Acta Informatica 13, 189–197 (1980)

An Ogden-Like Iteration Lemma for Rational Power Series

Christophe Reutenauer

CNRS, Institut de Programmation, 4 place Jussieu, F-75230 Paris cedex 05, France

Summary. An Ogden-like iteration lemma for languages that are support of rational power series is proved; it is a generalization of Jacob's iteration lemma. The new bound we obtain is much smaller than the one of Jacob and does no more depend on the cardinality of the alphabet. The proof consists in studying how pseudo-regular matrices appear as subproducts of long products of square matrices.

I. Introduction

Everyone knows the "pumping lemma" for recognizable (regular) languages; its proof is actually immediate. For languages which are support of a recognizable power series (it is the case for recognizable languages) there exists an iteration theorem due to Gérard Jacob [5]: the proof is rather lengthy. One part of the present work (part II) is devoted to a simplified proof of this result, using a combinatorial lemma of Schützenberger. In the other part (part II) we extend Jacob's theorem to cover the case of an infinite alphabet: the bound we give does no more depend on the cardinality of the alphabet, and even, is considerably smaller than the one of Jacob.

The techniques we use allow us to prove the main result, i.e. an Ogden like iteration lemma for the supports of recognizable power series, similar to the one for recognizable languages that can be found e.g. in [1, I.4.5]. As did Jacob, we study how appear "pseudo-regular matrices as subproduct in long products of square matrices". As a byproduct, we obtain a result about the multiplicative monoids of finite dimensional algebras, which can be stated informally as follows: from each long product of elements of such an algebra, one can extract a subproduct which belongs to a group contained in the multiplicative monoid of this algebra.

0001-5903/80/0013/0189/$01.80

II. Jacob's Iteration Theorem

1. Generalities about Formal Power Series

Let $\mathbf{X}$ be an alphabet, $\mathbf{X}^*$ the free monoid generated by $\mathbf{X}$; the elements of $\mathbf{X}^*$ are called *words* and the neutral element (the *empty word*) is denoted by 1.

Let $\mathbf{K}$ be a field. A *formal power series* on $\mathbf{X}$ with coefficients in $\mathbf{K}$ is a mapping $\mathbf{X}^* \to \mathbf{K}$; the set of all formal power series is denoted by $\mathbf{K}\langle\langle \mathbf{X} \rangle\rangle$ and $s \in \mathbf{K}\langle\langle \mathbf{X} \rangle\rangle$ by the infinite sum:

$$s = \sum_{w \in \mathbf{X}^*} (s, w)\, w$$

where (s, w) is the value of s at w.

The *support* of s, denoted by $\operatorname{supp}(s)$, is the language

$$\operatorname{supp}(s) = \{w \in \mathbf{X}^* \mid (s, w) \neq 0\}.$$

A (non commutative) *polynomial* is a formal power series with finite support; the set of all polynomials is denoted by $\mathbf{K}\langle \mathbf{X} \rangle$. $\mathbf{K}\langle\langle \mathbf{X} \rangle\rangle$ is a $\mathbf{K}$-algebra:

The sum of two series s and t is defined by:

$$(s+t, w) = (s, w) + (t, w).$$

The product of s and t is defined by

$$(st, w) = \sum_{uv = w} (s, u)(t, v).$$

A formal power series s is invertible in $\mathbf{K}\langle\langle \mathbf{X} \rangle\rangle$ if and only if $(s, 1) \neq 0$.

The subalgebra of *rational series* is the least subalgebra of $\mathbf{K}\langle\langle \mathbf{X} \rangle\rangle$ containing $\mathbf{K}\langle \mathbf{X} \rangle$ and containing the inverse of each of its invertible element.

A *recognizable series* is a series s such that there exists an integer $n \geqq 1$, a homomorphism from $\mathbf{X}^*$ into the multiplicative monoid $\mathbf{K}^{n \times n}$ of square matrices of order n $\mu: \mathbf{X}^* \to \mathbf{K}^{n \times n}$, matrices $\lambda \in \mathbf{K}^{1 \times n}$ and $\gamma \in \mathbf{K}^{n \times 1}$ such that:

$$\forall w \in \mathbf{X}^*, \ (s, w) = \lambda \mu w \gamma.$$

If $\mathbf{X}$ is finite, the Kleene-Schützenberger theorem [cf. 4 Th. VII.5.1] asserts that *a series is rational if and only if it is recognizable.*

2. Pseudo-Regular Matrices

Let n be an integer $\geqq 1$ and a be a square matrice of order n on $\mathbf{K}$: $a \in \mathbf{K}^{n \times n}$. We let act a on the right on $\mathbf{K}^n = \mathbf{K}^{1 \times n}$.

Proposition 1. *The following conditions are equivalent:*

(i) *a belongs to a group contained in the multiplicative monoid of* $\mathbf{K}^{n \times n}$.

(ii) *there exist $b, c \in \mathbf{K}^{n \times n}$ such that $a = cb$ and* $\operatorname{rank}(b) = \operatorname{rank}(bcb)$

(iii) *the kernel and the range of* a *are supplementary subspaces.*

(iv) λ^2 *does not divide the minimal polynomial* $P(\lambda)$ *of* a.

(v) a *is null or invertible or similar to a matrice of the form* $\begin{pmatrix} a' & 0 \\ 0 & 0 \end{pmatrix}$ *with* $a' \in GL_{n'}(\mathbf{K})$, $0 < n' < n$.

($GL_n(\mathbf{K})$ denotes the set of invertible square matrices of order n.)

This result can be found in [7] and [5]. We make the proof for sake of completeness.

Proof. (i)$\Rightarrow$(ii) Let e be the neutral element of this group and d the inverse of a. We have $aead = a$ hence

$$\mathrm{rank}(a) = \mathrm{rank}(aead) \leqq \mathrm{rank}(aea) \leqq \mathrm{rank}(a).$$

Thus $ea = a$ and $\mathrm{rank}(a) = \mathrm{rank}(aea)$.

(ii)$\Rightarrow$(iii) We denote by $\mathrm{Ker}(a)$, $\mathrm{Im}(a)$ the kernel, the image of a, respectively.

From the hypothesis follows that $\mathrm{Im}(b) \cap \mathrm{Ker}(cb) = 0$, that is $\mathrm{Im}(b) \cap \mathrm{Ker}(a) = 0$. Moreover

$$\mathrm{rank}(b) = \mathrm{rank}(bcb) \leqq \mathrm{rank}(cb) \leqq \mathrm{rank}(b) \text{ hence } \mathrm{rank}(b) = \mathrm{rank}(cb).$$

Because $\mathrm{Im}(cb) \subset \mathrm{Im}(b)$ we obtain $\mathrm{Im}(b) = \mathrm{Im}(cb)$.

This implies $\mathrm{Im}(a) \cap \mathrm{Ker}(a) = 0$.

(iii)$\Rightarrow$(v) If $\mathrm{Ker}(a) = 0$ or $\mathrm{Im}(a) = 0$ we are done. In the remaining cases $\mathrm{Im}(a)$ and $\mathrm{Ker}(a)$ are supplementary subspaces and the restriction of a to $\mathrm{Im}(a)$ is an automorphism of $\mathrm{Im}(a)$. By change of basis we obtain the desired form for a.

(v)$\Rightarrow$(iv) If $a = 0$ or a is invertible we are done. In the other cases let $Q(\lambda)$ be the minimal polynomial of a'. Then $Q(0) \neq 0$ and $P(\lambda) = \lambda Q(\lambda)$.

(iv)$\Rightarrow$(v) If $P(\lambda) = \lambda$ or $P(0) \neq 0$ we are done. Otherwise $P(\lambda) = \lambda Q(\lambda)$ with Q non constant and $Q(0) \neq 0$. Then $\mathbf{K}^n = \mathrm{Ker}(a) \oplus \mathrm{Ker}(Q(a))$ and these two subspaces are stable under a. Moreover $Q(0) \neq 0$ implies that $a | \mathrm{Ker}(Q(a))$ is an automorphism of $\mathrm{Ker}(Q(a))$. By change of basis the result follows.

(v)$\Rightarrow$(i) It's obvious. □

A matrice that satisfies the equivalent conditions of proposition 1 is said to be *pseudo-regular*.

Lemma 1. *Let* $a \in \mathbf{K}^{n \times n}$, $\lambda \in \mathbf{K}^{1 \times n}$, $\gamma \in \mathbf{K}^{n \times 1}$ *and let* (p_k) *be the sequence:* $p_k = \lambda\, a^k \gamma$. *If* a *is pseudo-regular and* $p_1 \neq 0$, *there exists an infinity of* k *such that* $p_k \neq 0$.

Proof. Let $\lambda^m + \alpha_1 \lambda^{m-1} + \ldots + \alpha_{m-1} \lambda + \alpha_m$ be the minimal polynomial of a. We have $\alpha_m \neq 0$ or $\alpha_{m-1} \neq 0$. The sequence (p_k) satisfies the linear recursion formula:

$$\forall k \in \mathbf{N},\ p_{k+m} + \alpha_1 p_{k+m-1} + \ldots + \alpha_{m-1} p_{k+1} + \alpha_m p_k = 0$$

Let be $i \geqq 1$: if $p_i \neq 0$ then there exists $j > i$ such that $p_j \neq 0$. Indeed:

– If $\alpha_m \neq 0$, then

$$p_{i+m} + \alpha_1 p_{i+m-1} + \ldots + \alpha_{m-1} p_{i+1} + \alpha_m p_i = 0$$

hence there exists $j\in\{i+1,\dots,i+m\}$ such that $p_j\neq 0$.

– If $\alpha_m=0$, then $\alpha_{m-1}\neq 0$ and

$$p_{i-1+m}+\alpha_1 p_{i-2+m}+\dots+\alpha_{m-1} p_i=0$$

hence there exists $j\in\{i+1,\dots,i-1+m\}$ such that $p_j\neq 0$. The lemma follows by induction. □

The following theorem shows that in "long products" of matrices of a finitely generated monoid there are "subproducts" that are pseudo-regular.

Theorem 1 [Jacob 5]. *Let* $\mathbf{X}$ *be a finite alphabet and* n *an integer* $\geqq 1$. *There exists* N *such that for each homomorphism* $\mu: \mathbf{X}^*\to\mathbf{K}^{n\times n}$, *for each word* w *longer than* N, w *has a factor* $v\neq 1$ *such that* μv *is a pseudoregular matrix.*

(A factor of a word w is a word v such that $w=uvt$ for some words u and t.)

We give here a simplified proof of this result, using a combinatorial lemma of Schützenberger. One could remark that the bound N given below is the same as the one of Jacob.

We define particular words, called *quasi-powers* in the following manner:

. Each word $\neq 1$ is a quasi-power of order 0.
. A quasi-power of order $n\geqq 1$ is a word of the form uvu where u is a quasi-power of order $n-1$.

Example: $uvuwuvu$ is a quasi-power of order 2.

Lemma 2 [Schützenberger 8, IV. 5]. *Let* $\mathbf{X}$ *be a finite alphabet and* $n\geqq 1$. *There exists an integer* N *such that each word of length at least* N *has a factor that is a quasi-power of order* n.

Proof. Let $d=\mathrm{Card}(\mathbf{X})$ and $C_0=1$, and by induction, $C_{k+1}=C_k(1+d^{C_k})$. Then each word of length at least C_k has a factor that is a quasi-power of order k.

It's clear if $k=0$.

Let $k\geqq 0$ and w a word with length $\geqq C_{k+1}=C_k(1+d^{C_k})$; w has a factor of the form

$$u_1 u_2 \dots u_{d'} \quad \text{where } d'=1+d^{C_k}$$

with $\forall i$, $|u_i|=C_k$. The number of words of length C_k is equal to d^{C_k}, hence two of the u_i's are equal and w contains a factor of the form uvu with $|u|=C_k$; by induction, $u=au'b$ where u' is a quasi-power of order k, hence w contains the quasi-power $u'bvau'$ of order $k+1$. □

Proof of Theorem 1. Let N be the integer of Lemma 2 and w a word of length at least N; w contains a factor that is a quasi-power of order n. Let us call it u_n; then there exist words $u_0\neq 1, u_1,\dots,u_{n-1}, v_1,\dots,v_n$ such that:

$$\forall i\in\{1,\dots,n\}\ u_i=u_{i-1} v_i u_{i-1}.$$

Let μ be an homomorphism $\mathbf{X}^*\to\mathbf{K}^{n\times n}$.

We have: $\forall i\in\{1,\dots,n\}$

$$n\geqq \mathrm{rank}(\mu u_{i-1})\geqq \mathrm{rank}(\mu u_{i-1} v_i u_{i-1})=\mathrm{rank}(\mu u_i).$$

Hence there exists i such that
$\operatorname{rank}(\mu u_{i-1}) = \operatorname{rank}(\mu u_{i-1} v_i u_{i-1})$ and $\mu v_i u_{i-1}$ is pseudo-regular [Prop. 1 (ii)]. □

Remark. As the proof shows, Theorem 1 is still true for skew fields.

3. Iteration Theorem

The following theorem is an easy consequence of Theorem 1.

Theorem 2 [Jacob 5]. *Let s be a recognizable series on the finite alphabet* **X**. *There exists an integer N such that for each word w in the support of s, of length at least N, for each factorization $w = aub$ with $|u| \geqq N$, u has a factorization $u = u_1 u_2 u_3$ such that $a u_1 u_2^* u_3 b \cap \operatorname{supp}(s)$ is infinite.*

Let us recall that u^* denotes the language $\{u^n | n \in \mathbb{N}\}$.

Proof. Let λ, μ, γ be such that $\forall w \in \mathbf{X}^*$ $(s, w) = \lambda \mu w \gamma$ [cf. § 1] where μ is an homomorphism $\mathbf{X}^* \to \mathbf{K}^{n \times n}$. Let N be the constant of Theorem 1. Then $u = u_1 u_2 u_3$ with $u_2 \neq 1$ and μu_2 is a pseudo-regular matrix.

The sequence $p_k = \lambda \mu a u_1 \mu u_2^k \mu u_3 b \gamma$ satisfies the hypothesis of Lemma 1 because $p_1 = (s, w) \neq 0$. There exists an infinity of k such that $p_k \neq 0$ and the theorem follows. □

In the following paragraph, we extend these results to infinite alphabets, using other techniques.

III. Extension to Infinite Alphabets

Theorem 3. *Let n be an integer $\geqq 1$. There exists $N = N(n)$ such that for each alphabet* **X**, *for each homomorphism $\mu: \mathbf{X}^* \to \mathbf{K}^{n \times n}$, each word w of length at least N has a factor $v \neq 1$ such that μv is a pseudo-regular matrix.*

This result may be stated as follows:

Theorem 3′. *Let n be an integer $\geqq 1$. There exists $N = N(n)$ such that for all family $(a_i)_{1 \leqq i \leqq N}$ of square matrices of order n, there exist i, j, $1 \leqq i \leqq j \leqq N$, such that $a_i \dots a_j$ is pseudo-regular.*

Remark. We shall see that $N(n) = \prod_{i=1}^{n} \left[\binom{n}{i} + 1\right]$ which is smaller than 2^{n^2}. One has $N(1) = 1$, $N(2) = 3$, $N(3) = 16$. It can be shown directly that one could choose $N(2) = 2$, $N(3) = 9$; hence the bound we give is far from being the best possible.

Before proving this result, we state an easy corollary about the multiplicative monoid of a finite dimensional algebra, that is of independent interest.

Corollary. *Let* **A** *be a finite dimensional algebra over* **K**. *Then there exists a constant N (depending only of the dimension of* **A**) *such that: for each family $(a_i)_{1 \leqq i \leqq N}$ of elements of* **A**, *there exist i, j, $1 \leqq i \leqq j \leqq N$, such that $a_i \dots a_j$ belongs to a group contained in the multiplicative semigroup of* **A**.

In other words, from each "long product" of elements of **A**, one can "extract a subproduct" that belongs to a group in **A**.

Proof. If $\dim(\mathbf{A})=n$, **A** admits a faithful representation by square matrices of order n. Hence we may suppose that **A** is contained in $\mathbf{K}^{n\times n}$. By Theorem 3′ it remains to show that if $a\in\mathbf{A}$ is a pseudo-regular matrix, there exists a group G contained in the multiplicative monoid of **A** such that $a\in G$. But if a is pseudo-regular, we may suppose, after change of basis, that

$$a=\begin{pmatrix} b & 0\\ 0 & 0\end{pmatrix}$$

where $b\in GL_{n'}(\mathbf{K})$. Let $I_{n'}$ be the identity matrix of order n' and

$$I'=\begin{pmatrix} I_{n'} & 0\\ 0 & 0\end{pmatrix}.$$

Let $P(\lambda)=\lambda^k+\alpha_1\lambda^{k-1}+\ldots+\alpha_{k-1}\lambda+\alpha_k$ be the minimal polynomial of b. Then $\alpha_k\neq 0$ because b is invertible and we have

$$0=b^k+\alpha_1 b^{k-1}+\ldots+\alpha_{k-1}b+\alpha_k I_{n'} \quad \text{which implies}$$
$$0=a^k+\alpha_1 a^{k-1}+\ldots+\alpha_{k-1}a+\alpha_k I'.$$

This implies $I'\in A$. Let $c=-\alpha_k^{-1}(\alpha_{k-1}I'+\alpha_{k-2}a+\ldots+\alpha_1 a^{k-2}+a^{k-1})$.

Because a $I'=a$, we have $ac=ca=I'$. Furthermore, $c\in A$, and a, c generate a group with unit I'. □

We need a combinatorial lemma, similar to a lemma of Jacob [5].

Lemma 3. *Let* **X** *be an alphabet, $n, k_0,\ldots,k_n$ integers $\geqq 1$ and $r:\mathbf{X}^*\to\{0,1,\ldots,n\}$ a mapping such that: $\forall u, v, w\in\mathbf{X}^*$, $r(uvw)\leqq r(v)$. Then for each word w of length at least $k_0k_1\ldots k_n$, there exists $l, 0\leqq l\leqq n$, such that w has a factor of the form $w_1w_2\ldots w_{k_l}$ with: $\forall i, w_i\neq 1$ and $\forall i,j$, $1\leqq i\leqq j\leqq k_l$, $r(w_i\ldots w_j)=l$.*

Proof. Let

$$r_n=k_n$$
$$r_{n-1}=k_nk_{n-1}$$
$$\vdots$$
$$r_0=k_nk_{n-1}\ldots k_0.$$

We show:

(∗) $\forall l\in\{0,\ldots,n\}\,\forall w\in\mathbf{X}^*$ such that $r(w)=l$ and $|w|\geqq r_l$, w has a factor of the form $w_1\ldots w_{k_l}$ like above.

– If $|w|\geqq r_n=k_n$ and $r(w)=n$, w has a factor $x_1\ldots x_{k_n}$, $x_i\in\mathbf{X}$, and: $\forall i\leqq j$

$$n\geqq r(x_i\ldots x_j)\geqq r(w)=n\Rightarrow r(x_i\ldots x_j)=n.$$

– Let $0\leqq l<n$ and suppose (∗) is true for $l'>l$. Let w be a word such that $|w|\geqq r_l=k_lr_{l+1}$ and $r(w)=l$; w has a factor $w_1w_2\ldots w_{k_l}$ with $\forall i\,|w_i|=r_{l+1}$.

If for an i, $r(w_i)=l'>l$, we conclude by induction, because $|w_i|=r_{l+1}\geqq r_{l'}$.
On the other hand, if $\forall i$, $r(w_i)\leqq l$, then for $i\leqq j$

$$l=r(w)\leqq r(w_i\dots w_j)\leqq r(w_i)\leqq l\Rightarrow r(w_i\dots w_j)=l. \quad \square$$

Let $V=\mathbf{K}^n$. Let us recall that the *tensor algebra* of V is defined by the direct sum

$$T(V)=\bigoplus_{k\geqq 0} V^{\otimes k}$$

where $V^{\otimes k}$ denotes the k-fold tensor product of V and in particular $V^{\otimes 0}=\mathbf{K}$. It is a graded algebra.

The *exterior algebra* of V (or Grassmann algebra), denoted by $\wedge V$, is by definition the quotient of $T(V)$ by the relations

$$v\otimes v\sim 0, \qquad v\in V$$

that is, the quotient of $T(V)$ by the ideal generated by the elements $v\otimes v$, $v\in V$. This ideal is homogeneous hence $\wedge V$ is also a graded algebra

$$\wedge V=\bigoplus_{k\geqq 0} \bigwedge^k V$$

where $\bigwedge^k V$ is the image of $V^{\otimes k}$ in $\wedge V$. It is well-known that

$$\dim(\bigwedge^k V)=\binom{n}{k}.$$

In particular $\bigwedge^0 V=\mathbf{K}$, $\bigwedge^1 V=V$ and for $k>n$ $\bigwedge^k V=0$. The product in $\wedge V$ is denoted by $\wedge$. If $v, w\in V$ we have $(v+w)\wedge(v+w)=0$ hence $v\wedge w=-w\wedge v$.

This implies that if $v_1, v_2, \dots, v_r$ are linearly dependant vectors in V then

$$(1) \quad v_1\wedge v_2\wedge\dots\wedge v_r=0$$

The converse of this fact is true:if (1) holds then $v_1, v_2, \dots, v_r$ are linearly dependant (see [3] Th. 1).

Let E be a subspace of V and $(e_1, e_2, \dots, e_k)$ a basis of E. We define an element $\bar{E}$ of $\wedge V$ by

$$\bar{E}=e_1\wedge e_2\wedge\dots\wedge e_k.$$

If we had chosen another basis for E, $\bar{E}$ would have been multiplied by a non zero scalar [3, Corollaire 2]. We define in this way a mapping from the set of subspaces of V into $\wedge V$ by

$$E\mapsto\bar{E}.$$

If $E=0$ we define $\bar{E}=1$. The above result implies that if E and F are subspaces of V then

$$E\cap F=0\Leftrightarrow\bar{E}\wedge\bar{F}\neq 0 \quad \text{(see [3] Proposition 5).}$$

This will be very useful in the sequel. Another useful remark is

$$\bar{E} \in \bigwedge^{\dim(E)} V.$$

Proof of Theorem 3. Let $k_0 = 1$, $k_n = 1$ and $\forall i \in \{1, \dots, n-1\}$ $k_i = \binom{n}{i} + 1$. Let $N(n) = k_0 k_1 \dots k_n$, $r : \mathbf{X}^* \to \{0, \dots, n\}$ the mapping defined by $r(w) = \operatorname{rank}(\mu w)$ and w a word of length at least $N(n)$. By Lemma 3, there exists l, $0 \leqq l \leqq n$, such that w has the factor $w_1 \dots w_{k_l}$ with $\forall i$, $w_i \neq 1$ and $\forall i \leqq j$, $r(w_i \dots w_j) = l$.

If $l = 0$, $r(w_1) = 0$ and $\mu w_1 = 0$ is pseudo-regular.

If $l = n$, $r(w_1) = n$ and μw_1 is invertible hence pseudo-regular. Suppose $1 < l < n-1$.

Let $E_i = \operatorname{Im}(\mu w_i)$ i.e. the image subspace of μw_i.

$F_i = \operatorname{Ker}(\mu w_i)$ i.e. the kernel of μw_i.

We have: $\forall j$, $1 \leqq j \leqq k_l - 1$, $r(w_j w_{j+1}) = r(w_j)$ hence $E_j \cap F_{j+1} = 0 \Rightarrow \bar{E}_j \wedge \bar{F}_{j+1} \neq 0$.

On the other hand, $\forall i, j$, $1 \leqq i \leqq j \leqq k_l$, $r(w_i \dots w_j) = r(w_i) = r(w_j)$ hence

$$\operatorname{Im}(\mu w_i \dots w_j) = \operatorname{Im}(\mu w_j) = E_j \quad \text{and} \quad \operatorname{Ker}(\mu w_i \dots w_j) = F_i.$$

Suppose that for all i, j, $1 \leqq i \leqq j \leqq k_l$, $\mu w_i \dots w_j$ is not pseudo-regular; then

$$\operatorname{Im}(\mu w_i \dots w_j) \cap \operatorname{Ker}(\mu w_i \dots w_j) \neq 0 \quad \text{and this implies } \bar{E}_j \wedge \bar{F}_i = 0.$$

But for each $j \in \{1, \dots, k_l\}$, $\bar{F}_j \in \bigwedge^{n-l} V$ the dimension of which is equal to $\binom{n}{n-l} = \binom{n}{l} = k_l - 1$. This implies that there exists j, $1 \leqq j \leqq k_l - 1$ such that $\bar{F}_{j+1}$ is a linear combination of the $\bar{F}_i$, $i \leqq j$:

$$\bar{F}_{j+1} = \sum_{i \leqq j} \alpha_i \cdot \bar{F}_i \qquad (\alpha_i \in \mathbf{K}).$$

Hence $\bar{E}_j \wedge \bar{F}_{j+1} = \sum_{i \leqq j} \alpha_i \bar{E}_j \wedge \bar{F}_i = 0$, a contradiction. □

2. An Ogden-like Iteration Theorem

Let w be a word of length k: $w = x_1 x_2 \dots x_k$ ($x_i \in \mathbf{X}$). *A set of l marked positions in* w is a subset E of cardinality l of $\{1, \dots, k\}$; if w is written $a u b$, we say that *the factor u of w contains m marked positions* if $u = x_i \dots x_j$ and $E \cap \{i, i+1, \dots, j\}$ has cardinality m.

Theorem 4. *Let* $\mathbf{X}$ *be an alphabet and* $s \in \mathbf{K}\langle\langle \mathbf{X} \rangle\rangle$ *a recognizable series. There exists* N *such that for each word* $w \in \operatorname{supp}(s)$ *having at least* $N+2$ *marked positions,* w *can be written* $a u b$ *where* a (resp. b) *contains at least one marked position,* u *contains at least one and at most* N *marked positions and such that:*

$$\operatorname{supp}(s) \cap a u^* b \quad \textit{is infinite}.$$

Proof. We have $(s, w) = \lambda \mu w \gamma$ where μ is an homomorphism $\mathbf{X}^* \to \mathbf{K}^{n \times n}$. Let $N = N(n)$ [cf. Th. 3′]; w has a factorization $a u_1 \dots u_N b$ where each u_i contains exactly one marked position and a (resp. b) contains at least one marked position. By Theorem 3′ there exist i, j, $1 \leqq i \leqq j \leqq N$ such that $\mu u_i \dots u_j$ is pseudo-regular. We conclude then like in the proof of Theorem 2. □

Application. Iteration lemmas are often used to prove that a given language does not belong to a given family of languages. From this point of view, Theorem 4 is more "powerful" than Theorem 2, as shows the following example due to Boasson [2]:

$$L = \{y x^{i_1} y x^{i_2} \dots y x^{i_k} \mid k \geqq 1 \;\&\; \forall j,\ 1 \leqq j \leqq k,\ i_j \geqq j\}.$$

– If $w = aub \in L$ and $|u| \geqq 2$, then u contains at least one occurrence of x, hence $u = u_1 x u_2$ and $a u_1 x^+ u_2 b \subset L$. This implies: $a u_1 x^* u_2 b \cap L$ is infinite.
(x^+ denotes $x^* \setminus 1$).
Theorem 2 can therefore not be used to show that L is not the support of a recognizable series.
– Let $N \geqq 1$ and $w = y x y x^2 y x^3 \dots y x^{N+2}$ where the $N+2$ occurrence of y's are marked. If $w = aub$ where u contains at least one marked position, then it is easy to show that for large enough n $a u^n b \notin L$. Hence $a u^* b \cap L$ is finite, and therefore, by Theorem 4, L is not the support of a recognizable power series.

Acknowledgements. The author is grateful to Jean Berstel for many helpful discussions and for suggesting Theorem 4.

References

1. Berstel, J.: Transductions and context free languages. Stuttgart: Teubner 1979
2. Boasson, L.: Private communication
3. Bourbaki, N.: Algèbre, chapitre 3 (algèbre multilinéaire) § 7 n° 3. Paris: Hermann 1958
4. Eilenberg, S.: Automata, languages and machines. vol. A. New York: Academic Press 1974
5. Jacob, G.: Un théoreme de factorisation des produits d'endomorphismes. J. Algebra, (in press 1979)
6. Ogden, W.: A helpful result for proving inherent ambiguity. Math. System Theory **2**, 191–194 (1968)
7. Ranum, A.: The group-membership of singular matrices. Amer. J. Math. **31**, 18–41 (1909)
8. Schützenberger, M.P.: On a special class of recurrent events. Ann. of Math. **32**, 1201–1213 (1961)

Received May 21 / Revised October 15, 1979