JOURNAL OF COMBINATORIAL THEORY, Series A 38, 48–57 (1985)

The Shuffle Algebra on the Factors of a Word Is Free

CHRISTOPHE REUTENAUER

Institut de Programmation, 4 Place Jussieu, Paris 75005, France

Communicated by the Managing Editors

Received January 11, 1983

DÉDIÉ À M. P. SCHÜTZENBERGER

The shuffle algebra generated by the factors of a given word is shown to be free, with transcendance degree equal to the dimension of a Lie algebra canonically associated to this word. © 1985 Academic Press, Inc.

Nous montrons que l'algèbre de mélange engendrée par les facteurs d'un mot donné est libre, de degré de transcendance égal à la dimension d'une algèbre de Lie canoniquement associée à ce mot. © 1985 Academic Press, Inc.

I. INTRODUCTION

Let $w = a_1 \cdots a_n$ be a word of length n on the alphabet A. A factor of w is a word of the form $a_i \cdots a_j$, $i \leqslant j$. We show that the shuffle algebra over $\mathbb{Q}$ generated by the factors of w is isomorphic to a free commutative polynomial algebra. Actually, this result is proved twice. Associate to the given word w the $(n+1)$ by $(n+1)$ matrix

$$\sum_{i=1}^{n} a_i E_{i,i+1},$$

where the E's are elementary matrices. We define for each letter a the matrix φa: it is the coefficient of a in the above sum. Let $\mathfrak{M}$ be the (associative) algebra generated by the φa's and $\mathscr{L}$ be the Lie algebra generated by them. We show that the dimension of $\mathfrak{M}$ is equal to the number of distinct factors of w, while the dimension of $\mathscr{L}$ is equal to the transcendance degree of these factors in the shuffle algebra (cf. the theorem). In the course of the proof, we obtain that the shuffle algebra generated by the factors of w is free.

Actually, we prove a more precise result (cf. the proposition): if P is a set

0097-3165/85 $3.00

of words containing each left factor of any of its elements, then the shuffle algebra generated by P is free over some subset of P.

II. Result

Let A be a finite set (called the *alphabet*), whose elements are called *letters.*

We denote by A^* the free monoid generated by A, whose elements are *words* and whose neutral element, the *empty word,* is denoted by 1. Let $\mathbb{Q}\langle A\rangle$ denote the free associative algebra over the field $\mathbb{Q}$ of rational numbers generated by A; in other words, $\mathbb{Q}\langle A\rangle$ is the set of noncommutative polynomials, which may also be identified with the set of mappings $A^* \to \mathbb{Q}$ with finite support. Each polynomial P is a (finite) linear combination of words

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

where (P, w) is the coefficient of the word w. The product in $\mathbb{Q}\langle A\rangle$ is just the one which extends linearly the concatenation of words in A^*, once A^* is identified as a subset of $\mathbb{Q}\langle A\rangle$. In this way, $\mathbb{Q}\langle A\rangle$ becomes an associative algebra, which is noncommutative when $\mathrm{Card}(A) \geqslant 2$. This algebra structure on $\mathbb{Q}\langle A\rangle$ will be referred to as the "Cauchy algebra."

We define now another product on $\mathbb{Q}\langle A\rangle$, the shuffle product [5], denoted by $\sqcup\!\sqcup$ which turns out to be associative and commutative. It suffices to define the product of two words u and v, because A^* is a basis of the vector space $\mathbb{Q}\langle A\rangle$ over $\mathbb{Q}$.

Let $w = a_1 a_2 \cdots a_n$ be a word, with a_i in A. If $I \subset \{1,..., n\}$, we define $w \mid I$ to be the word $a_{i_1} a_{i_2} \cdots a_{i_k}$, when $I = \{i_1 < i_2 < \cdots < i_k\}$.

Let u be of length n and v of length p. Then $u \sqcup\!\sqcup v$ is the polynomial

$$u \sqcup\!\sqcup v = \sum w(I, J),$$

where the sum is extended to all partitions $\{1, 2,..., n+p\} = I \cup J$ with $\mathrm{Card}(I) = n$, $\mathrm{Card}(J) = p$ and $w(I, J) \mid I = u$, $w(I, J) \mid J = v$. This sum has $\binom{n+p}{p}$ summands. With this product, $\mathbb{Q}\langle A\rangle$ will be called the "shuffle algebra."

Example 1. $ab \sqcup\!\sqcup ac = abac + 2aabc + 2aacb + acab.$

With this product, $\mathbb{Q}\langle A\rangle$ becomes a commutative and associative algebra, without zero divisors (see [5]).

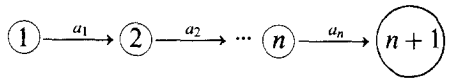
Remark 1. Recall that $\mathbb{Q}\langle A\rangle$ (Cauchy structure) may be identified with the enveloping algebra of the free Lie algebra generated by A over $\mathbb{Q}$.

As an enveloping algebra, it becomes a coalgebra structure, where the coproduct is the homomorphism (concatenation structure) $\mathbb{Q}\langle A\rangle \to \mathbb{Q}\langle A\rangle \otimes \mathbb{Q}\langle A\rangle$ defined by

$$a \mapsto a \otimes 1 + 1 \otimes a, \qquad a \in A.$$

(see [2]). Then the shuffle product is just the transpose of the coproduct.

Let $w = a_1 \cdots a_n$ be a word. We associate to it the graph with $n+1$ vertices and n edges with label in A,

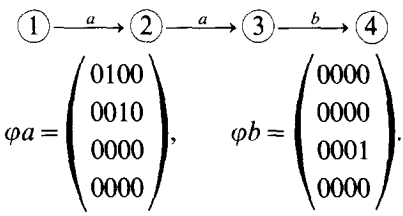


(1)

This graph may be identified with the family of matrices $(\varphi a)_{a \in A}$ in $\mathcal{M}_{n+1}(\mathbb{Q})$ defined by

$$(\varphi a)_{i,i+1} = 1 \qquad \text{if} \quad \text{the } i\text{th letter of } w \text{ is } a,$$
$$(\varphi a)_{i,j} = 0 \qquad \text{in the other cases.}$$

EXAMPLE 2. $w = aab$



Remark 2. The graph is just the minimal automaton of the language $\{w\}$ and the matrices are the linear representation of it; see [3].

A *factor* of w is a word x such that there exist words u and v (possibly empty) with $w = uxv$; if moreover $u = 1$, then x is called a *left factor* of w.

THEOREM. *Let $\mathfrak{M}$ denote the subalgebra (associative with unit) of $\mathcal{M}_{n+1}(\mathbb{Q})$ generated by the matrices φa, $a \in A$. Similarly let $\mathcal{L}$ be the Lie algebra generated by them. Then the dimension of $\mathfrak{M}$ is equal to the number of factors of the word w, while the dimension of $\mathcal{L}$ is equal to the transcendance degree over $\mathbb{Q}$ of this set in the shuffle algebra. Moreover the shuffle algebra generated by the factors of w is a free commutative algebra and admits as a basis a subset of the set of factors of w.*

EXAMPLE 3. Let $w = aab$. Then $\varphi a = E_{12} + E_{23}$, $\varphi b = E_{34}$ (E_{ij} is the (i, j)-elementary matrix). Then $\mathcal{L}$ admits the matrices $E_{12} + E_{23}$, E_{34}, E_{24}, E_{14} as a basis. Moreover, the nonempty factors of w are a, b, aa, ab, aab.

But $aa = \frac{1}{2}(a \sqcup\!\sqcup a)$ and a, b, ab, aab are algebraically independent in the shuffle algebra, because they are Lyndon words, that is, words which are lexicographically minimal in their conjugation class: it is known that these words form a transcendance basis of the shuffle algebra, see [4, Ex. 5.3.6].

III. Proof of the Theorem

(1) The first assertion is easy to prove. The mapping $\varphi: A \to \mathcal{M}_{n+1}(\mathbb{Q})$, $a \mapsto \varphi a$, extends uniquely to a algebra homomorphism $\varphi: \mathbb{Q}\langle A\rangle \to \mathcal{M}_{n+1}(\mathbb{Q})$. We show that the set f, f a factor of w, is a basis of $\mathfrak{M} = \varphi(\mathbb{Q}\langle A\rangle)$ over $\mathbb{Q}$.

First, note that for each word u, the coefficient $(\varphi u)_{i,j}$ is equal to 1 or 0, depending on where there exists (or not) a path from i to j labelled by u in the graph (1). This shows that φu is zero unless u is a factor of w.

The same remark shows that for each factor f of w, of length $|f| = k$, $(\varphi f)_{i,j}$ is equal to 1 only if $j = i + k$ and if w may be written $w = ufv$ with $|u| = i - 1$. Hence φf is a linear combination of elementary matrices $E_{i,i+k}$, $1 \leqslant i \leqslant n+1$. Hence to each factor f of w, there corresponds a unique elementary matrix $E_{i,i+|f|}$ defined by: $(\varphi f)_{i,i+|f|} = 1$ and i is chosen minimal. But $E_{i,i+|f|}$ determines uniquely f, because i determines the beginning of the occurrence of f as a factor of w and $|f|$ determines its length.

Finally, in each linear combination of φg (g factor of w), the coefficient of φf is the coefficient $(i, i+|f|)$ of the resulting matrix. Hence the φf are linearly independent. They span $\mathfrak{M}$ because φA^* spans $\mathfrak{M}$ and, as we saw, $\varphi u = 0$ if u is not a factor of w. Hence the φf form a basis of $\mathfrak{M}$ over $\mathbb{Q}$.

(2) For each word u, define a linear mapping $\bar{u}: \mathbb{Q}\langle A\rangle \to \mathbb{Q}\langle A\rangle$; for each v in A^*, $\bar{u}(v)$ is the word v_1 if $v = v_1 u$ and $\bar{u}(v) = 0$ if v does not end with u. It is easily verified that $\overline{u_1 u_2} = \overline{u_1} \circ \overline{u_2}$, hence $u \mapsto \bar{u}$ is an homomorphism of monoids $A^* \to \mathrm{End}(\mathbb{Q}\langle A\rangle)$, the endomorphisms of $\mathbb{Q}\langle A\rangle$ considered as a vector space. It extends linearly to an algebra homomorphism $\mathbb{Q}\langle A\rangle \to \mathrm{End}(\mathbb{Q}\langle A\rangle)$, $P \mapsto \bar{P}$.

Let E denote the vector space generated by the factors of w. Define $\varphi': \mathbb{Q}\langle A\rangle \to \mathrm{End}(E)$ by restriction: $\varphi'(P) = \bar{P} \mid E$. We show that $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\varphi'$. By part 1 of the proof, $\mathrm{Ker}\,\varphi$ is the vector space generated by the words which are not factors of w. But if u is such a word and f is any factor of w, then $\bar{u}(f) = 0$, because f does not end with u (otherwise u, factor of f would be also factor of w). Hence $u \in \mathrm{Ker}\,\varphi'$ and so $\mathrm{Ker}\,\varphi \subset \mathrm{Ker}\,\varphi'$.

Conversely, let $P \notin \mathrm{Ker}\,\varphi$. Then $P = \sum(P, u)\, u$ with $(P, f) \neq 0$ for some factor f of w. Then $\bar{P}(f)$ is a polynomial with nonzero constant term, hence $\bar{P}(f) \neq 0$. Thus $P \notin \mathrm{Ker}\,\varphi'$ and $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\varphi'$.

(3) Let $\mathscr{L}(A)$ denote the Lie algebra generated by A in $\mathbb{Q}\langle A\rangle$ (Cauchy

algebra). The Lie algebra $\mathscr{L}$ generated by the φa's is just $\varphi(\mathscr{L}(A))$, hence by part 2, is isomorphic to $\varphi'(\mathscr{L}(A))$. Note that for each letter a in A, $\bar{a}$ is a derivation of the shuffle algebra, that is: $\bar{a}(u \sqcup\!\sqcup v) = \bar{a}(u) \sqcup\!\sqcup v + u \sqcup\!\sqcup \bar{a}(v)$, as is easily verified with the definition of the shuffle product.

Let $\mathscr{A}$ be the shuffle algebra generated by the factors of w (hence by E). As $\bar{a}(E) \subset E$, we have $\bar{a}(\mathscr{A}) \subset \mathscr{A}$. Now, let $\mathscr{F}$ be the field of fractions of $\mathscr{A}$, whose product we still denote by $\sqcup\!\sqcup$. Then the derivation $\bar{a}: \mathscr{A} \to \mathscr{A}$ extends uniquely to a $\mathbb{Q}$-linear derivation $\tilde{a}: \mathscr{F} \to \mathscr{F}$. The mapping $a \mapsto \tilde{a}$, $A \mapsto \mathrm{End}_{\mathbb{Q}}(\mathscr{F})$, extends to an algebra homomorphism over $\mathbb{Q}$: $\mathbb{Q}\langle A\rangle \to \mathrm{End}_{\mathbb{Q}}(\mathscr{F})$, $P \mapsto \tilde{P}$. Note that for each polynomial P and y in E, we have $\tilde{P}(y) = \bar{P}(y)$.

Let $P_1, \ldots, P_r$ be elements of $\mathscr{L}(A)$ such that $\varphi(P_1), \ldots, \varphi(P_r)$ form a basis of $\mathscr{L} = \varphi(\mathscr{L}(A))$ over $\mathbb{Q}$. As the Lie bracket of two derivations is again a derivation, each $\tilde{P}_i$ is a derivation of $\mathscr{F}$. We claim that the P_i's are linearly independent over $\mathscr{F}$.

Suppose that this is not the case. Then we have a relation

$$\sum x_i \sqcup\!\sqcup \tilde{P}_i = 0 \qquad (x_i \in \mathscr{A}, \text{ not all zero})$$

hence

$$\sum x_i \sqcup\!\sqcup \bar{P}_i(y) = 0$$

for any y in E. Let f be a factor of w appearing in one of the P_i with $x_i \neq 0$, P_1 say, and of minimal length (it exists because $\varphi(P_i) \neq 0$).

We may suppose that f appears only in P_1 (indeed, substract from each P_i, $i \geqslant 2$, a suitable scalar multiple of P_1). But $f \in E$, hence

$$\sum x_i \sqcup\!\sqcup \bar{P}_i(f) = 0.$$

Now, $\bar{P}_1(f)$ is nonzero (because f appears in P_1) and $\bar{P}_i(f) = 0$ for $i \geqslant 2$ (because $\bar{P}_i(f) = \sum(P_i, u)\,\bar{u}(f) \neq 0$ would imply that a word u with $\bar{u}(f) \neq 0$ appears in P_i; then u is a factor of f, hence $u = f$ by minimality: f appears in P_i). Thus $x_1 \sqcup\!\sqcup \bar{P}_1(f) = 0 \Rightarrow x_1 = 0$, a contradiction.

Now, it is well known that the dimension over $\mathscr{F}$ of the space of all $\mathbb{Q}$-derivations of $\mathscr{F}$ is equal to the transcendance degree of $\mathscr{F}$ over $\mathbb{Q}$. This implies that the dimension of $\mathscr{L}$ over $\mathbb{Q}$ $(= r)$ is $\leqslant$ to the transcendance degree over $\mathbb{Q}$ of the factors of w, because these generate the field $\mathscr{F}$ over $\mathbb{Q}$.

(4) A *Lie element* of $\mathbb{Q}\langle A\rangle$ is an element of the Lie algebra over $\mathbb{Q}$ generated by the letters in $\mathbb{Q}\langle A\rangle$. Let $\mathscr{T}$ be the complete tensor product

over $\mathbb{Q}$ of the shuffle algebra $\mathbb{Q}\langle A\rangle$ by the Cauchy algebra $\mathbb{Q}\langle A\rangle$. Each element of $\mathcal{T}$ is an infinite linear combination

$$\sum_{u,v\in A^*} \alpha_{u,v} u\otimes v, \qquad \alpha_{u,v}\in\mathbb{Q}.$$

Let $\mathcal{S}$ be the subalgebra of $\mathcal{T}$ consisting of the infinite linear combination of $u\otimes v$, where u and v have the same length. $\mathcal{S}$ is a graded algebra, complete with respect to the topology defined by this gradation. Define an element S of $\mathcal{S}$ by

$$S=\sum_{w\in A^*} w\otimes w.$$

Note that $S=1\otimes 1+T$, where $\lim_{n\to\infty} T^n=0$. Hence we may define

$$\log S=\sum_{n\geqslant 1}(-1)^{n-1}T^n/n.$$

We use the following formula

$$\log S=\sum_{u\in A^*} u\otimes P_u, \tag{2}$$

where P_u is a Lie element of $\mathbb{Q}\langle A\rangle$ and an homogeneous polynomial of degree equal to the length of u. This formula, which is a variant of Friedrich's criterion, is proved by Ree, in a slightly different formulation (see [5, Theorem 2.5 or the beginning of the proof of Theorem 3.1]). The homomorphism $\varphi\colon \mathbb{Q}\langle A\rangle\to\mathcal{M}_{n+1}(\mathbb{Q})$ (Cauchy algebra), defined by the given word w, extends uniquely to an homomorphism $\varphi\colon \mathcal{S}\to \mathcal{M}_{n+1}(\mathbb{Q}\langle A\rangle)$ ($\mathbb{Q}\langle A\rangle$ with the shuffle) by the formula

$$\varphi\left(\sum_{|u|=|v|}\alpha_{u,v}u\otimes v\right)=\sum_{|u|=|v|}\alpha_{u,v}u\varphi v$$

because, for any word u, there are only finitely many words v of the same length as u.

Now, apply this extension of φ to both sides of (2), obtaining

$$\log\left(\sum_{v\in A^*} v\otimes\varphi v\right)=\sum_{u\in A^*} u\varphi P_u$$

in $\mathcal{M}_{n+1}(\mathbb{Q}\langle A\rangle)$ (shuffle structure). The left-hand side is $\log(\sum_f f\varphi f)$ where the sum is extended to all factors f of w; and because each φP_u is in $\mathcal{L}$ (the Lie algebra generated by the φa's) we may write $\varphi P_u=\sum_{1\leqslant i\leqslant l}\alpha_{u,i}M_i$, where $M_1,\ldots, M_l$ is a basis of $\mathcal{L}$. Thus the right-hand side is

$\sum_{u\in A^*} u \sum_{1\leqslant i\leqslant l} \alpha_{u,i} M_i = \sum_i P_i M_i$, where P_i is the polynomial $\sum_{u\in A^*} \alpha_{u,i} u$ (the sum is finite because $\alpha_{u,i}=0$ when u is long enough). Hence $\sum P_i M_i = \log(\sum f\varphi f)$ and this shows that each P_i is in the shuffle algebra generated by the factors of w. Conversely we have

$$\sum f\varphi f = \exp\left(\sum P_i M_i\right)$$

Hence each f is in the shuffle algebra generated by the P_i's. Moreover, the transcendance degree of the f's being $\geqslant l$, (by part (3) of the proof) we obtain that $\mathscr{A}$ is free over $P_1,\ldots, P_l$.

(5) The following proposition will imply that some factors of w form a basis of $\mathscr{A}$, which concludes the proof of the theorem. ▮

PROPOSITION. *Let P be a set of words containing any left factor of any of its elements. Then the shuffle algebra generated by P is free over some subset of P.*

Remark 3. The proposition admits as a corollary the following well-known result: the shuffle algebra $\mathbb{Q}\langle A\rangle$ is free (take $P=A^*$).

For the proof, we need the following

LEMMA. *Let V be a finite set of words and u a word not in V such that V contains each proper left factor of $V\cup\{u\}$ and such that u is algebraically dependent on V in the shuffle algebra. Then u is in the algebra generated by V.*

Proof. Let $\mathscr{A}$ be the shuffle subalgebra generated by V. Let a be any letter; recall that $\bar{a}$ is a derivation of the shuffle algebra, defined for any word f by $\bar{a}(f)=f'$ if $f=f'a$ and $\bar{a}(f)=0$ if f does not end with the letter a. Hence, either $\bar{a}(f)=0$ or $\bar{a}(f)$ is a left factor of f. This shows that $\bar{a}(V)\subset V\cup\{0\}$, hence $\bar{a}(\mathscr{A})\subset\mathscr{A}$. Similarly $\bar{a}(u)\in\mathscr{A}$. Note that for any polynomial P, we have

$$P=(P,1)+\sum_{a\in A}\bar{a}(P)\,a.$$

Thus, if $P\notin\mathbb{Q}$, there exists a letter a such that $\bar{a}(P)\neq 0$. From now on, we denote the shuffle product $f \sqcup\!\sqcup g$ simply by fg. Because u is algebraically dependent on $\mathscr{A}$, there exists an integer $k\geqslant 1$ and elements $Q_k,\ldots, Q_0$ in $\mathscr{A}$ such that $Q_k\neq 0$ and that

$$u^k Q_k + u^{k-1}Q_{k-1} + \cdots + Q_0 = 0. \tag{3}$$

To show that $u \in \mathscr{A}$, we use induction on the couple $(k, \deg(Q_k))$, ordered lexicographically. If $(k, \deg(Q_k)) = (1, 0)$, it is clear that $u \in \mathscr{A}$. Otherwise, either $\deg(Q_k) \geqslant 1$ (hence $Q_k \notin \mathbb{Q}$), or $k \geqslant 2$. Let a be any letter and derive (3) with respect to $\bar{a}$, obtaining

$$u^k P_k + u^{k-1} P_{k-1} + \cdots + P_0 = 0, \tag{4}$$

where the P_i's are defined by

$$\begin{aligned} P_k &= \bar{a}(Q_k), \\ P_{k-1} &= k\bar{a}(u)\, Q_k + \bar{a}(Q_{k-1}), \\ &\vdots \\ P_0 &= \bar{a}(u)\, Q_1 + \bar{a}(Q_0). \end{aligned}$$

Because $\bar{a}(u)$ and $\bar{a}(Q_i)$ are in $\mathscr{A}$, we have $P_i \in \mathscr{A}$. In the case where $Q_k \notin \mathbb{Q}$, choose a letter a such that $P_k = \bar{a}(Q_k) \neq 0$. Then $\deg(P_k) < \deg(Q_k)$, and we can therefore assume that $Q_k \in \mathbb{Q}$. Now consider $P_{k-1} = \bar{a}(kuQ_k + Q_{k-1})$. If $kuQ_k + Q_{k-1} \in \mathbb{Q}$, we obtain $u \in \mathscr{A}$, because kQ_k is a nonzero scalar and $Q_{k-1} \in \mathscr{A}$. Otherwise, choose a such that $P_{k-1} \neq 0$. Then (4) becomes

$$u^{k-1} P_{k-1} + \cdots + P_0 = 0$$

and we conclude $u \in \mathscr{A}$ again, by induction. ∎

Proof of the Proposition. P may be written as a disjoint union

$$P = P_1 \cup P_2 \cup P_3 \tag{5}$$

with the following properties

(i) The elements of P_1 are algebraically independent.

(ii) The elements of P_2 are in the subalgebra generated by P_1.

(iii) $P_1 \cup P_2$ contains any left factor of any of its elements.

(iv) $1 \in P_2$.

Indeed we have $P = \varnothing \cup \{1\} \cup (P \backslash 1)$. Consider an expression (5) with P_3 minimal. Then $P_3 = \varnothing$ (and the result follows). Indeed, otherwise, P_3 contains some word f: as $1 \in P_2$, there is some left factor g of f which is in P_3 and such that each proper left factor of g is in $P_1 \cup P_2$. Then, either g is algebraically independent over $P_1 \cup P_2$ and

$$P = (P_1 \cup \{g\}) \cup P_2 \cup (P_3 \backslash \{g\})$$

which contradicts the minimality of P_3. Or g is algebraically dependent over $P_1 \cup P_2$. Then, by the lemma, g is in the subalgebra generated by $P_1 \cup P_2$, hence in the subalgebra generated by P_1. Thus

$$P = P_1 \cup (P_2 \cup \{g\}) \cup (P_3 \setminus \{g\})$$

which also contradicts the minimality of P_3. ∎

IV. Comment

The theorem suggests that there is an algebraic group associated to the given word w whose algebra of polynomial functions is $\mathscr{A}$ and whose Lie algebra is $\mathscr{L}$. This is indeed true: this group is the subgroup of $GL_{n+1}(\mathbb{Q})$ that admits as generic point the matrix

$$\sum_{u \in A^*} u\varphi u$$

with coefficients in the shuffle algebra. This is a particular case of [6] where it is shown that this matrix is a generic point of the smallest algebraic group whose Lie algebra contains the matrices φa (for any matrices φa). For the special case here, we still need a result of Chevalley [1] asserting that if the matrices φa are nilpotent, then the Lie algebra they generate is the Lie algebra of an algebraic group (in general, it is bigger).

The proof here is self contained and independent of all these results, and we obtain even more that the shuffle algebra generated by the factors is free and admits as a basis a subset of the set of factors.

Acknowledgments

I want to thank the referee who pointed out that there was a gap in the proof of the lemma in the first version of this paper and Dominique Perrin, who listened carefully to the new proof of this lemma.

References

1. C. Chevalley, "Théorie des groupes de Lie. II. Groupes algébriques," Hermann, Paris, 1946.
2. J. Dixmier, "Algèbres enveloppantes," Chapter 2, Section 7, Gauthier-Villars, Paris, 1974.
3. S. Eilenberg, "Automata, Languages, and Machines A," Academic Press, New York, 1974.

4. M. LOTHAIRE, "Combinatorics on Words," Addison-Wesley, Reading, Mass., 1983.
5. R. REE, Lie elements and an algebra associated with shuffles, *Ann. of Math.* **68** (1958), 210–220.
6. C. REUTENAUER, Point générique du plus petit groupe algébrique dont l'algèbre de Lie contient plusieurs matrices données, *C. R. Acad. Sci. Paris* **293** (1981), 577–580.