Semigroup Forum Vol. 23 (1981)327-342

RESEARCH ARTICLE

SEMISIMPLICITY OF THE ALGEBRA ASSOCIATED TO A BIPREFIX CODE

Christophe Reutenauer

Communicated by G. Lallement

1. INTRODUCTION

There exists a canonical way to associate to each language (that is, to each subset of a free monoid) an algebra on a given field: we call it its syntactic algebra. This construction is in fact a particular case of a more general one that applies to formal power series in non commutative variables similar to the construction of the syntactic monoid of a language. In this paper we are interested in syntactic algebras of a special class of languages : free submonoids of the free monoid.

Recall that a submonoid of a free monoid is not necessarily free, and that if it is, then it admits a unique basis : such a basis is also called a code. A code is said to be prefix if it contains no left factor of any of its elements (this condition ensures that it is a code) and biprefix if the dual condition is also fullfilled. We call (by a slight abuse of language) syntactic algebra of a code the syntactic algebra of the submonoid it generates. When the code is

0037-1912/81/0023-0327 $03.20

rational, then its syntactic algebra is finite dimensional.

Our first theorem is the following : if a code is rational and biprefix, then its syntactic algebra is semisimple (theorem 1). Here then field is assumed to be of characteristic zero, or of a characteristic not dividing the order of the Suschkewitch group of the code. Observe that this result is a generalization of Maschke's theorem because to each finite group, one can canonically associate a rational biprefix code whose syntactic algebra is the group algebra. Of course, we need the theorem of Maschke in the course of the proof of the result above.

As a converse we prove the following result : if the syntactic algebra of a rational and maximal code (maximal as a code) is semisimple, then the code is biprefix (theorem 2). Hence, one obtains that a rational and maximal code is biprefix if and only if its syntactic algebra is semisimple.

Let us give an outline of the proofs. As it is easily seen, there is a canonical surjective algebra homomorphism

$$\nu : K[M] \to \mathcal{M}$$

where M is the syntactic monoid of the code C, $K[M]$ the K-algebra of this monoid and $\mathcal{M}$ the syntactic algebra of C. We show that if C is biprefix, then the radical of $K[M]$ is contained in $\mathrm{Ker}\,\nu$; thus $\mathcal{M}$ is semisimple. Conversely, if $\mathcal{M}$ is semisimple, let S be the minimal ideal of M. Then the radical of $K[S]$ is seen to be contained in $\mathrm{Ker}\,\nu$. This implies that the canonical image in M of the submonoid generated by C meets all maximal subgroups of S, showing that C is biprefix. The two proofs use strongly Suschkewitsch's theorem.

2A. RATIONAL CODES AND (0)-MINIMAL IDEALS.

For most of the results not proved here, see [1], [2] or [5]. We fix an alphabet X (that is, a finite non empty set) whose elements are called letters. X^* denotes the free monoid generated by X, whose elements are called words ; its neutral element, the empty word, is denoted by 1. A language is a subset of X^*.

The rational languages are defined in the following way :

- Each finite language is rational.
- If L_1 and L_2 are rational, then their union and their product $L_1 L_2 = \{uv | u \in L_1, v \in L_2\}$ are rational.
- If L is rational, then the submonoid it generates $L^* = \bigcup_{n \geqslant 0} L^n$ is rational.

The syntactic congruence of a language L is the largest congruence on X^* for which L is a union of classes ; we denote it by $\sim$. Then one has

(1) $u \sim v$ if and only if for all words a and b, $aub \in L \Leftrightarrow avb \in L$.

The syntactic monoid of a language is the quotient of X^* by its syntactic congruence. By Kleene's theorem, a language is rational if and only its syntactic monoid is finite.

Recall that a submonoid M of X^* is not always a free monoid, but that this is the case if and only if for all words u and v

(2) $u, uv, vu \in M \Rightarrow v \in M$

A language C is a code if the submonoid C^* generated by C is free, with basis C ; this basis is necessarily unique and it is also the smallest generating set of C . Equivalently, C is a code if and only if for all words $u_1, \ldots, u_n$, $v_1, \ldots, v_m$ in C, one has

$$u_1 \ldots u_n = v_1 \ldots v_m \Rightarrow n = m \text{ and } u_i = v_i$$

for each i.

A language C is called prefix if for all words u and v

(3) $u, uv \in C \Rightarrow v = 1$

A prefix language different from $\{1\}$ is a code and in this case we call it a prefix code. A submonoid M of X^* is generated by a prefix code if and only if for all words u and v one has

(4) $u, uv \in M \Rightarrow v \in M$

In this case we say that M is right unitary. A code C is called biprefix if both C and its mirror image are prefix, that is if C satisfies (3) and the dual condition

(5) $u, vu \in C \Rightarrow v = 1$

Biprefix codes were introduced and studied by Schützenberger [10].

As a corollary to Kleene's theorem, one shows that a code C is rational if and only if C^* is rational. Note that a finite code is always rational. A more sophisticated result, due to Schützenberger, is that a rational code is maximal (C is maximal if for any code C' containing C, $C' = C$) if and only it is complete (C is complete if C meets each ideal of X^*).

By an abuse of language, the syntactic monoid of a code C will mean the syntactic monoid of C^*.

Let M be a finite monoid. Then M has an ideal which is the smallest ideal of M : it is called the minimal ideal of M. Now two cases may occur : either this ideal has at least two elements or it has only one element ; in the last case, this element is the zero of M and M possesses at least one ideal which is minimal in the set of all ideals containing properly the zero : such an ideal is called a 0-minimal ideal.

Let C be a rational code and M its syntactic monoid ; M is finite by Kleene's theorem. If C is complete, M does not have a zero.

If C is not complete, M has a zero and only one 0-minimal ideal. Following the notation of [5] chapter 8 the minimal ideal in the first case, and the 0-minimal ideal in the second case, will be called the (0)-minimal ideal of M.

Further, the image of C^* in M meets this (0)-minimal ideal but does not contain zero.

A semigroup is called simple if it has only one ideal.

A semigroup with a zero is called 0-simple if it has only two ideals (the semigroup itself and the zero) and if it is not of square zero. To unify the notations, we call such a semigroup (0)-simple, following [5] chapter 8. If a finite semigroup S is (0)-simple, it is isomorphic to a Rees-matrix semigroup (see [1] chapter 3 or [5] chapter 3).

(6) $$S \cong \mathcal{M}_0(G, I, \Lambda, P)$$

where G is a finite group, I and Λ are finite sets and $P = (p_{\lambda,i})$ is a $\Lambda \times I$ matrix with coefficients in $G \cup 0$. Each element in S has the form $(g)_{i,\lambda}$ where $g \in G$, $i \in I$, $\lambda \in \Lambda$ or is zero (in case S has a zero). The composition is defined by

$$(g)_{i,\lambda}\,(h)_{j,\mu} = (g\, p_{\lambda,j} h)_{i,\mu} \quad \text{if} \quad p_{\lambda,j} \neq 0$$
$$= 0 \quad \text{if} \quad p_{\lambda,j} = 0$$

If S has no zero, then $p_{\lambda,i} \neq 0$ for any λ, i. G is uniquely determined by S and is called the structure group of S. We shall often use the following normalization : let $i_o \in I$, $\lambda_o \in \Lambda$; we may suppose, without loss of generality, that $i_o = \lambda_o = 1 \in I \cap \Lambda$. Furthermore, it is possible to assume that for any $i \in I$ and $\lambda \in \Lambda$

(7) $$p_{1,i},\ p_{\lambda,1} \in \{0, e\}$$

where e is the unit element of G (see [5] corollary 2.9 of chapter 3).

The following lemma is a classical consequence of the Rees-Suchkewitsch theorem ; we give the proof for sake of completeness.

LEMMA 1 Let $S = \mathcal{M}(G,I,\Lambda,P)$ be a finite Rees-matrix semigroup and S' a subsemigroup not containing zero. Then there exist subsets I' of I and Λ' of Λ and a subgroup H of G such that

$$S' = \{ (g)_{i,\lambda} \mid g \in H,\ i \in I',\ \lambda \in \Lambda' \}$$

and for any $\lambda \in \Lambda'$, $i \in I'$ $p_{\lambda,i} \in H$.

PROOF Following the remarks above, suppose $1 \in I \cap \Lambda$ and that (7) holds. Suppose also that S' meets the set $\mathcal{H} = \{ (g)_{1,1} \mid g \in G \}$ (i.e the $\mathcal{H}$-class of coordinate $(1,1)$).

Since $0 \notin S'$, one has $p_{1,1} \neq 0$ hence $p_{1,1} = e$. It follows that the mapping

$$(g)_{1,1} \mapsto g$$

from $\mathcal{H}$ onto G is an isomorphism. Let H be the image of $S' \cap \mathcal{H}$: H is a subsemigroup of a finite group hence a subgroup. In particular, $(e)_{1,1} \in S'$. Similarly, if S' meets the $\mathcal{H}$-class of coordinates (i,λ), say $\mathcal{H}'$, then $p_{\lambda,i} \neq 0$ and the mapping

$$\mathcal{H}' \mapsto G$$

$$(g)_{i,\lambda} \mapsto g\, p_{\lambda,i}$$

is an isomorphism, hence the image of $S' \cap \mathcal{H}'$ is a subgroup H' of G and in particular $(p^{-1}_{\lambda,i})_{i,\lambda} \in S'$. But $(g)_{i,\lambda} \in S'$ implies $(g)_{1,1} = (e)_{1,1}(g)_{i,\lambda}(e)_{1,1} \in S'$ hence $g \in H$. It follows $p^{-1}_{\lambda,i} \in H$ and $p_{\lambda,i} \in H$. Hence $H' p^{-1}_{\lambda,i} \subset H$ and $H' \subset H$. Conversely $h \in H$ implies

$$(p^{-1}_{\lambda,i}\, h\, p^{-1}_{\lambda,i})_{i,\lambda} = (p^{-1}_{\lambda,i})_{i,\lambda}\, (h)_{1,1}\, (p^{-1}_{\lambda,i})_{i,\lambda} \in S'$$

hence $H = p^{-1}_{\lambda,i} H \subset H'$ which implies $H = H'$.

To conclude the proof, we remark that if S' meets the $\mathcal{H}$-classes

(i,λ) and (j,μ) then (taking product), since $0 \notin S'$, S' meets the $\mathcal{H}$-class (i,μ). □

Let C be a rational code. Then the (0)-minimal ideal of the syntactic monoid of C is a finite (0)-simple semigroup whose structure group is called the Suschkewitsch group of C.

LEMMA 2 Let C be a rational code, M its syntactic monoid, S the (0)-minimal ideal of M and S' the intersection of S and of the image M' of C^* in M. Following the notation of lemma 1, C is prefix if and only if

(8) $\forall\ \lambda \in \Lambda'$, $\forall i \in I \setminus I'$ $\quad p_{\lambda,i} = 0$

Furthermore C is biprefix if and only if (8) holds together with the symmetric condition.

(9) $\forall i \in I'$, $\forall\ \lambda \in \Lambda \setminus \Lambda'$ $\quad p_{\lambda,i} = 0$.

In case C is complete, that is, when S has no zero (and hence $p_{\lambda,i} \neq 0$ for any i,) condition (8) says exactly that $I' = I$. This is equivalent to the fact that M' meets all minimal right ideals in M, hence that C^* meets all right ideals in X^* : this is just proposition 4.2 in [5] chapter 6, due to Schützenberger

PROOF Suppose that C is prefix. Then by (4) for any x,y in M : $x,\ xy \in M'$ implies $y \in M'$. Suppose now that $p_{\lambda,i} \neq 0$ for some $\lambda \in \Lambda$ and $i \in I \setminus I'$. Then we have $(e)_{1,\lambda} \in S' \subset M'$ (assuming $1 \in I'$ and following (7)), but also $(e)_{1,\lambda}\ (p^{-1}_{\lambda,i})_{i,\lambda} = (e)_{1,\lambda} \in M'$, hence $(p^{-1}_{\lambda,i})_{i,\lambda} \in M'$, which cannot be true because $i \notin I'$.

Conversely suppose that (8) holds. Let x,y in M be such that $x,\ xy \in M'$. Multiplying x on the left by some element of S', we may assume that $x \in S'$, hence $x = (h)_{i,\lambda}$ with $i \in I'$, $\lambda \in \Lambda'$, $h \in H$ and $xy \in S'$.

Now $yx \in S$ and it is a left multiple of x ; S being finite this implies $yx = (g)_{i',\lambda}$ for some $i' \in I$ and $g \in G$ (see example 3.12 in [5] chapter 2). If $i' \notin I'$, then $p_{\lambda,i'} = 0$ which implies $0 = (h)_{i,\lambda}\ (g)_{i',\lambda} = xyx = (xy)x \in S'$, a contradiction. Hence $i' \in I'$, $p_{\lambda,i'} \in H$ and $(h\ p_{\lambda,i'}\ g)_{i,\lambda} = (h)_{i,\lambda}\ (g)_{i',\lambda} \in S'$ implies $g \in H$. Thus $yx \in S'$. Since $x,xy,yx \in M'$ it follows from (2) that $y \in M'$. Hence C is prefix by (4). □

2.B. FORMAL POWER SERIES AND MONOID ALGEBRAS.

We fix a field K. $K\langle X\rangle$ denotes the set of all noncommutative polynomials on X with coefficients in K ; $K\langle\langle X\rangle\rangle$ denotes the set of noncommutative formal power-series, which is isomorphic to the set of all mappings

$$S : X^* \to K$$

A series S is denoted by

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

where (S,w) denotes the image by S of the word w. $K\langle\langle X\rangle\rangle$ is the dual space of $K\langle X\rangle$ viewed as a vector space over K. Duality is denoted by (S,P) for each formal power-series S and for each polynomial P. One has

$$(S,P) = \sum_{w \in X^*} (S,w)\ (P,w)$$

(this sum is finite because P is a polynomial), Considering S as a linear form on $K\langle X\rangle$ we define as usual

$$\text{Ker}\ \ S = \{P \in K\langle X\rangle \mid (S,P) = 0\}$$

The syntactic ideal of S is the largest (two-sided) ideal of $K\langle X\rangle$ contained in Ker S. This ideal exists because a sum of ideals is an ideal.

The set of rational formal power series is defined as the smallest subalgebra of $K\langle\langle X\rangle\rangle$ containing $K\langle X\rangle$ and the inverse of all its invertible elements (a series S is invertible in $K\langle\langle X\rangle\rangle$ if and only if its constant term $(S,1)$ is nonzero). A formal power-series S is called recognizable if there exists a linear representation of S of dimension $n \geq 1$, that is a triple (λ,α,γ) where $\lambda \in K^{1xn}$, $\gamma \in K^{nx1}$ and α is an algebra homomorphism

$$\alpha : K\langle X\rangle \to K^{nxn}$$

such that $(S,w) = \lambda\, \alpha w\, \gamma$ for each word w (K^{ixj} denotes the set of all (i,j)-matrices over K).

By the Kleene-Schützenberger theorem, a power series is recognizable if and only if it is rational.

As a corollary (see [9] th. II.1.2) one obtains that a power series is rational if and only if its syntactic algebra is finite dimensional.

Let L be a language that contains no ideal of X^*. The characteristic power-series of L, also denoted by L, is

$$L = \sum_{w \in L} w$$

Let M be the syntactic monoid of L. Denote $K_o[M]$ the contracted algebra of M : this is just the algebra $K[M]$ of M if M has no zero, and if M has a zero, it is obtained from $K[M]$ by identifying the zero of $K[M]$ and the zero of M (see [1] chapter 5§2). The canonical morphism

$$\varphi : X^* \to M$$

extends to an algebra homomorphism

$$\varphi : K\langle X\rangle \to K_o[M]$$

Let ψ be the linear form on $K[M]$ defined for each $m \in M$ by $\psi(m) = 1$ if $m \in \varphi(L)$ and $\psi(m) = 0$ if not. Since L does not contain any ideal of X^* the image by ψ of the eventual zero of M

is zero, hence ψ induces a linear form, also denoted by ψ

$$\psi : K_o[M] \to K$$

such that $L = \psi \circ \rho$ (here L denotes the linear form on $K\langle X\rangle$ associated to L). Hence $\operatorname{Ker}\rho$ is an ideal contained in Ker L, and denoting by $\mathcal{M}$ the syntactic algebra of L and μ the homomorphism $\mu: K\langle X\rangle \to \mathcal{M}$, we obtain the following commutative diagramm :

(10)

$$\begin{array}{ccc} & K\langle X\rangle & \\ {\scriptstyle\rho}\swarrow & & \searrow{\scriptstyle\mu} \\ K_o[M] & \overset{\nu}{\dashrightarrow} & \mathcal{M} \end{array}$$

(see [9] I.3).

In particular, if L is a rational language, M is finite hence $\mathcal{M}$ is finite dimensional and L is a rational power-series.

Let S be a finite (0)-simple semigroup and $K_o[S]$ the contracted algebra of S. Recall that in a finite dimensional algebra, the radical can be defined as the largest nilpotent ideal, see [4]. Denote by R' the radical of $K_o[S]$. By the Teissier-Munn theorem (see 6 p. 404) we have

$$R' = \{ x \in K_o[S] \mid SxS = 0 \}$$

We shall only need a weak form of this result, namely :

LEMMA 3 Let S be a finite (0)-simple semigroup, K a field whose characteristic does not divide the order of the structure group G of S, e an idempotent in S and R' the radical of $K_o[S]$. Then $e R' e = 0$.

PROOF If S has no zero, eSe is a group isomorphic to G (use e.g. the Rees matrix form of S) and if S has a zero, $eSe \cong G \cup 0$. Hence in both cases the image of the mapping $K_o[S] \to K_o[S]$, $x \mapsto exe$

is isomorphic to $K[G]$. Recall that, by Maschke's theorem, $K[G]$ has no nonzero nilpotent ideal (see [4] th. 1.4.1). Now, R' is a nilpotent ideal of $K_o[S]$ (because $K_o[S]$ is finite dimensional) hence $e R' e$ is a nilpotent ideal of $K[G]$. Indeed, if $x \in K[G]$ then $x = exe$, hence $xe R'e = exe R' e \subset e R' e$ because R' is an ideal ; thus $e R' e$ is an ideal in $K[G]$. Furthermore, there exists k such that $R'^k = 0$; it follows $(e R' e)^k \subset R'^k = 0$ and $e R' e$ is nilpotent. This shows that $e R' e = 0$. □

3. THE MAIN RESULT.

We call syntactic algebra of a code the syntactic algebra of the submonoid generated by the code.

THEOREM 1 Let C be a rational biprefix code and K a field whose characteristic does not divide the order of the Suschkewitsch group of C. Then the syntactic algebra of C, is semisimple.

REMARKS 1. This statement contains Maschke's theorem. Indeed let G be a finite group of order not divisible by the characteristic of K. Consider the alphabet $X = G$ and let $\varphi : X^* \to G$ be the canonical morphism. Let $M = \varphi^{-1}(e)$ where e is the identity of G. Then M satisfies (4) and the dual condition. Thus M is a free submonoid generated by a rational biprefix code. Further-more the syntactic monoid of M is G, which is the Suschkewitsch group of the code. It is not difficult to show that the syntactic algebra of M is $K[G]$ (because the only ideal of $K[G]$ contained in the kernel of the linear form $e \mapsto 1$, $g \mapsto 0$ if $g \neq e$, is zero). Hence theorem 1 shows that $K[G]$ is semisimple.2. Let C be a rational (or even finite) complete code and M its syntactic monoid. Then it is not true in general that $K[M]$ is semisimple. Indeed, let S be the

minimal ideal of M. If K[M] is semisimple, then K[S] is also semisimple and this is true only if S is a group, by a theorem of Teissier ([1] corollary 5.24 chapter 5). Now, in general, S is not a group (see e.g. [8] p. 35).

However, Perrin showed that a finite complete code is biprefix if and only if its syntactic monoid is nil-simple (M with identity e is nil-simple if there exists some $k \geq 1$ such that $(M \setminus e)^k$ is contained in the minimal ideal of M) see [7] corollary 5.4.

PROOF OF THEOREM 1 Let $\mathcal{M}$ be the syntactic algebra of C and

$$\mu : K\langle X\rangle \to \mathcal{M}$$

the canonical algebra homomorphism. Let M be the syntactic monoid of C and

$$\varphi : X^* \to M$$

the canonical monoid homomorphism. As we have seen (see diagram (10) and the remarks preceding it) φ extends to a canonical algebra homomorphism

$$\varphi : K\langle X\rangle \to K_o[M]$$

Let $M' = \varphi(C^*)$. C^* does not contain any ideal otherwise, by (2), we should have $C^* = X^*$ and hence $C = X$, a trivial case which we exclude. Hence the mapping

$$\psi : M \to K$$

$$m \mapsto 1 \quad \text{if} \quad m \in M'$$

$$m \mapsto 0 \quad \text{if not}$$

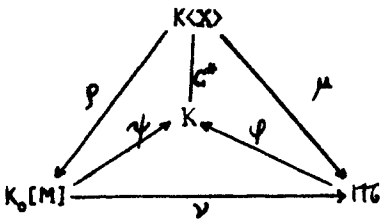
induces a linear form

$$\psi : K_o[M] \to K$$

such that $C^* = \psi \circ \varphi$ (ibid.) ; in this last equality, C^* denotes the linear form on $K\langle X\rangle$ defined by C^*. Furthermore, the syntactic ideal $\operatorname{Ker}\mu$ of C^* is contained in $\operatorname{Ker} C^*$; hence the linear

form C^* induces a linear form φ on $\mathcal{H}$. Thus the following diagramm is commutative

(11)



(see (10)).

Let S be the (0)-minimal ideal of M and $S' = M' \cap S$. $K_0[S]$ embeds into $K_0[M]$. Let R' be the radical of $K_0[S]$. Let $S = \mathcal{M}(G,I,\Lambda,P)$ where G is the Suschke witsch group of C ; we may suppose that relation (7) holds and that S' meets the $\mathcal{H}$-class of coordinates (1,1). Let $e_1 = (e)_{1,1} \in S'$ be the idempotent of this $\mathcal{H}$-class. Then (lemma 3)

$$e_1 R' e_1 = 0$$

Let x be an element of R'. Then x can be written

$$x = \sum_{\substack{g \in G \\ i \in I,\ \lambda \in \Lambda}} a_{g,i,\lambda} \ (g)_{i,\lambda} \quad (a_{g,i,\lambda} \in K)$$

Thus we have $e_1 \, x \, e_1 = 0$. Now lemma 2 shows that $p_{\lambda,i} = 0$ if $\lambda \in \Lambda'$ and $i \in I \setminus I'$ or if $\lambda \in \Lambda'$ and $i \in I \setminus I'$. Hence (because $1 \in I' \cap \Lambda'$), $i \notin I'$ or $\lambda \notin \Lambda'$ implies $(e)_{1,1} (g)_{i,\lambda} (e)_{1,1} = 0$. Furthermore if $i \in I'$ and $\lambda \in \Lambda'$, then by lemma 2 and (7) we have $p_{1,i} = p_{\lambda,1} = e$, hence $(e)_{1,1}(g)_{i,\lambda}(e)_{1,1} = (g)_{1,1}$. Thus

$$\sum_{\substack{\lambda \in \Lambda', i \in I' \\ g \in G}} a_{g,i,\lambda} \ (g)_{1,1} = 0$$

and this implies that for any $g \in G$

$$\sum_{\lambda \in \Lambda',\ i \in I'} a_{g,i,\lambda} = 0$$

Now, lemma 1 together with this relation shows that

$$\psi(x) = \sum_{\substack{g \in H \\ i \in I', \lambda \in \Lambda'}} a_{g,i,\lambda} = 0$$

proving that $R' \subset \operatorname{Ker} \psi$.

Now, let R be the radical of $K_o[M]$. Then, S being an ideal in M, $K_o[S]$ is an ideal in $K_o[M]$, hence

$$R' = R \cap K_o[S]$$

(see [4] th. 1.2.5). Hence if $x \in R$, $e_i x \in R'$ (recall that $e_1 \in S' = S \cap M^1$) and by what we have just seen $\psi(e_1 x) = 0$.

Now, C being a prefix code, (4) implies that for any m in M

$$m \in M' \Leftrightarrow e_1 m \in M'$$

Let $x = \sum_{m \in M} a_m m \qquad (a_m \in K)$

Then $\psi(x) = \sum_{m \in M'} a_m$

and $$e_1 x = \sum_{m \in M} a_m e_1 m$$

hence

$$0 = \psi(e_1 x) = \sum_{e_1 m \in M'} a_m = \sum_{m \in M} a_m = \psi(x).$$

Therefore $R \subset \operatorname{Ker} \psi$ and $\mathcal{M}$ is a quotient of the semisimple algebra $K_o[M]/R$ hence is semisimple (see [4] th. 1.4.4). □

REMARK It is possible to show that $\mathcal{M}$ is equal to $\nu(K_o[S])$.

We come now to the converse of theorem 1, under the stronger hypothesis that C is complete (or maximal, see § 1). We assume that the characteristic of K does not divide the order of the Suschkewitsch group of C.

THEOREM 2 If a complete rational code has a semisimple syntactic algebra, then it is biprefix.

COROLLARY A complete rational code is biprefix if and only if its syntactic algebra is semisimple.

REMARK Without the assumption "complete" theorem 2 is not true as shown by the example of $C = \{x, yx\}$ which is prefix but not biprefix and has K^{2x2} as syntactic algebra (x,y are letters).

PROOF OF THEOREM 2. We keep the notation of the beginning of the preceding proof. If $\mathcal{M}$ is semisimple, then $\nu(K_o[S])$ is semisimple, being an ideal in $\mathcal{M}$. This implies that the radical R of $K_o[S]$ is contained in Ker ν. Let $S = \mathcal{M}(G,I,\Lambda,P)$. C being complete, S has no zero and the $p_{\lambda,i}$ are all in G. Using the notations of lemma 2, we show that $I' = I$ and $\Lambda = \Lambda'$ (which implies that C is biprefix). Let $i,j \in I$ and $\lambda \in \Lambda'$. Put

$$x = \sum_{g \in G} (g)_{i,\lambda} - (g)_{j,\lambda}$$

Then for each $s \in S$, $s = (h)_{k,\mu}$, one has

$$sx = \sum_{g \in G} (h\, p_{\mu,i} g)_{k,\lambda} - \sum_{g \in G} (h\, p_{\mu,j} g)_{k,\lambda} = 0$$

because $G = h\, p_{\mu,i}\, G = h\, p_{\mu,j}\, G$. Hence the ideal generated by x is nilpotent and thus $x \in R$. Therefore

$$\psi(x) = \varphi \circ \nu(x) = \varphi(0) = 0$$

Suppose now $I \setminus I' \neq \emptyset$ and $i \in I'$, $j \notin I'$. Then $\psi((g)_{i,\lambda}) = 1$ if $g \in H$ and $\psi((g)_{i,\lambda}) = 0$ if not (see lemma 1).
Furthermore $\psi((g)_{j,\lambda}) = 0$ for all g. Hence $0 = \psi(x) = \mathrm{Card}(H)$ which contradicts the assumption on the characteristic of K. Hence $I' = I$ and similarly $\Lambda' = \Lambda$. □

AKNOWLEDGEMENTS I want to express my gratitude to Pr. Betréma for many helpul discussions, which contributed in particular to simplify the proof of theorem 1.

REFERENCES

[1] Clifford A.H. and G.B. Preston, The Algebraic Theory of Semigroups, A.M.S. Providence (1961).

[2] Eilenberg S., Automata, Languages and Machines vol. A Academic Press New York (1974).

[3] Fliess M., Matrices de Hankel, J. Maths Pures et Appliquées 53 197-224 (1974).

[4] Herstein I.N., Noncommutative Rings, The Carus Mathematical Monographs (1968).

[5] Lallement G., Semigroups and Combinatorial Applications, John Wiley New York (1979).

[6] Lallement G. and M. Petrich, Irreducible matrix representations of finite semigroups, Trans. Amer. Math. Soc. 139 (1969) 393-412.

[7] A. de Luca, D. Perrin, A. Restivo and S. Termini : Synchronization and simplification, Discrete Mathematics 27 (1979) 297-308.

[8] Perrin D., Codes bipréfixes et groupes de permutations, Thèse de Doctorat d'Etat, Université de Paris 7 (1975).

[9] Reutenauer C., Séries formelles et algèbres syntactiques, J. Algebra 66 (1980) 448-483.

[10] Schützenberger M.P., On a special class of recurrent events, Annals of Math. Stat. 32 (1961) 1201-1213.

Institut de Programmation
Université Pierre et Marie Curie
4 Place Jussieu
Paris, 75230 Cedex 05

Received June 10, 1981, and September 24, 1981 in final form.