapir M., *Algorithmic Problems in Varieties*, (to appear).
25. Lothaire M., *Combinatorics on Words, Encyclopedia of Mathematics*, Addison Wesley, Reading, MA, **17**, (1983).

26. Pin J.E., *Varieties of Formal Languages (english trans.)*, Plenum, London, (1986).
27. ———, *Power semigroups and related varieties of finite semigroups in* S. Goberstein and P.M. Higgins (Eds.), *Proc. Chico Conf.*, D. Reidel, Semigroups and their applications, (1987), pp 139-152.
28. Reiterman J., *The Birkhoff theorem for finite algebras*, Algebra Universalis, **14**, (1982), pp 1-10.
29. Rhodes J., *New techniques in global semigroup theory in* S. Goberstein and P.M. Higgins (Eds.), *Proc. Chico Conf.*, D. Reidel, Semigroups and their applications, (1987), pp 25-35.
30. Simon I., *Piecewise testable events*, Springer, Proc. 2nd GI Conf., Lect. Notes in Comp. Sci., (1975), pp 214-222.
31. Weil P., *Implicit operations on pseudovarieties: an introduction*, in J. Rhodes (Ed.), World Scientific, Singapore, Semigroups and Monoids and Applications, (1991).
32. Zeitoun M., *Opérations Implicites et Variétés de Semigroupes Finis*, Université Paris 7, Thèse, (1993).
33. ———, *A simple example of a non-finitely based semigroup variety*, (to appear).