On bases of identities for the ω-variety generated by locally testable semigroups [1]

José Carlos Costa [a,2,3], Conceição Nogueira [b]

[a] *Centro de Matemática, Universidade do Minho, Portugal.*

[b] *Dep. Matemática, Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria, Portugal.*

Abstract

In this paper, we exhibit an infinite basis of ω-identities for the ω-variety generated by the pseudovariety LSI, of semigroups which are locally semilattices, and we show that this ω-variety is not finitely based.

Key words: Semigroup, pseudovariety, locally testable, omega-term, word problem, identity basis.

1 Introduction

This paper is concerned with a problem involving the pseudovariety LSI of all finite semigroups which are locally semilattices, that is, semigroups S such that eSe is an idempotent and commutative semigroup for all idempotents $e \in S$. This pseudovariety corresponds, in Eilenberg's correspondence, to the well known variety of locally testable languages, as shown independently by Brzozowski and Simon [5] and McNaughton [9]. Recall that a language L is *locally testable* if membership of a given word u in L can be decided by considering the factors of a fixed length k of u and its prefix and suffix of length

[1] Both authors acknowledge partial support by the FCT project PTDC/MAT/65481/2006, which is funded in part by the European Community Fund FEDER.

[2] Partial support by FCT, through the *Centro de Matemática da Universidade do Minho*, is also gratefully acknowledged.

[3] Corresponding author. Centro de Matemática, Universidade do Minho, Campus de Gualtar, 4700-320 Braga, Portugal.

Email addresses: jcosta@math.uminho.pt, conceicao.nogueira@estg.ipleiria.pt

$k-1$. In terms of automata, this corresponds to finite automata equipped with a "sliding" window of size k through which the word is scanned. This special kind of automata, called *scanners*, is considered as a model for computations that require only "local" information. The concept of locally testable semigroup is similar and was introduced by Zalcstein in [10]. A semigroup S is *locally testable* if there is a positive integer k such that, whenever two words over the alphabet S have the same factors of length k and the same prefix and suffix of length $k-1$, the products in S determined by these words are equal. Also in [10], Zalcstein proved that a language is locally testable if and only if its syntactic semigroup is locally testable. So, the class of locally testable semigroups is precisely the pseudovariety LSl.

An ω-term is a term obtained from letters of an alphabet A using the binary concatenation, $(x, y) \mapsto x \cdot y$, and the unary ω-power, $x \mapsto x^\omega$. An ω-semigroup is an algebra over the signature $\{\_ \cdot \_, \_^\omega\}$. Each finite semigroup has a natural interpretation as an ω-semigroup, by interpreting concatenation as the semigroup multiplication and s^ω as the unique idempotent of the subsemigroup generated by s. For a pseudovariety V, let V^ω be the variety of ω-semigroups generated by V. The free ω-semigroup generated by A in the variety V^ω is denoted by $\Omega_A^\omega \mathsf{V}$ and its elements are called ω-terms over V. In [3], Almeida and Steinberg showed that detailed knowledge of these ω-semigroups is sufficient to get important results about V.

An ω-identity is a formal equality $u = v$ of ω-terms. By Birkhoff's theorem, the variety V^ω is defined by ω-identities. The problem of finding a basis of ω-identities for V^ω (and so for $\Omega_A^\omega \mathsf{V}$) has received some attention lately, since it is intimately connected with the ω-word problem for V, that is, the problem of determining whether two ω-terms represent the same element of $\Omega_A^\omega \mathsf{V}$. The case of the pseudovariety J of all $\mathcal{J}$-trivial semigroups, solved by Almeida in [1], constitutes an important example. Another remarkable example, which plays an important role on the Krohn-Rhodes complexity problem, is given by the pseudovariety A of all aperiodic semigroups. A basis for A^ω was discovered by McCammond [8]. More recently, Almeida and Zeitoun [4] found a basis for R^ω, where R is the pseudovariety of $\mathcal{R}$-trivial semigroups. In this paper, we exhibit a basis of ω-identities for LSl^ω. Although this basis is not used to solve the ω-word problem for LSl, which was already described by the first author in [6], the work presented here throws a new light on the subject.

The results obtained in this paper are mainly combinatorial. We describe a normal form for ω-terms of rank 1, which is close to that given by McCammond [8] for A. Contrary to the case of A, this normal form is not unique for LSl in general. However, which is not totally surprising in view of the definition of locally testable languages and semigroups, the equality of two such terms depends only on the equality of their prefixes and suffixes involving a unique ω-power and on the equality of the factors involving two ω-powers (which we

call 2-factors). So, the techniques involved in the proofs are designed to deal with the combinatorics on these 2-factors.

2 Preliminaries

In this section, we briefly recall notation and basic definitions and results. For general background about combinatorics on words and pseudovarieties of semigroups, the reader is referred to [7,2].

2.1 Words

Throughout this paper, A denotes a finite non-empty set, called an *alphabet*. The free semigroup (resp. the free monoid) generated by A is denoted by A^+ (resp. by A^*). The length of a word $w \in A^*$ is denoted by $|w|$. The empty word is denoted by 1. A word $w \in A^*$ is a *prefix* (resp. a *suffix*, a *factor*) of a word $z \in A^*$ if there exist words $x, y \in A^*$ such that $z = wy$ (resp. $z = xw$, $z = xwy$).

The following result is known as Fine and Wilf's Theorem (see [7]).

Proposition 2.1 *Let $u, v \in A^+$. If two powers u^k and v^n of u and v have a common prefix (resp. suffix) of length at least $|u| + |v| - gcd(|u|, |v|)$, then u and v are powers of the same word.*

A word $w \in A^+$ is said to be *primitive* if it is not a power of another word; that is, if $w = u^n$ for some $u \in A^+$ and $n \geq 1$, then $w = u$ (and $n = 1$). Two words w and z are said to be *conjugate* if there exist words $u, v \in A^*$ such that $w = uv$ and $z = vu$. We notice that, if w is a primitive word and z is a conjugate of w, then z is also primitive. Let a total order be fixed for the letters of the alphabet A. A *Lyndon word* is a primitive word which is minimal, with respect to the lexicographic ordering, in its conjugation class.

2.2 Pseudovarieties, ω-terms and ω-identities

A semigroup *pseudovariety* is a class V of finite semigroups closed under taking subsemigroups, homomorphic images and finite direct products. We denote by S the pseudovariety of all finite semigroups.

The variety V^ω is the Birkhoff variety generated by all structures $(S, \_ \cdot \_, \_^\omega)$, where $(S, \_ \cdot \_)$ is a finite semigroup of V and where s^ω is interpreted as the

only idempotent power of $s \in S$. For a given alphabet A, we denote by $\Omega_A^\omega \mathsf{V}$ the V-free ω-semigroup over A. Elements of $\Omega_A^\omega \mathsf{V}$ are called ω-terms over V.

An ω-identity is a pair (u, v) of ω-terms over S, and is usually denoted by $u = v$. A finite semigroup S *satisfies* an ω-identity $\pi = \rho$ if, for every homomorphism $\varphi : \Omega_A^\omega \mathsf{S} \longrightarrow S$, $\varphi(\pi) = \varphi(\rho)$. A class C of finite semigroups *satisfies* an ω-identity $\pi = \rho$, and we write $C \models \pi = \rho$, if every element of C satisfies it. It is well known that LSl is *defined* by the two ω-identities $x^\omega y x^\omega y x^\omega = x^\omega y x^\omega$ and $x^\omega y x^\omega z x^\omega = x^\omega z x^\omega y x^\omega$, in the sense that LSl is the class of all finite semigroups that satisfy these ω-identities. Notice also that A is defined by $x^\omega = x^\omega x = x x^\omega$, and that LSl is a subpseudovariety of A.

3 The ω-word problem for LSl

In this section we briefly recall the solution of the ω-word problem for LSl obtained by the first author [6].

A term of rank 0 is an ω-term not involving the ω-power. A term of rank 1 is an ω-term π of the form

$$\pi = u_0 x_1^\omega u_1 x_2^\omega \cdots x_n^\omega u_n \tag{3.1}$$

with $n \geq 1$, $u_0, \ldots, u_n \in A^*$ and $x_1, \ldots, x_n \in A^+$. For an integer $1 \leq \ell \leq n$, an *ℓ-factor* of π is any subterm of π of the type

$$\pi(i, i+\ell-1) = x_i^\omega u_i x_{i+1}^\omega \cdots x_{i+\ell-1}^\omega$$

with $i + \ell - 1 \leq n$. We denote by $F_\ell(\pi)$ the set of ℓ-factors of π.

Definition 3.1 (normal ω-term) *A* normal *ω-term is a rank 1 term of the form* (3.1) *where:*

(1) each x_i is a Lyndon word;
(2) x_1 is not a suffix of u_0;
(3) x_n is not a prefix of u_n;
(4) if $x^\omega y x^\omega$ is a 2-factor of π, then $x^\omega y x^\omega$ has exactly one occurrence in π;
(5) each 2-factor $x^\omega u y^\omega$ of π verifies the three following conditions:
  (a) u is not a prefix of x^j for any integer j;
  (b) u is not a suffix of y^j for any integer j;
  (c) if $u = x^j u'$ or $u = u' y^j$ for some integer $j \geq 1$, then $x^\omega u' y^\omega$ fails at least (a) or (b).

We notice that this normal form for 2-factors was defined by McCammond in [8]. His construction of these normal forms is used in the fifth step of the proof of Theorem 4.3 below.

We will be particularly interested in normal ω-terms of the form

$$\pi = x_1^\omega u_1 x_2^\omega \cdots x_n^\omega.$$

A term of this type will be called a *reduced* ω-term, and the number n will be called the ω-length of π and denoted by $|\pi|_\omega$. In this case the ℓ-factor $\pi(1,\ell)$ (resp. $\pi(n-\ell+1,n)$) is called the *ℓ-prefix* (resp. the *ℓ-suffix*) of π. An ℓ-factor γ of π is said to occur in *position* i when $\gamma = \pi(i, i+\ell-1)$. Of course an ℓ-factor may occur in different positions. For instance, the 2-factor $a^\omega aab(ab)^\omega$ of the reduced term

$$\pi = (aab)^\omega aabb(ab)^\omega ba^\omega aab(ab)^\omega abaaa^\omega bba^\omega aab(ab)^\omega \tag{3.2}$$

has two occurrences in π, in positions 3 and 6. Moreover, it is a 2-suffix of π. The number of occurrences of an ℓ-factor γ in π will be denoted by $\mathsf{occ}(\gamma,\pi)$.

The following property, over LSl, of ω-terms with non-null rank, permits to reduce the ω-word problem for LSl to identities involving only ω-terms of rank at most 1.

Lemma 3.2 *If $\pi \in \Omega_A^\omega \mathsf{S} \setminus A^+$, then $\mathsf{LSl} \models \pi^\omega = \pi^2$.*

Proof. We can write $\pi = uv^\omega w$ for some ω-terms u, v and w, with u and w possibly empty. Then, since LSl satisfies the ω-identity $x^\omega y x^\omega y x^\omega = x^\omega y x^\omega$, we have that LSl verifies

$$(\pi^2)^2 = (uv^\omega w)^4 = (uv^\omega w)^2 = \pi^2.$$

This shows that π^2 is idempotent over LSl, whence $\mathsf{LSl} \models \pi^\omega = \pi^2$. ∎

Notice now that, if an ω-identity $\pi = \rho$ holds in LSl, then either π and ρ are the same finite word or they both are not words. Therefore, on the ω-word problem for LSl it suffices to consider ω-identities involving ω-terms of rank at least 1. The following characterization of the ω-identities satisfied by LSl is a simple reformulation of [6, Theorem 7.1].

Proposition 3.3 *Let $\pi \in \Omega_A^\omega \mathsf{S} \setminus A^+$ be an ω-term. Then, there is a normal ω-term $\pi' = u_0 x_1^\omega u_1 x_2^\omega \cdots x_n^\omega u_n$ such that LSl satisfies $\pi = \pi'$.*

Moreover, if $\rho \in \Omega_A^\omega \mathsf{S} \setminus A^+$ is another ω-term and $\rho' = v_0 y_1^\omega v_1 y_2^\omega \cdots y_m^\omega v_m$ is a normal ω-term which is equal to ρ over LSl, then LSl satisfies $\pi = \rho$ if and only if

i) $u_0 x_1^\omega = v_0 y_1^\omega$;
ii) $x_n^\omega u_n = y_m^\omega v_m$;
iii) $F_2(\pi') = F_2(\rho')$ *(i.e., π' and ρ' have the same 2-factors).*

Furthermore, it is effectively decidable whether LSl *satisfies* $\pi = \rho$.

Of course (its a consequence of the previous proposition), an ω-term π from $\Omega_A^\omega \mathsf{S} \setminus A^+$ may be equal to more than one normal ω-term over LSl. However, we illustrate in the next example a procedure (described in the proof of Theorem 4.3 below, in another context) which, as one can convince himself, is convergent in the sense that departing from π it produces a unique such normal ω-term π'.

Example 3.4 *Consider the* ω*-term*

$$\pi = b(babbab)^\omega ba\Big((a^5)^\omega b(ab)^\omega aba\Big)^\omega (ba)^\omega baa$$

and assume that $a < b$. *The pseudovariety* LSl *verifies the following* ω*-identities*

$$\begin{aligned}
\pi &= b\Big((bab)^2\Big)^\omega ba\Big((a^5)^\omega b(ab)^\omega aba\Big)^2 (ba)^\omega baa && \text{by Lemma 3.2}\\
&= b(bab)^\omega baa^\omega b(ab)^\omega abaa^\omega b(ab)^\omega aba(ba)^\omega baa && \text{as } \mathsf{LSl} \models (x^r)^\omega = x^\omega\\
&= bbab(bab)^\omega baa^\omega b(ab)^\omega abaa^\omega b(ab)^\omega aba(ba)^\omega baa && \text{as } \mathsf{LSl} \models x^\omega = xx^\omega\\
&= bb(abb)^\omega abbaa^\omega b(ab)^\omega abaa^\omega b(ab)^\omega ab(ab)^\omega abaa && \text{as } \mathsf{LSl} \models x(yx)^\omega = (xy)^\omega x\\
&= bb(abb)^\omega abbaa^\omega b(ab)^\omega abaa^\omega b(ab)^\omega ab(ab)^\omega aa && \text{as } \mathsf{LSl} \models x^\omega = x^\omega x\\
&= bb(abb)^\omega abbaa^\omega b(ab)^\omega abaa^\omega b(ab)^\omega aa && \text{as } \mathsf{LSl} \models x^\omega x = x^\omega = x^\omega x^\omega\\
&= bb(abb)^\omega abbaaa^\omega aab(ab)^\omega abaaa^\omega aab(ab)^\omega aa && \text{as } \mathsf{LSl} \models x^\omega = x^\omega x = xx^\omega.
\end{aligned}$$

Then, $\pi' = bb(abb)^\omega abbaaa^\omega aab(ab)^\omega abaaa^\omega aab(ab)^\omega aa$ *since this* ω*-term is already in normal form.*

A normal term ρ is said to be a 2-*permutation* of a normal term π, when π and ρ are equal over LSl and they have the same number of occurrences of each 2-factor. For instance,

$$\rho = (aab)^\omega aabb(ab)^\omega abaaa^\omega bba^\omega aab(ab)^\omega ba^\omega aab(ab)^\omega$$

is a 2-permutation of the normal term π in (3.2). Evidently, two normal terms need not to be 2-permutations one of the other to be equal over LSl. An example of this fact is given by

$$a^\omega bc^\omega ab^\omega ac^\omega ba^\omega \quad \text{and} \quad a^\omega bc^\omega ba^\omega bc^\omega ab^\omega ac^\omega ba^\omega.$$

4 The ω-variety generated by LSl

In this section, we study bases of ω-identities for the ω-variety LSl^ω generated by the pseudovariety LSl. In Subsection 4.1, we introduce one such basis Σ and show that there is not a finite one. The proof that Σ is indeed a basis is completed in Subsections 4.2 and 4.3.

4.1 The basis Σ

Let Σ be the following set of ω-identities:

$$(\Sigma)\quad \begin{cases} (x^r)^\omega = x^\omega, \qquad r \geq 2 & (4.1)\\ x^\omega x^\omega = x^\omega, & (4.2)\\ x^\omega = x^{\omega+1}, & (4.3)\\ (xy)^\omega x = x(yx)^\omega, & (4.4)\\ (xy^\omega z)^\omega = (xy^\omega z)^2, & (4.5)\\ x^\omega y x^\omega = x^\omega y x^\omega y x^\omega, & (4.6)\\ x^\omega y x^\omega z x^\omega = x^\omega z x^\omega y x^\omega, & (4.7) \end{cases}$$

where $x^{\omega+1}$ denotes either $x^\omega x$ or xx^ω. Notice that $x^\omega x = xx^\omega$ is a consequence of identities (4.1) and (4.4). Indeed, from them we derive

$$x^\omega x = (xx)^\omega x = x(xx)^\omega = xx^\omega.$$

The notation $\Sigma \vdash u = v$ will be used to indicate that the ω-identity $u = v$ is provable from Σ.

Fact 4.1 *By* (4.3) *and* (4.4)*, we have that* $\Sigma \vdash (xy)^\omega = xy(xy)^\omega = x(yx)^\omega y$.

It is important to refer the following three other ω-identities which are consequences of Σ.

Lemma 4.2 *The set* Σ *implies the following* ω*-identities.*

$$\begin{cases} (x^\omega)^\omega = x^\omega, & (4.8)\\ x^\omega y x^\omega z x^\omega y x^\omega = x^\omega y x^\omega z x^\omega, & (4.9)\\ x^\omega z_1 y^\omega z_2 x^\omega z_3 y^\omega = x^\omega z_3 y^\omega z_2 x^\omega z_1 y^\omega. & (4.10) \end{cases}$$

Proof. The ω-identity (4.8) is a consequence of (4.2) and (4.5). Indeed, from these ω-identities we may deduce that

$$(x^\omega)^\omega = (x^\omega x^\omega x^\omega)^\omega = (x^\omega x^\omega x^\omega)^2 = x^\omega.$$

Now, from (4.7) and (4.6) we obtain ω-identity (4.9) as follows

$$x^\omega y x^\omega z x^\omega y x^\omega = x^\omega y x^\omega y x^\omega z x^\omega = x^\omega y x^\omega z x^\omega.$$

Finally, we have that (where we underline the ω-powers which are used to derive the next term)

$$\begin{aligned}
\Sigma \vdash x^\omega z_1 \underline{y}^\omega z_2 x^\omega z_3 \underline{y}^\omega &= \underline{x}^\omega z_1 y^\omega z_2 \underline{x}^\omega z_3 y^\omega z_2 \underline{x}^\omega z_3 y^\omega && \text{by (4.6)} \\
&= x^\omega z_3 \underline{y}^\omega z_2 x^\omega z_1 \underline{y}^\omega z_2 x^\omega z_3 \underline{y}^\omega && \text{by (4.7)} \\
&= \underline{x}^\omega z_3 y^\omega z_2 \underline{x}^\omega z_3 y^\omega z_2 \underline{x}^\omega z_1 y^\omega && \text{by (4.7)} \\
&= x^\omega z_3 y^\omega z_2 x^\omega z_1 y^\omega && \text{by (4.6)}
\end{aligned}$$

which establishes (4.10). ∎

In this section, we prove the main result of the paper.

Theorem 4.3 *1) The set Σ is a basis of ω-identities for LSl^ω.*
2) The ω-variety LSl^ω has no finite basis of ω-identities.

Proof. For the proof of *2)*, it suffices to follow step by step the proof of [4, Theorem 5.2 *(2)*], where Almeida and Zeitoun show that R^ω is not finitely based. We will include it here only for the sake of completeness. By equational completeness, and assuming *1)*, it suffices to prove that no finite subset of Σ defines the variety LSl^ω. For each positive integer, let S_p be the semigroup presented by

$$\begin{aligned}
S_p = \langle a, e, f : a^p = 1,\ ea = ef = e^2 = e,\ fa = fe = f^2 = f, \\
ae = e,\ af = f \rangle.
\end{aligned}$$

This semigroup has $p+2$ elements and is realized for instance as the semigroup of transformations of the set $\{1, \ldots, p, p+1, p+2\}$, where a acts on $\{1, \ldots, p\}$ as the cycle $(1, \ldots, p)$ and fixes the other two points, and e and f are constant maps, respectively with values $p+1$ and $p+2$. Let τ be the unary operation defined on S_p by

$$\tau(e) = e,\ \tau(f) = f,\ \tau(1) = e,\ \tau(a^k) = f\ (k \in \mathbb{Z} \setminus p\mathbb{Z}),$$

which determines a unary semigroup $\mathcal{S}_p = (S_p, \cdot, \tau)$. Note that $\tau(a^p) = \tau(1) = e \neq f = \tau(a)$ and so $\mathcal{S}_p$ does not satisfy the identity $(x^p)^\omega = x^\omega$. Now it is simply a matter of routine to verify that $\mathcal{S}_p$ verifies the identities (4.2)-(4.7) and (4.1) for r relatively prime with p, which completes the proof of statement *2)*.

For *1)*, we have to prove that, for all ω-terms $\pi, \rho \in \Omega_A^\omega \mathsf{S}$,

$$\mathsf{LSl} \models \pi = \rho \quad \text{if and only if} \quad \Sigma \vdash \pi = \rho.$$

To prove the only if part, it suffices to notice that $\mathsf{LSl} \models \Sigma$. Indeed, ω-identities (4.1), (4.2) and (4.4) are verified by any finite semigroup. On the other hand, LSl is aperiodic and is defined by the ω-identities (4.6) and (4.7). Therefore it satisfies (4.3), (4.6) and (4.7). Finally, it follows immediately from Lemma 3.2 that (4.5) is valid in LSl.

We now show that, given an ω-term $\alpha \in \Omega_A^\omega \mathsf{S} \setminus A^+$, $\Sigma \vdash \alpha = \alpha'$ for some normal ω-term $\alpha' \in \Omega_A^\omega \mathsf{S}$. The following procedure to compute one such term α' consists in 6 steps (see Example 3.4 for an illustration of this algorithm). The term obtained after the jth step will be denoted by α_j, and $\alpha' = \alpha_6$. First, as in the proof of (4.8), using ω-identities (4.5) and (4.2) if necessary, we derive from α an ω-term α_1 of rank 1. Then, with the application of (4.1) one gets a rank 1 ω-term α_2 whose 1-factors x^ω are all such that x is a primitive word. Next, by Fact 4.1, we deduce from α_2 a rank 1 ω-term α_3 of the form

$$\alpha_3 = u_0 x_1^\omega u_1 x_2^\omega \cdots x_n^\omega u_n$$

where $x_1, \ldots, x_n$ are Lyndon words. This term satisfies condition *(1)* of the definition of normal term (Definition 3.1), and the remaining steps of reduction will not change this situation. In step 4, we apply identity (4.3) to cancel from u_0 the greatest power of x_1 which is a suffix of u_0, and to cancel from u_n the greatest power of x_n which is a prefix of u_n. The resulting term α_4 satisfies conditions *(2)* and *(3)* of Definition 3.1.

After the fifth step, applied to term α_4, all 2-factors will be in normal form. First, we apply ω-identities (4.3) and (4.2) to eliminate 2-factors of the form $x^\omega x^j x^\omega$, where $j \geq 0$. Next, let $\beta = x^\omega u y^\omega$ be a 2-factor of the resulting term and let $j, k \geq 1$ be the smallest integers such that $|x^j| \geq |x| + |y|$ and $|y^k| \geq |x| + |y|$. The term $\beta_1 = x^\omega x^j u y^k y^\omega$ is a consequence of (4.3). Moreover, since β is not of the form $x^\omega x^j x^\omega$, we claim that Proposition 2.1 guarantees that β_1 satisfies conditions *(a)* and *(b)* of Definition 3.1. Indeed, suppose for instance that *(a)* is not verified. Then $x^j u y^k$ is a prefix of a power of x, whence uy^k also is. Hence y^k is a factor of a power of x, so that y^k is a prefix of some power z^p of some conjugate z of x. Therefore, since $|z| = |x|$ and $|y^k| \geq |x| + |y|$, y^k and z^p have a common prefix of length at least $|y| + |z| - gcd(|y|, |z|)$. Then, Proposition 2.1 implies that y and z are powers of the same word. As y and z are both primitive, it follows that they are the same word so that z is a Lyndon word. Since z is a conjugate of x and they are both Lyndon words, we deduce that $x = z$ and, whence, that $x = y$. Therefore ux^k is a prefix of a power of x. Now, the fact that x is a primitive word implies that $u = x^\ell$ is a power of x since, otherwise, we would have $x = rs = sr$ for some $r, s \in A^+$ and, as a consequence, $r = t^p$, $s = t^q$ and $x = t^{p+q}$ for some $t \in A^+$ and

$p, q \geq 1$. We conclude that $\beta = x^\omega x^\ell x^\omega$, which contradicts our assumptions and proves the claim.

We now apply (4.3) to cancel from $x^j u y^k$ any prefix x^ℓ and any suffix y^m which preserve properties *(a)* and *(b)*. The resulting term β_2 is in normal form, that is, it satisfies conditions *(a)*, *(b)* and *(c)*. The term α_5 is obtained by replacing each such 2-factor β by β_2. The term α_5 clearly verifies conditions *(1)-(3)* and *(5)* of Definition 3.1.

Finally, we apply ω-identity (4.9) to eliminate in α_5 all occurrences, except one (say the leftmost one), of each 2-factor of the form $x^\omega u x^\omega$. The resulting ω-term α_6 is in normal form and, taking $\alpha' = \alpha_6$, we have that $\Sigma \vdash \alpha = \alpha'$.

Therefore, to complete the proof of the theorem it suffices to prove that, for all ω-terms π and ρ in normal form,

$$\mathsf{LSI} \models \pi = \rho \quad \Rightarrow \quad \Sigma \vdash \pi = \rho. \tag{4.11}$$

This will be done in the remaining of this section. ■

Recall that, if $\pi = u_0 x_1^\omega u_1 x_2^\omega \cdots x_n^\omega u_n$ and $\rho = v_0 y_1^\omega v_1 y_2^\omega \cdots y_m^\omega v_m$ are ω-terms in normal form such that LSI satisfies $\pi = \rho$, then, by Proposition 3.3, $u_0 x_1^\omega = v_0 y_1^\omega$, $x_n^\omega u_n = y_m^\omega v_m$ and π and ρ have the same 2-factors. In particular $u_0 = v_0$, $x_1 = y_1$, $x_n = y_m$ and $u_n = v_m$, and LSI verifies $x_1^\omega u_1 x_2^\omega \cdots x_n^\omega = y_1^\omega v_1 y_2^\omega \cdots y_m^\omega$. We may therefore assume in (4.11), without loss of generality, that π and ρ are reduced ω-terms

$$\pi = x_1^\omega u_1 x_2^\omega \cdots x_n^\omega, \qquad \rho = y_1^\omega v_1 y_2^\omega \cdots y_m^\omega,$$

with $x_1 = y_1$ and $x_n = y_m$. More formally, to establish Theorem 4.3 it remains to prove the following result.

Theorem 4.4 *Let π and ρ be two reduced ω-terms such that LSI verifies the ω-identity $\pi = \rho$. Then the ω-identity $\pi = \rho$ is a consequence of Σ.*

4.2 Intermediate results

In Subsection 4.3 below, it will be shown that the equality over LSI of two ω-terms π and ρ is characterized by the equality over LSI of certain subterms (which we call "blocks") of π and ρ. Therefore, the proof of Theorem 4.4 will be reduced to blocks. In the present subsection, we prove some technical intermediate results. Informally speaking, the general idea of the algorithm is to derive (under certain conditions, which are verified by blocks) from given ω-terms π and ρ such that $\mathsf{LSI} \models \pi = \rho$, new ω-terms π' and ρ' with an equal

prefix α of sufficiently large ω-length and then to cancel the suffixes. This way, we are able to pass from π to ρ ($\pi \to \pi' \to \alpha \to \rho' \to \rho$) using the ω-identities from Σ, which shows that $\Sigma \vdash \pi = \rho$.

We begin by showing that ρ can be reduced to a new ω-term with an equal 2-prefix of π.

Proposition 4.5 *Let $\pi = x_1^\omega u_1 x_2^\omega \cdots x_n^\omega$ and $\rho = y_1^\omega v_1 y_2^\omega \cdots y_m^\omega$ be reduced ω-terms such that $\mathsf{LSI} \models \pi = \rho$.*

i) If $n \leq 2$, then $\pi = \rho$.
ii) If $n > 2$, then there exists a 2-permutation ρ_1 of ρ such that $\Sigma \vdash \rho = \rho_1$ and $x_1^\omega u_1 x_2^\omega$ is the 2-prefix (resp. $x_{n-1}^\omega u_{n-1} x_n^\omega$ is the 2-suffix) of ρ_1.

Proof. If $n = 1$, then $\pi = x_1^\omega$ and it does not have 2-factors. Therefore, since $\mathsf{LSI} \models \pi = \rho$, ρ does not have 2-factors too, which means that $m = 1$, and so $\rho = y_1^\omega = x_1^\omega = \pi$. Suppose now that $n = 2$ so that $\pi = x_1^\omega u_1 x_2^\omega$. If $x_1 \neq x_2$, it is clear that ρ coincides with π since they both have the unique 2-factor $x_1^\omega u_1 x_2^\omega$. If $x_1 = x_2$, then ρ also coincides with π since, by definition of reduced form, $x_1^\omega u_1 x_1^\omega$ has only one occurrence in ρ. This proves *i)*.

We prove statement *ii)* in the prefix case. The suffix case is proved symmetrically. Let $n > 2$, so that also $m > 2$. Since $x_1 = y_1$, if $v_1 = u_1$ and $y_2 = x_2$, then we take $\rho_1 = \rho$. Otherwise, since $\mathsf{LSI} \models \pi = \rho$, the 2-factor $x_1^\omega u_1 x_2^\omega$ of π is also a 2-factor of ρ and the 2-factor $x_1^\omega v_1 y_2^\omega$ of ρ is also a 2-factor of π. Suppose that they have occurrences at position i in ρ and j in π, respectively. Then $i, j \neq 1$ and π and ρ are of the form (where π' and ρ' are, possibly empty, ω-terms)

$$\pi = x_1^\omega u_1 x_2^\omega \cdots x_{j-1}^\omega u_{j-1} x_1^\omega v_1 y_2^\omega \pi',$$

$$\rho = x_1^\omega v_1 y_2^\omega \cdots y_{i-1}^\omega v_{i-1} x_1^\omega u_1 x_2^\omega \rho'.$$

If $j = 2$, then $x_2 = x_1$. In this case,

$$\rho = \underline{x_1^\omega} v_1 y_2^\omega \cdots y_{i-1}^\omega v_{i-1} \underline{x_1^\omega} u_1 \underline{x_1^\omega} \rho' \tag{4.12}$$

and we take $\rho_1 = x_1^\omega u_1 x_1^\omega v_1 y_2^\omega \cdots y_{i-1}^\omega v_{i-1} x_1^\omega \rho'$. Hence ρ_1 and π have the same 2-prefix $x_1^\omega u_1 x_1^\omega$, and $\Sigma \vdash \rho = \rho_1$ by (4.7). Assume now that $j > 2$. We will define an iterative process which will produce the desired ω-term ρ_1 in at most $j - 2$ steps.

Step 1. Since $x_2^\omega u_2 x_3^\omega$ is a 2-factor of π, it occurs in ρ, say in position k_1. If $k_1 = 1$, then $x_1 = x_2$ and this case was treated above (ρ is of form (4.12)). If $1 < k_1 < i$, since x_2^ω occurs in position k_1, then ρ can be factored as (where α_1 and α_2 are ω-terms)

$$\rho = \underline{x_1^\omega} \alpha_1 \underline{x_2^\omega} \alpha_2 \underline{x_1^\omega} u_1 \underline{x_2^\omega} \rho'.$$

We then take $\rho_1 = x_1^\omega u_1 x_2^\omega \alpha_2 x_1^\omega \alpha_1 x_2^\omega \rho'$, which is a consequence of (4.10) and so of Σ.

Notice that k_1 can not be equal to i. Indeed, $k_1 = i$ would imply that $x_1^\omega u_1 x_2^\omega = x_2^\omega u_2 x_3^\omega$, and so $x_1 = x_2 = x_3$ and $u_1 = u_2$ which is not possible since π is in reduced form.

Suppose now that $k_1 > i$. Then x_3^ω occurs in ρ in a position greater than $i+1$.

Step ℓ (with $1 < \ell \leq j-2$). In step ℓ we consider the 2-factor $x_{\ell+1}^\omega u_{\ell+1} x_{\ell+2}^\omega$ of π and suppose that it occurs in ρ in position k_ℓ. For each $p < \ell$, we assume that $k_p > i$, which means that x_{p+2}^ω has an occurrence in ρ in a position greater than $i+1$.

If $k_\ell = 1$ or $k_\ell = i$, then $x_1 = x_{\ell+1}$. Since we are assuming, from step $p = \ell - 1$, that $x_{\ell+1}^\omega$ has an occurrence in ρ in a position greater than $i+1$, then ρ is of the form (where α_3 may be empty)

$$\rho = \underline{x_1^\omega} \alpha_1 \underline{x_1^\omega} u_1 x_2^\omega \alpha_2 \underline{x_1^\omega} \alpha_3. \tag{4.13}$$

In this case we consider $\rho_1 = x_1^\omega u_1 x_2^\omega \alpha_2 x_1^\omega \alpha_1 x_1^\omega \alpha_3$, which clearly satisfies the properties of the statement.

Suppose now that $1 < k_\ell < i$. Then

$$\rho = \underline{x_1^\omega} \alpha_1 \underline{x_{\ell+1}^\omega} \alpha_2 \underline{x_1^\omega} u_1 x_2^\omega \alpha_3 \underline{x_{\ell+1}^\omega} \alpha_4.$$

We then take $\rho_1 = x_1^\omega u_1 x_2^\omega \alpha_3 x_{\ell+1}^\omega \alpha_2 x_1^\omega \alpha_1 x_{\ell+1}^\omega \alpha_4$, which as above has the desired form.

Suppose at last that $k_\ell > i$. We assume at this point that we reached the last step, that is, we assume that $\ell = j-2$. Then $\ell + 2 = j$ and $x_{\ell+1}^\omega u_{\ell+1} x_{\ell+2}^\omega = x_{j-1}^\omega u_{j-1} x_j^\omega$, which is equal to $x_{j-1}^\omega u_{j-1} x_1^\omega$ and occurs in ρ in a position $> i$. In particular x_1^ω occurs after position $i+1$ and therefore ρ is of the form (4.13) and ρ_1 is defined as in that case.

Notice that since the only ω-identities used to derive ρ_1 from ρ were (4.7) and (4.10), which do not transform the 2-factors and do not change their number of occurrences, ρ_1 is a 2-permutation of ρ. This concludes the proof of the proposition. ∎

Under certain conditions, one can apply repeatedly Proposition 4.5 to obtain equal prefixes with a greater ω-length.

Proposition 4.6 *Let $\pi = x_1^\omega u_1 x_2^\omega \cdots x_n^\omega$ and $\rho = y_1^\omega v_1 y_2^\omega \cdots y_m^\omega$ be reduced ω-terms such that $\mathsf{LSI} \models \pi = \rho$. For each $1 \leq r \leq n$, denote by $\alpha_r = x_1^\omega u_1 x_2^\omega \cdots x_r^\omega$ the r-prefix of π. For a fixed $1 < \ell \leq n$, suppose that the following condition*

$$(C_\ell) \qquad \forall \gamma \in F_2(\alpha_{\ell-1}),\ \textit{either } \mathsf{occ}(\gamma, \pi) = \mathsf{occ}(\gamma, \rho), \textit{ or } \mathsf{occ}(\gamma, \pi), \mathsf{occ}(\gamma, \rho) > \mathsf{occ}(\gamma, \alpha_{\ell-1})$$

is verified. Then there exists a 2-permutation $\rho_{\ell-1}$ of ρ of the form $\rho_{\ell-1} = \alpha_\ell \rho'_\ell$ such that $\Sigma \vdash \rho = \rho_{\ell-1}$.

Proof. We prove the result by induction on ℓ. The case $\ell = 2$ is an immediate consequence of Proposition 4.5. Let now $2 < \ell \leq n$ and suppose that (C_ℓ) is verified. Then it is clear that $(C_{\ell-1})$ is also verified. Suppose, by induction hypothesis, that the result is valid for $\ell-1$, whence there exists a 2-permutation $\rho_{\ell-2} = \alpha_{\ell-1}\rho'_{\ell-1}$ of ρ such that

$$\Sigma \vdash \rho = \rho_{\ell-2}. \tag{4.14}$$

Then $\mathsf{LSI} \models \rho_{\ell-2} = \rho = \pi$ and therefore, by Proposition 3.3, π, ρ and $\rho_{\ell-2}$ have the same 2-factors. Since $\rho_{\ell-2}$ is a 2-permutation of ρ, ρ and $\rho_{\ell-2}$ have the same number of occurrences of each 2-factor (whence, in particular, $|\rho_{\ell-2}|_\omega = |\rho|_\omega = m$). Therefore, it follows from the hypotheses that, for each 2-factor γ of $\alpha_{\ell-1}$, either $\mathsf{occ}(\gamma, \pi) = \mathsf{occ}(\gamma, \rho_{\ell-2})$, or $\mathsf{occ}(\gamma, \pi), \mathsf{occ}(\gamma, \rho_{\ell-2}) > \mathsf{occ}(\gamma, \alpha_{\ell-1})$. In both cases, we deduce that

$$\mathsf{LSI} \models \pi(\ell-1, n) = x_{\ell-1}^\omega u_{\ell-1} x_\ell^\omega \cdots x_n^\omega = x_{\ell-1}^\omega \rho'_{\ell-1}.$$

Indeed, $\sigma = \pi(\ell-1, n) = x_{\ell-1}^\omega u_{\ell-1} x_\ell^\omega \cdots x_n^\omega$ and $\tau = x_{\ell-1}^\omega \rho'_{\ell-1}$ have the same 1-prefix, the same 1-suffix and the same 2-factors (which are precisely the 2-factors of π and ρ, except those γ such that $\mathsf{occ}(\gamma, \pi) = \mathsf{occ}(\gamma, \rho) = \mathsf{occ}(\gamma, \alpha_{\ell-1})$).

Therefore, applying Proposition 4.5 to the ω-terms σ and τ, we obtain a 2-permutation $\tau_1 = x_{\ell-1}^\omega u_{\ell-1} x_\ell^\omega \tau'$ of τ such that

$$\Sigma \vdash \tau = \tau_1. \tag{4.15}$$

It follows that

$$\begin{aligned}
\Sigma \vdash \rho &= \rho_{\ell-2} && \text{by (4.14)} \\
&= \alpha_{\ell-1}\rho'_{\ell-1} && \text{by definition of } \rho_{\ell-2} \\
&= x_1^\omega \cdots x_{\ell-2}^\omega u_{\ell-2} x_{\ell-1}^\omega \rho'_{\ell-1} && \text{by definition of } \alpha_{\ell-1} \\
&= x_1^\omega \cdots x_{\ell-2}^\omega u_{\ell-2} \tau && \text{by definition of } \tau \\
&= x_1^\omega \cdots x_{\ell-2}^\omega u_{\ell-2} \tau_1 && \text{by (4.15)} \\
&= x_1^\omega \cdots x_{\ell-2}^\omega u_{\ell-2} x_{\ell-1}^\omega u_{\ell-1} x_\ell^\omega \tau' && \text{by definition of } \tau_1 \\
&= \alpha_\ell\, \tau' && \text{by definition of } \alpha_\ell.
\end{aligned}$$

We then take $\rho_{\ell-1} = \alpha_\ell\, \tau'$, which concludes the proof. ∎

The next result is a simple corollary of the dual of Proposition 4.6 for suffixes, and presents a sort of absorption law.

Corollary 4.7 *Let π be a reduced ω-term of the form $\pi = \alpha_1 x^\omega \alpha_2 x^\omega$. If each 2-factor of $x^\omega \alpha_2 x^\omega$ has at least two occurrences in $\alpha_1 x^\omega$, then $\Sigma \vdash \pi = \alpha_1 x^\omega$.*

Proof. A reduced ω-term ρ is said to be 2-*linear* if each 2-factor has exactly one occurrence in ρ. We prove first the result for the case where $\beta = x^\omega \alpha_2 x^\omega$ is a 2-linear ω-term. Then, for each 2-factor γ of β, $\mathsf{occ}(\gamma, \beta) = 1 < \mathsf{occ}(\gamma, \alpha_1 x^\omega)$. Hence, since $\mathsf{LSI} \models \pi = \alpha_1 x^\omega$ by the hypotheses, we deduce from the dual of Proposition 4.6 that there exists an ω-term of the form $\alpha_3 x^\omega \alpha_2 x^\omega$ such that $\Sigma \vdash \alpha_1 x^\omega = \alpha_3 x^\omega \alpha_2 x^\omega$. Therefore,

$$\begin{aligned}
\Sigma \vdash \pi &= \alpha_1 x^\omega \alpha_2 x^\omega && \text{by definition of } \pi \\
&= \alpha_3 x^\omega \alpha_2 x^\omega \alpha_2 x^\omega && \text{since } \Sigma \vdash \alpha_1 x^\omega = \alpha_3 x^\omega \alpha_2 x^\omega \\
&= \alpha_3 x^\omega \alpha_2 x^\omega && \text{by } \omega\text{-identity (4.6)} \\
&= \alpha_1 x^\omega && \text{since } \Sigma \vdash \alpha_1 x^\omega = \alpha_3 x^\omega \alpha_2 x^\omega,
\end{aligned}$$

which proves the result when $x^\omega \alpha_2 x^\omega$ is 2-linear.

We now prove the general case. To show that

$$\Sigma \vdash \pi = \alpha_1 x^\omega, \tag{4.16}$$

it suffices to iterate the following procedure. If $x^\omega \alpha_2 x^\omega$ is 2-linear, then (4.16) is already proved. Otherwise we choose any 2-linear subterm of $x^\omega \alpha_2 x^\omega$ of the form $y^\omega \sigma y^\omega$, so that $\pi = \alpha_3 y^\omega \sigma y^\omega \alpha_4$ for some ω-terms α_3 and α_4 with α_4 possibly empty. Since each 2-factor of $y^\omega \sigma y^\omega$ has at least two occurrences in $\alpha_3 y^\omega$, we may apply the 2-linear case to eliminate the subterm σy^ω. We obtain a reduced ω-term π_1, Σ-equivalent to π, of the form $\pi_1 = \alpha_1 x^\omega \alpha_2' x^\omega$, where $|\alpha_2'|_\omega < |\alpha_2|_\omega$. Applying the same procedure to π_1, and iterating it if necessary, we eventually obtain, after a finite number of steps, the ω-term $\alpha_1 x^\omega$, which proves (4.16) and completes the proof of the corollary. ■

4.3 Block factorization of a normal term

The objective of this subsection is to reduce Theorem 4.4 to the case where π and ρ are *blocks* (to be defined below). In this case, Proposition 4.6 may be applied to obtain two ω-terms π' and ρ' verifying the following conditions: Σ implies $\pi = \pi'$ and $\rho = \rho'$; π' and ρ' have the same "sufficiently large" prefix α; the prefix α contains all the 2-factors of π (and ρ). We then use Corollary 4.7 to deduce that Σ implies $\pi_1 = \alpha = \rho_1$ and, as a consequence, to establish Theorem 4.4.

A reduced term $\pi = x_1^\omega u_1 x_2^\omega \cdots x_n^\omega$ $(n > 1)$ is said to be a *block* if either $n = 2$

and $x_1 = x_2$, or $n > 2$ and

$$\forall i \in \{2, \ldots, n-1\}\ \exists \ell, r \in \{1, \ldots, n\},\ \ell < i < r,\ x_\ell = x_r.$$

That is, π is a block if it can be "covered" by subterms of the form $x^\omega \alpha x^\omega$. Notice that, in particular, x_1^ω and x_n^ω must have more than one occurrence in π.

The following property of blocks will be useful to show that Theorem 4.4 is valid for blocks.

Lemma 4.8 *Let $\pi = x_1^\omega u_1 x_2^\omega \cdots x_n^\omega$ be a block. There exists a block π', Σ-equivalent to π, and a factorization $\pi' = x_1^\omega \alpha_1 x_1^\omega \alpha_2$ such that every 2-factor of π (and π') has at least one occurrence in $x_1^\omega \alpha_1 x_1^\omega$.*

Proof. Let i be the greatest position of π containing an occurrence of x_1^ω. By definition of a block, $i > 1$ and so

$$\pi = x_1^\omega u_1 x_2^\omega \cdots x_{i-1}^\omega u_{i-1} x_1^\omega u_i x_{i+1}^\omega \cdots x_n^\omega.$$

Let $f(\pi)$ be the number of 2-factors of π which do not occur in the i-prefix $\pi(i) = x_1^\omega u_1 x_2^\omega \cdots x_{i-1}^\omega u_{i-1} x_1^\omega$ of π. That is $f(\pi)$ is the number of 2-factors that fail to have the property desired for π'. The proof proceeds by induction on $k = f(\pi)$. If $k = 0$, there is nothing to prove. It suffices to take $\pi' = \pi$ in this case.

Suppose now that $k \geq 1$ and assume, by induction hypothesis, that the result holds for every block ρ with $f(\rho) < k$. Let p be the least position of π where occurs a 2-factor which does not occur in $\pi(i)$. Then $x_p^\omega u_p x_{p+1}^\omega$ is the referred 2-factor and, obviously, $i \leq p < n$.

Consider first that $p = i$. In this case $x_p^\omega u_p x_{p+1}^\omega = x_1^\omega u_i x_{i+1}^\omega$ and, by definition of a block, there exist $\ell, r \in \{1, \ldots, n\}$ such that $x_\ell = x_r$, where either (1) $\ell < i + 1 < r$ or (2) $\ell < i + 1 = n = r$. Notice that, as $r > i$, $x_r \neq x_1$ by definition of i, whence $\ell < i$. Therefore π is of the form

$$\pi = \begin{cases} x_1^\omega \beta_1 \underline{x_r^\omega} \beta_2 x_1^\omega u_i x_{i+1}^\omega \beta_3 \underline{x_r^\omega} \beta_4 \text{ in case (1)} \\ x_1^\omega \beta_1 \underline{x_{i+1}^\omega} \beta_2 x_1^\omega u_i \underline{x_{i+1}^\omega} \qquad \text{in case (2).} \end{cases}$$

In the first case, we let

$$\pi_1 = x_1^\omega \beta_1 x_r^\omega \beta_2 x_1^\omega u_i x_{i+1}^\omega \beta_3 x_r^\omega \beta_2 x_1^\omega u_i x_{i+1}^\omega \beta_3 x_r^\omega \beta_4.$$

The ω-identity $\pi = \pi_1$ is a consequence of Σ, since π_1 is obtained from π using ω-identity (4.6). However π_1 is possibly not reduced since in $x_r^\omega \beta_2 x_1^\omega$

or in $x_{i+1}^{\omega}\beta_3 x_r^{\omega}$ may occur 2-factors of the form $y^{\omega}vy^{\omega}$ and, therefore, they appear two times in π_1. It suffices, in that situation, to apply identity (4.9) to eliminate the rightmost occurrence of each of those 2-factors. We obtain a reduced ω-term (a block to be more precise)

$$\pi_2 = x_1^{\omega}\beta_1 x_r^{\omega}\beta_2 x_1^{\omega}u_i x_{i+1}^{\omega}\beta_3 x_r^{\omega}\beta_2' x_1^{\omega}u_i x_{i+1}^{\omega}\beta_3' x_r^{\omega}\beta_4,$$

which has an occurrence of x_1^{ω} to the right of an occurrence of $x_1^{\omega}u_i x_{i+1}^{\omega}$ (and of all the 2-factors of $\pi(i)$). Therefore $f(\pi_2) < k$. The case (2) can be treated analogously and, so, the result for blocks π such that $f(\pi) = k$ follows by induction.

Let us now consider the case in which $p > i$. By definition of p, the 2-factor $x_{p-1}^{\omega}u_{p-1}x_p^{\omega}$ occurs in π in a position $q < i$. To be more precise $q < i-1$ since $x_p \neq x_1$. Therefore, x_p^{ω} occurs in position $q+1 < i$ and π admits a factorization of the form

$$\pi = x_1^{\omega}\beta_1 x_p^{\omega}\beta_2 x_1^{\omega}\beta_3 x_p^{\omega}u_p x_{p+1}^{\omega}\beta_4. \tag{4.17}$$

Since π is a block, there exist $\ell, r \in \{1,\ldots,n\}$ such that $x_\ell = x_r$, where either $\ell < p+1 < r$ or $\ell < p+1 = n = r$. If $x_r = x_p$, we proceed as above in the case $p = i$, using the occurrences of x_p in positions $q+1 < i$ and $r \geq p+1$, to obtain a block π_2 such that $f(\pi_2) < k$. The result for $f(\pi) = k$ then follows by the induction hypothesis. The case in which $\ell < i$ can be treated analogously, using the occurrences of x_r in positions $\ell < i$ and $r \geq p+1$. Hence, we may assume that $x_r \neq x_p$, whence $\ell < p$, and that $\ell > i$. Therefore, the factorization (4.17) of π can be refined as follows (the case $r = i+1$ being similar, we assume that $r > i+1$)

$$\pi = x_1^{\omega}\beta_1\underline{x_p^{\omega}}\beta_2 x_1^{\omega}\beta_3'\underline{x_r^{\omega}}\beta_3''\underline{x_p^{\omega}}u_p x_{p+1}^{\omega}\beta_4'\underline{x_r^{\omega}}\beta_4''.$$

Applying identity (4.10), we obtain a block

$$\pi_2 = x_1^{\omega}\beta_1 x_p^{\omega}u_p x_{p+1}^{\omega}\beta_4' x_r^{\omega}\beta_3'' x_p^{\omega}\beta_2 x_1^{\omega}\beta_3' x_r^{\omega}\beta_4''$$

such that $f(\pi_2) < k$. Then, the induction hypothesis implies the validity of result in the case $f(\pi) = k$.

The lemma follows by induction. ∎

We may now show that Theorem 4.4 is verified when π and ρ are blocks.

Proposition 4.9 *If π and ρ are two blocks such that $\mathsf{LSI} \models \pi = \rho$, then $\Sigma \vdash \pi = \rho$.*

Proof. Suppose first that π has a unique 1-factor x^{ω}. Since $\mathsf{LSI} \models \pi = \rho$ it follows that x^{ω} is also the only 1-factor of ρ. In this case it is immediate that $\Sigma \vdash \pi = \rho$ since $\pi = \rho$ is provable from ω-identity (4.7).

We now assume that π (and so also ρ) has at least two different 1-factors, say x^ω and y^ω where x^ω is the 1-prefix of π (and ρ). Let z^ω be the 1-suffix of π (and ρ). From Lemma 4.8, there is a block $\pi_1 = x^\omega\alpha_1 x^\omega\alpha_2 z^\omega$ such that $\Sigma \vdash \pi = \pi_1$ and $x^\omega\alpha_1 x^\omega$ contains all the 2-factors of π. In particular, y^ω and z^ω are factors of α_1. We apply ω-identity (4.6) three times to derive from π_1 a (possibly non-reduced) ω-term $\pi_2 = (x^\omega\alpha_1)^4 x^\omega\alpha_2 z^\omega$. The need of 4 copies of $x^\omega\alpha_1$ should be clear by definition of the ω-term π_3 bellow obtained from π_2. However we advance that: the prefix $x^\omega\alpha_1 x^\omega\alpha_1 x^\omega$ contains at least two occurrences of each 2-factor, which will permit to apply Corollary 4.7 to π_3; the third copy of $x^\omega\alpha_1$ contains an occurrence of z^ω, which will appear as the first distinguished occurrence in (4.18); the fourth copy permits to obtain an extra occurrence of each 2-factor, which will guarantee that the total number of occurrences of each 2-factor (not of the form $v^\omega u v^\omega$) in π_3 will be greater than the number of occurrences of that 2-factor in the prefix $x^\omega\alpha_3 z^\omega$ of π_3 and which will permit to apply Proposition 4.6.

Now, using ω-identity (4.9) in π_2 to delete all except the leftmost occurrence of each 2-factor of the form $v^\omega u v^\omega$, we obtain a reduced ω-term π_3 such that $\Sigma \vdash \pi = \pi_3$ and

$$\pi_3 = x^\omega\alpha_3 z^\omega\alpha_4 z^\omega \tag{4.18}$$

where:

i) LSl verifies the ω-identity $\pi_3 = x^\omega\alpha_3 z^\omega$ (which is equivalent to say that each 2-factor of π_3 occurs in $x^\omega\alpha_3 z^\omega$);
ii) each 2-factor of π_3 occurs in $z^\omega\alpha_4 z^\omega$ except those of the form $v^\omega u v^\omega$;
iii) for each 2-factor γ of $z^\omega\alpha_4 z^\omega$, $\mathsf{occ}(\gamma, x^\omega\alpha_3 z^\omega) \geq 2$.

We notice that these conditions are indeed verified since the existence of the 1-factor y^ω guarantees the existence of 2-factors which are not of the form $v^\omega u v^\omega$.

On the other hand, $\mathsf{LSl} \models \pi = \rho$ by hypothesis. So, as above and applying, if necessary, ω-identities (4.6) and (4.9) a sufficiently large number of times, we can find a reduced ω-term ρ_1 such that $\Sigma \vdash \rho = \rho_1$ and, for each 2-factor γ of ρ_1, $\mathsf{occ}(\gamma, \rho_1) \geq \mathsf{occ}(\gamma, \pi_3)$. In particular, for each 2-factor γ of the form $v^\omega u v^\omega$, $\mathsf{occ}(\gamma, \rho_1) = \mathsf{occ}(\gamma, \pi_3) = 1$. Therefore, since $\mathsf{LSl} \models \pi_3 = \rho_1$, we may deduce from Proposition 4.6 a 2-permutation ρ_2 of ρ_1, of the form

$$\rho_2 = x^\omega\alpha_3 z^\omega\alpha_5 z^\omega,$$

such that $\Sigma \vdash \rho_2 = \rho_1$.

Now, by Corollary 4.7, $\Sigma \vdash \pi_3 = x^\omega\alpha_3 z^\omega = \rho_2$. Since the sequence of ω-identities $\pi = \pi_3 = \rho_2 = \rho_1 = \rho$ is provable from Σ, the proof of the proposition is complete. ∎

We now introduce the block factorization of a normal ω-term, which will allow to reduce Theorem 4.4 to blocks. Since we finished to solve that case in Proposition 4.9, the general case will then be obtained. So, consider a normal term

$$\pi = u_0 x_1^\omega u_1 x_2^\omega \cdots x_m^\omega u_m.$$

If each 1-factor x_k^ω has exactly one occurrence in π, then we define $\alpha_0 = \pi$. Otherwise, let i_1 be the least $k \in \{1, \ldots, m\}$ such that x_k^ω has at least two occurrences in π, and define $\alpha_0 = u_0 x_1^\omega u_1 \cdots x_{i_1-1}^\omega u_{i_1-1}$. Now let j_1 be the greatest $k \in \{i_1 + 1, \ldots, m\}$ such that $x_{i_1}^\omega u_{i_1} x_{i_1+1}^\omega \cdots u_{k-1} x_k^\omega$ is a block, and define $\pi_1 = x_{i_1}^\omega u_{i_1} x_{i_1+1}^\omega \cdots u_{j_1-1} x_{j_1}^\omega$. Now, applying the same procedure to the subterm $\rho_1 = u_{j_1} x_{j_1+1}^\omega \cdots x_m^\omega u_m$ of π, we get subterms $\alpha_1 = u_{j_1} x_{j_1+1}^\omega u_{j_1+1} \cdots x_{i_2-1}^\omega u_{i_2-1}$ and $\pi_2 = x_{i_2}^\omega u_{i_2} x_{i_2+1}^\omega \cdots u_{j_2-1} x_{j_2}^\omega$. We iterate this process until we get $\alpha_n = \rho_n$ in some step $n + 1$, where $n \geq 0$ and $\rho_0 = \pi$. Then π admits the following factorization

$$\pi = \alpha_0 \pi_1 \alpha_1 \pi_2 \cdots \pi_n \alpha_n \tag{4.19}$$

called the *block factorization* of π. Notice that the block factorization has the following properties:

- for each $1 \leq i \leq n$, the factor π_i is a block;
- for each $1 \leq i < n$, α_i is non-empty. Indeed π_i ends with an ω-power and π_{i+1} begins with another ω-power and, by definition of normal ω-term, π does not have two ω-powers as consecutive factors;
- if a 1-factor x^ω has at least two occurrences in π, then all the occurrences of x^ω are contained in some unique block π_i;
- if a 1-factor of π occurs in some α_i, then it has exactly one occurrence in π.

However, the converse of this last property is not true. If a 1-factor of π has exactly one occurrence, then this occurrence does not necessarily happen in some α_i. Indeed it can occur in some π_i provided another 1-factor has an occurrence before and another one after it in π_i.

The next result states that for LSl, the ω-word problem for arbitrary terms can be reduced to the ω-word problem for blocks.

Proposition 4.10 *Let $\pi = \alpha_0 \pi_1 \alpha_1 \cdots \pi_n \alpha_n$ and $\rho = \beta_0 \rho_1 \beta_1 \cdots \rho_m \beta_m$ be the block factorizations of two normal ω-terms π and ρ. Then, $\mathsf{LSl} \models \pi = \rho$ if and only if*

i) $n = m$;
ii) $\alpha_i = \beta_i$, *for every* $i \in \{0, 1, \ldots, n\}$;
iii) $\mathsf{LSl} \models \pi_j = \rho_j$, *for every* $j \in \{1, \ldots, n\}$.

Proof. The sufficient condition is trivial. Conversely, assume without loss of generality that $n \leq m$ and that π and ρ are reduced. The proof is made by induction on n.

Suppose first that $n = 0$. Then $\pi = \alpha_0$ and α_0 is non-empty, say

$$\alpha_0 = x_1^\omega u_1 x_2^\omega \cdots x_k^\omega.$$

If $k \leq 2$, then the result follows immediately from Proposition 4.5 *i)*. So, we assume that $k > 2$. By definition of block factorization, x_1^ω has a unique occurrence in π. Hence, as $\mathsf{LSI} \models \pi = \rho$ by hypothesis, x_1^ω is the 1-prefix of ρ and has a unique occurrence in ρ, since otherwise ρ (and so also π) would have a 2-factor of the form $y^\omega v x_1^\omega$. Therefore β_0 is non-empty, say

$$\beta_0 = y_1^\omega v_1 y_2^\omega \cdots y_\ell^\omega$$

with $y_1 = x_1$. Now, since x_1^ω has only one occurrence in ρ and $x_1^\omega u_1 x_2^\omega$ is a 2-factor of ρ, $x_1^\omega u_1 x_2^\omega$ has a unique occurrence in ρ, in position 1 to be more precise. Moreover, x_2^ω has a unique occurrence in π, which implies that it has also a unique occurrence in ρ, since otherwise ρ (and so also π) would have a 2-factor of the form $y^\omega v x_2^\omega$ distinct of $x_1^\omega u_1 x_2^\omega$. This implies that $\ell \geq 2$ and that $u_1 = v_1$ and $x_2 = y_2$. Iterating the above process, we deduce that $\ell \geq k$ and that $u_{i-1} = v_{i-1}$ and $x_i = y_i$ for every $i \leq k$. Now, since x_k^ω has precisely one occurrence in π, we conclude, as above, that necessarily $\rho = \beta_0$ (whence $m = 0$) and $\alpha_0 = \beta_0$.

Suppose now that $n \geq 1$ (so that also $m \geq 1$) and assume, by induction hypothesis, that the result is valid for $n - 1$. Let

$$\pi_1 = e_1^\omega f_1 e_2^\omega \cdots e_r^\omega \quad \text{and} \quad \rho_1 = g_1^\omega h_1 g_2^\omega \cdots g_s^\omega.$$

As above one can show that α_0 is non-empty if and only if β_0 is non-empty. In this case, if $\alpha_0 = x_1^\omega u_1 x_2^\omega \cdots x_k^\omega u_k$ and $\beta_0 = y_1^\omega v_1 y_2^\omega \cdots y_\ell^\omega v_\ell$, one can show that $k = \ell$, $u_{i-1} = v_{i-1}$ and $x_i = y_i$ for every $1 \leq i \leq k$. Moreover, $x_k^\omega u_k e_1^\omega$ occurs in ρ in position k, since $x_k = y_k$ and y_k^ω has only one occurrence in ρ. Therefore $u_k = v_k$ and $e_1 = g_1$. This proves that $\alpha_0 = \beta_0$ and that π_1 and ρ_1 have the same 1-prefix. To prove that $\mathsf{LSI} \models \pi_1 = \rho_1$, we now show that the blocks π_1 and ρ_1 have the same 2-factors.

Suppose that there exists some 2-factor $e_i^\omega f_i e_{i+1}^\omega$ of π_1 that does not occur in ρ_1 and assume that $1 \leq i < r$ is minimal with this property. Since e_i^ω occurs in ρ_1 (and in ρ it does not occur outside ρ_1), $e_i^\omega f_i e_{i+1}^\omega$ occurs in ρ in the last position of ρ_1, so that e_{i+1}^ω is the first ω-power to the right of ρ_1. Consider now the 2-factors

$$e_{i+1}^\omega f_{i+1} e_{i+2}^\omega, \ldots, e_{r-1}^\omega f_{r-1} e_r^\omega$$

of π_1 (and of ρ). Since none of the 1-factors $e_{i+1}^\omega, e_{i+2}^\omega, \ldots, e_r^\omega$ may occur in ρ both inside and outside ρ_1, we deduce that all these 2-factors occur to the right of ρ_1. But π_1 is a block, whence there exist $p, q \in \{1, \ldots, r\}$, with $p < i < q$ or $1 = p = i < q$, such that $e_p = e_q$, which is absurd since e_p^ω occurs in ρ_1 by minimality of i. Therefore, all the 2-factors of π_1 occur in ρ_1. By symmetry, we

deduce that π_1 and ρ_1 have the same 2-factors. To establish that $\mathsf{LSl} \models \pi_1 = \rho_1$, it remains to prove that $e_r = g_s$.

Suppose that the suffix

$$\pi' = \alpha_1\pi_2 \cdots \pi_n\alpha_n$$

of π is non-empty and let ux^ω be the unique prefix of π' with $u, x \in A^+$. Then $e_r^\omega ux^\omega$ is a 2-factor of π with a unique occurrence, since otherwise x^ω could not occur outside π_1. Hence $e_r^\omega ux^\omega$ is also a 2-factor of ρ and, as above, one can show that it has a unique occurrence in ρ, in the last position of ρ_1 to be more precise. Therefore $e_r = g_s$ and the suffix

$$\rho' = \beta_1\rho_2 \cdots \rho_m\beta_m$$

of ρ is non-empty. We conclude in particular that $\mathsf{LSl} \models \pi_1 = \rho_1$. Moreover, if vy^ω is the unique prefix of ρ' with $v, y \in A^+$, then $u = v$ and $x = y$. Notice that, by the above arguments, it is now clear that π' is empty if and only ρ' is empty. In this case e_r^ω and g_s^ω are, respectively, the 1-suffixes of π and ρ. Therefore they coincide, since LSl verifies $\pi = \rho$ by hypothesis, and the result is proved. So, we may assume that π' and ρ' are both non-empty. We let π'' and ρ'' be the reduced ω-terms obtained from π' and ρ', respectively, by deleting the prefix u. Then

$$\mathsf{LSl} \models \pi'' = \rho''$$

since π'' and ρ'' have the same 1-prefix x^ω, the same 1-suffix (which is the one of π and ρ) and the same 2-factors (which are the ones of π and ρ except those occurring in $\alpha_0\pi_1ux^\omega$). Moreover the block factorizations of π'' and ρ'' are precisely $\pi'' = \alpha_1'\pi_2 \cdots \pi_n\alpha_n$ and $\rho'' = \beta_1'\rho_2 \cdots \rho_m\beta_m$ where α_1' and β_1' are the ω-terms obtained from α_1 and β_1, respectively, by deleting the prefix u. The result is now an immediate consequence of the induction hypothesis. ■

We are finally able to complete the proof that Σ is a basis of ω-identities for LSl^ω.

Proof of Theorem 4.4. Let $\pi = \alpha_0\pi_1 \cdots \pi_n\alpha_n$ and $\rho = \beta_0\rho_1 \cdots \rho_m\beta_m$ be the block factorizations of π and ρ. Then, by Proposition 4.10,

i) $n = m$;
ii) $\alpha_i = \beta_i$, for every $i \in \{0, 1, \ldots, n\}$;
iii) $\mathsf{LSl} \models \pi_j = \rho_j$, for every $j \in \{1, \ldots, n\}$.

Hence, from condition iii) and Proposition 4.9, we deduce that $\Sigma \vdash \pi_j = \rho_j$, for every $j \in \{1, \ldots, n\}$. Therefore, it follows immediately from conditions i) and ii) that $\Sigma \vdash \pi = \rho$. This proves Theorem 4.4 and, therefore, completes the proof of Theorem 4.3. ■

References

[1] J. Almeida, Implicit operations on finite $\mathcal{J}$–trivial semigroups and a conjecture of I. Simon, J. Pure Appl. Algebra 69 (1990) 205–218.

[2] J. Almeida, Finite semigroups: an introduction to a unified theory of pseudovarieties, in: G. Gomes, J.-E. Pin, P. Silva (Eds.), Semigroups, Algorithms, Automata and Languages, World Scientific, 2002.

[3] J. Almeida, B. Steinberg, Syntactic and global semigroup theory: a synthesis approach, in: Algorithmic problems in groups and semigroups (Lincoln, NE, 1998), Trends Math., Birkhäuser Boston, Boston, MA, 2000, pp. 1–23.

[4] J. Almeida, M. Zeitoun, An automata-theoretical approach to the word problem for ω-terms over R, Theoret. Comput. Sci. 370 (2007) 131–169.

[5] J. Brzozowski, I. Simon, Characterization of locally testable events, Discrete Mathematics 4 (1973) 243–271.

[6] J.C. Costa, Free profinite locally idempotent and locally commutative semigroups, J. Pure Appl. Algebra 163 (2001) 19-47.

[7] M. Lothaire, Algebraic combinatorics on words, Cambridge University Press, 2002.

[8] J. McCammond, Normal forms for free aperiodic semigroups, Internat. J. Algebra Comput. 11 (2001) 581–625.

[9] R. McNaughton, Algebraic decision procedures for local testability, Math. Systems and Theory 8 (1974) 60–76.

[10] Y. Zalcstein, Locally testable semigroups, Semigroup Forum 5 (1973) 216–227.