JOURNAL OF ALGEBRA **85**, 32–39 (1983)

Cyclic Derivation of Noncommutative Algebraic Power Series

CHRISTOPHE REUTENAUER

CNRS Institut de Programmation, 4 place Jussieu, 7500 Paris, France

Communicated by D. Buchsbaum

Received June 15, 1981

We show that the cyclic derivative of any algebraic formal power series in noncommuting variables is again algebraic.

INTRODUCTION

Rota *et al.* [8] have introduced two operators C and D of the algebra of noncommutative formal power series; they are defined in the following way: the image Cw of a word w is

$$Cw = \sum_{\substack{uv=w \\ v \neq 1}} vu$$

(and C is extended by linearity and continuity) and the *cyclic derivation* D is obtained by composing C with the map T such that

$$T(xw) = w,$$

$$T(x) = 0$$

if w does not begin with x where x is a fixed letter. In the case of one variable, D is the usual derivation. The above cited authors show that the image under C or D of any rational noncommutative power series is again rational. The purpose of the present note is to prove that the image of any *algebraic* power series is still algebraic (which is well known for one variable): the concept of algebraicity for noncommutative formal power series that we shall use here was introduced by Chomsky and Schützenberger [3]; it extends on one hand the usual concept in one variable and, on the other, the concept of context-free languages. These languages are closed with

0021-8693/83 $3.00

respect to C (and the same is true for rational (or regular) languages, as proved by Schützenberger (unpublished result, cited in [5, II.23])).

1. Preliminaries

Let X be an alphabet, X^* the *free monoid* generated by X. The neutral element of X^* is denoted by 1. The elements of X are *words* and 1 is the *empty word*. The length of a word w is denoted by $|w|$.

Let K be a field; the *algebra of noncommutative polynomials* $K\langle X\rangle$ is the set of all linear combinations

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

where (P, w) denotes the coefficient of the word w; $I = K^+\langle X\rangle$ denotes the ideal of the polynomials P such that $(P, 1) = 0$ (i.e., without constant term). The powers

$$I^n, \qquad n \geqslant 0,$$

of I define a fundamental set of neighbourhoods of 0 for a metrizable topology, see [8]. The completion of $K\langle X\rangle$ is the *algebra of noncommutative formal power series* $K\langle\langle X\rangle\rangle$, which can be identified with the (finite or infinite) sums

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

A language L is a subset of X^*; it can be identified with its *characteristic* series

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

The support of a formal power series S is the language

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

A formal power series is *rational* if it can be obtained from polynomials by a finite number of the following operations: sum, product, inversion. By a theorem of Schützenberger (which extends a well-known theorem of Kleene) a series is rational if and only if it is *recognizable*, that is, if there exist $n \geqslant 1$, an algebra homomorphism

$$\mu \colon K\langle X\rangle \to \mathscr{M}_n(K)$$

and matrices $\lambda \in \mathscr{M}_{1,n}(K)$, $\gamma \in \mathscr{M}_{n,1}(K)$ such that for each word w

$$(S, w) = \lambda \mu w \gamma$$

(for a proof of this theorem, see [4] or [9]).

Let us now define algebraic series. Let

$$\Xi = \{\xi_1, \ldots, \xi_n\}$$

be a new alphabet and

$$P_1(\xi_1, \ldots, \xi_n), \ldots, P_n(\xi_1, \ldots, \xi_n) \in K\langle X \cup \Xi \rangle.$$

We say that the system

$$\begin{aligned} \xi_1 &= P_1(\xi_1, \ldots, \xi_n) \\ &\vdots \\ \xi_n &= P_n(\xi_1, \ldots, \xi_n) \end{aligned} \tag{1.1}$$

is an *algebraic system of equations*. We now introduce two conditions on the polynomials P_i, each of which is sufficient to imply the existence and the uniqueness of an n-tuple of formal power series in $K\langle\langle X \rangle\rangle$ which is a solution of this system.

Call the system *proper* if for each i

$$\operatorname{supp}(P_i) \cap \{1, \xi_1, \ldots, \xi_n\} = \varnothing.$$

Call the system *strict* if for each i

$$\operatorname{supp}(P_i) \cap \Xi^* = \varnothing.$$

If the system is strict, it can be shown that there exists one and only one n-tuple $(S_1, \ldots, S_n) \in K\langle\langle X \rangle\rangle^n$ which is *solution* of this system, that is, such that

$$\begin{aligned} S_1 &= P_1(S_1, \ldots, S_n) \\ &\vdots \\ S_n &= P_n(S_n, \ldots, S_n), \end{aligned} \tag{1.2}$$

where $P_i(S_1, \ldots, S_n)$ denotes the series obtained by replacing each ξ_j in P_i by S_j. Similarly, if the system is proper, there exists one and only one n-tuple $(S_1, \ldots, S_n) \in K^+\langle\langle X \rangle\rangle^n$ (where $K^+\langle\langle X \rangle\rangle$ is the set of all series without constant term) such that one has (1.2); this n-tuple will be called the *proper solution* of the system.

One shows that the following conditions are equivalent for a formal power series S:

(i) S is a component of the solution of a strict system,

(ii) S is the sum of a constant and component of the proper solution of a proper system

(See [9, Chapter IV, Theorem 1.1, Definition p. 120 and Theorem 2.3].) In this case, we say that S is *algebraic*.

Let $C: K\langle\langle X\rangle\rangle \to K\langle\langle X\rangle\rangle$ be the K-linear and continuous mapping defined for each word $w = x_1 \cdots x_n$ $(x_i \in X)$ by

$$Cw = x_1 \cdots x_n + x_2 \cdots x_n x_1 + \cdots + x_n x_1 \cdots x_{n-1} = \sum_{\substack{w=uv \\ v\neq 1}} vu; \qquad C1 = 1.$$

Rota *et al.* [8] show that if S is rational, then CS is again rational. We want to deduce the following result.

THEOREM. *If S is algebraic, then CS is algebraic.*

The above-cited authors call *cyclic derivation* with respect to a given letter x_0, the operator D of $K\langle\langle X\rangle\rangle$ defined by

$$DS = x_0^{-1}(CS),$$

where, for each series T, $x_0^{-1}T$ is defined by

$$x_0^{-1}T = \sum_{w\in X^*} (T, x_0 w)\, w.$$

Now it is a classical result that if T is algebraic then $x_0^{-1}T$ is algebraic too (e.g., it is a consequence of Theorem 2.3. Chapter IV in [9]). Hence, the theorem above implies the

COROLLARY. *If S is algebraic, DS is algebraic.*

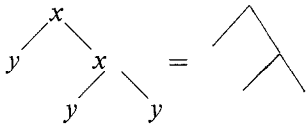
EXAMPLE. Consider the series defined by

$$S = xSS + y.$$

We have

$$S = x + xyy + xxyyy + xyxyy + xxxyyyy + \cdots .$$

S is just the characteristic series of the well-known Luckasiewicz language L (see [2, II.4]). A word in L can be pictured as a binary tree; for instance,

$xyxyy =$ 

Let $|w|_x$ denote the degree in x of w. Then for each w such that $|w|_x - |w|_y = -1$, there exists one and only one $u \in L$ conjugate to w (i.e., $u = ab$, $w = ba$), see [2, Proposition II.4.3]. Hence

$$CS = \sum_{|w|_x - |w|_y = -1} w$$

and, letting D denote the cyclic derivation with respect to y,

$$DS = \sum_{|w|_x - |w|_y = 0} w,$$

which is algebraic (ibid.)

Remarks. 1. The operator $x^{-1}T$ allows one to characterize rationality in a nice way: indeed a series S is recognizable if and only if the smallest subspace of $K\langle\langle X\rangle\rangle$ containing S and closed with respect to the operators x^{-1} (for all letters x) is finite dimensional. This dimension is the *rank* of S, which can also be defined by a Hankel matrix (see [4]).

2. Through the notion of recognizability, one can give another proof of the result of Rota *et al.*: indeed if

$$(S, w) = \lambda\mu w\gamma \qquad \text{(see above)}$$

then

$$(CS, w) = \sum_{\substack{w=uv \\ v\neq 1}} (S, vu) = \sum_{\substack{uv=w \\ v\neq 1}} \sum_{1\leqslant i\leqslant n} (\mu u\gamma)_i\,(\lambda\mu v)_i$$

$$= \sum_{i,u,v} (S_i, u)(T_i, v) = \sum_i (S_i T_i, w),$$

where S_i and T_i are the recognizable (hence rational) series defined by

$$(S_i, w) = \lambda_i \mu w\gamma, \qquad (T_i, w) = \lambda\mu w\gamma_i,$$

and where λ_i (resp. γ_i) are the matrices of the canonical basis of $\mathscr{M}_{1,n}(K)$ (resp. $\mathscr{M}_{n,1}(K)$). Hence $CS = \sum_i S_i T_i$ is rational.

2. Proof of the Theorem

The *Hadamard product* of two series S and T is the series

$$S \odot T = \sum_{w} (S, w)(T, w) w.$$

Let Y and $\bar{Y}$ be two alphabets and

$$\begin{aligned} y &\mapsto \bar{y} \\ Y &\to \bar{Y} \end{aligned}$$

be a bijection between them. We call *Dyck language* the language Δ on the alphabet $Z = Y \cup \bar{Y}$ defined by

$$\Delta = \varphi^{-1}(1),$$

where φ is the canonical morphism

$$\begin{aligned} Z^* &\to Y^{(*)}, \\ y &\mapsto y, \\ \bar{y} &\mapsto y^{-1} \end{aligned}$$

and $Y^{(*)}$ the free group generated by Y. We still denote by Δ the characteristic series of the Dyck language: Δ is an algebraic series (see [2, II.3)]. The theorem of Chomsky–Schützenberger [3] asserts that for each algebraic series $S \in K\langle\langle X \rangle\rangle$ there exists an alphabet $Z = Y \cup \bar{Y}$, a rational series $R \in K\langle\langle Z \rangle\rangle$ and an alphabetical morphism $\psi: Z^* \to X^*$ (alphabetical means that the image under ψ of each letter is either a letter or the empty word) such that the family of series

$$((R \odot \Delta, w)\, \psi(w))_{w \in Z^*}$$

is summable in $K\langle\langle X \rangle\rangle$ and that its sum is S. We then write

$$S = \psi(R \odot \Delta).$$

(For a proof of this result see [9, IV.4].)

There exists a more sophisticated version of this theorem: it says that there exists a *rational language* K (see [4] or [2]) and an integer k such that $\operatorname{supp}(R) \subset K$ and that

$$\forall\, aub \in K, \qquad |u| \geqslant k \Rightarrow |\psi(u)| \geqslant 1. \tag{2.1}$$

In other words, each factor of length at least k of any word in K contains at least one letter $z \in Z$ such that $\psi(z) \in X$. This improvement of the Chomsky–Schützenberger theorem is proved for languages in [1] and [2] (Ex. 3.8 of Chapter II), but its extension to formal power series is straightforward.

Now, let $S \in K\langle\langle X \rangle\rangle$ an algebraic series and Y, ψ, R, K and k as above. Let K' be the language defined by

$$K' = CK = \{vu \mid uv \in K\}.$$

Condition (2.1) implies that a similar condition is true for K' (with $2k$ in place of k); indeed each factor of length at least $2k$ of a work in K' contains a factor of length k of some word in K.

Let Z_1 be the set of all letters $z \in Z$ such that $\psi(z) = 1$ and $Z_2 = Z \backslash Z_1$. We denote by T the series

$$T = C(\Delta \odot R) \odot \underline{Z^* Z_2}$$

(recall that $\underline{Z^* Z_2}$ is the characteristic series of the language $Z^* Z_2$). Then $\text{supp}(R) \subset K$ implies that $\text{supp}(T) \subset K'$, hence the family of series $((T, w)\, \psi(w))_{w \in Z^*}$ is summable in $K\langle\langle X \rangle\rangle$; we denote by $\psi(T)$ its sum and show now that

$$\psi(T) = CS. \tag{2.2}$$

Indeed, let $w = u_0 z_1 u_1 \cdots z_n u_n$, $u_i \in Z_1^*$, $z_i \in Z_2$ with $\psi(z_i) = x_i \in X$. Then

$$C\psi(w) = x_1 \cdots x_n + x_2 \cdots x_n x_1 + \cdots + x_n x_1 \cdots x_{n-1}$$

and

$$\begin{aligned} \psi(Cw \odot \underline{Z^* Z_2}) &= (u_n u_0 z_1 u_1 \cdots z_n + u_{n-1} z_n u_0 z_1 u_1 \cdots z_{n-1} + \cdots \\ &\quad + u_1 \cdots z_n u_n u_0 z_1) \\ &= x_1 \cdots x_n + x_n x_1 \cdots x_{n-1} + \cdots + x_2 \cdots x_n x_1 \end{aligned}$$

hence $C\psi(w) = (Cw \odot \underline{Z^* Z_2})$ and (2.2) follows by linearity and continuity. We now show that $\psi(T)$ is algebraic. Let

$$\begin{aligned} \tau \colon Z^* &\to K\langle\langle X \rangle\rangle, \\ w &\mapsto \psi(w) \quad \text{if} \quad w \in K', \\ w &\mapsto 0 \quad \text{if} \quad w \notin K'. \end{aligned}$$

Because of the condition on K', the mapping τ extends by linearity and continuity to a mapping

$$\tau \colon K\langle\langle X \rangle\rangle \to K\langle\langle X \rangle\rangle$$

which is a *rational regulated transduction* (see [7] or [9, Chapter 3, Section 1]). Hence (ibid.) the image under τ of any algebraic series is algebraic. Now, because $\operatorname{supp}(T) \subset K'$ we have $\tau(T) = \psi(T)$. Furthermore, because $uv \in \Delta \Leftrightarrow vu \in \Delta$ we have

$$C(\Delta \odot R) = \Delta \odot CR$$

and: CR is rational [8], $\underline{Z^*Z_2}$ is rational because

$$\underline{Z^*Z_2} = (1 - \underline{Z})^{-1}\, \underline{Z}_2,$$

$T = \Delta \odot CR \odot \underline{Z^*Z_2}$ is algebraic by a theorem of Schützenberger [10] (the Hadamard product of an algebraic (resp. rational) series by a rational series is again algebraic (resp. rational)).

Acknowledgments

The author wants to thank Professor Schützenberger, who suggested this paper, and Professors Berstel, Autebert and Boasson for helpful discussions.

References

1. J.-M. Autebert and L. Boasson, Generators of cones and cylinders, *in* "Formal Language Theory, Open Problems and Perspectives" (R. Book, Ed.), pp. 49–87, Academic Press, New York/London, 1980.
2. J. Berstel, "Transductions and Context-Free Languages," Teubner, Stuttgart, 1979.
3. N. Chomsky and M. P. Schützenberger, The algebraic theory of context-free languages, *in* "Computer Programming and Formal Systems" (P. Brattfort and D. Hirschberg, Eds.), pp. 118–161, North-Holland, Amsterdam, 1963.
4. S. Eilenberg, "Automata, Languages and Machines," Vol. A, Academic Press, New York/London, 1974.
5. M. Fliess, "Sur certaines familles de séries formelles," Thesis, University Paris 7, 1972.
6. M. Fliess, Matrices de Hankel, *J. Math. Pures Appl.* **53** (1974), 197–224.
7. G. Jacob, Sur un théorème de Shamir, *Inform. and Control* **27** (1975), 218–261.
8. G.-C. Rota, B. Sagan, and R. Stein, A cyclic derivation in noncommutative algebra, *J. Algebra* **64** (1980), 54–75.
9. A. Salomaa and M. Soittola, "Automata-Theoretic Aspects of Formal Power Series," Springer–Verlag, New York/Berlin, 1978.
10. M. P. Schützenberger, On a theorem of Jungen, *Proc. Amer. Math. Soc.* **13** (1962), 885–890.