

# The local realization of generating series of finite Lie rank<sup>\*</sup>

Christophe Reutenauer<sup>†</sup>

## 1 Introduction

Realization of nonlinear systems by state-space is a classical problem in control theory. This problem has been completely solved by Kalman [10] in the case of linear systems. Similarly, it was solved for bilinear systems (see Brockett [2], d'Alessandro, Isidori, Ruberti [1], Fliess [3], Sussmann [12]). In the general case, let us mention the work of Sussmann [13], Hermann, Krener [7] and Jakubczyk [9]: they assume that the solutions are regular at any time and for any inputs. This restriction lead Fliess to study local realization of nonlinear systems [5].

The present paper deals with the latter subject; there are no new results here, but we give elementary proofs of Fliess' results [5]. He shows that to these systems correspond generating series (which are noncommutative formal power series) which have the property that their Lie rank is finite<sup>1</sup>. Then he shows existence and unicity of locally reduced (or minimal) realizations and shows that minimality is equivalent to the two following properties: weak local controllability and weak local observability.

We want to give here a simple proof of these results, especially the proof of unicity, for which Fliess uses in [5] sophisticated results on Lie groups and algebras. The present work extends the “syntactic” approach of series with finite Lie rank, as studied in [5], and of nonlinear systems. Hopefully, this will lead to find a realization, which is minimal (in some sense) and which is given directly by the generating series; this would be analogue to the bilinear case, where the minimal state-space is directly given by the Hankel matrix. Our main tool here is the theorem of Poincaré-Birkhoff-Witt. We treat only the “analytic” case of [5]. The “formal” case is simpler and is obtained by omitting in the sequel everything dealing with convergence or majoration of coefficients.

---

<sup>\*</sup>M. Fliess and M. Hazewinkel (eds.), Algebraic and Geometric Methods in Nonlinear Control Theory, 33-43.

<sup>†</sup>Université du Québec à Montréal and CNRS (Paris), Département de Mathématiques et d'Informatique, C.P. 8888 Succ. A, H3C 3P8, Canada

<sup>1</sup>Bilinear systems correspond to generating series whose rank is finite.

I want to thank Michel Fliess for encouraging and stimulating discussions on this subject.

## 2 Generating series of finite Lie rank

We consider a system of the following form

$$\begin{cases} \dot{q}(t) = A_0(q) + \sum_{i=1}^n u_i(t) A_i(q) \\ y(t) = h(q) \end{cases} \quad (1)$$

where the state  $q$  belongs to a connected analytic  $\mathbb{R}$ -variety  $Q$ , where the  $A_i$  's are analytic vector fields and  $h$  a real analytic function defined in a neighborhood of the given initial state  $q(0)$ . The inputs  $u_1, \dots, u_n$  are real and piecewise continuous.

By Fliess [4] th.III.2, the output  $y$  of system (1) is given by the following formula (for small enough time and inputs):

$$y(t) = h|_{q(0)} + \sum_{\nu \geq 0} \sum_{j_0, \dots, j_\nu \geq 0}^n \left( A_{j_0} \dots A_{j_\nu} h|_{q(0)} \right) \int_0^t d\xi_{j_\nu} \dots d\xi_{j_0} \quad (2)$$

where  $|_q(0)$  means evaluation in  $q(0)$  and where the iterated integrals  $\int d\xi_{j_\nu} \dots d\xi_{j_0}$  are defined by the formulas ( $u_0$  is the constant function equal to 1 ):

$$\begin{aligned} \int_0^t d\xi_j &= \int_0^t u_j(\tau) d\tau, \text{ and if } \nu \geq 1 \\ \int_0^t d\xi_{j_\nu} \dots d\xi_{j_0} &= \int_0^t \left[ u_{j_\nu}(\tau) d\tau \int_0^\tau d\xi_{j_{\nu-1}} \dots d\xi_{j_0} \right] \end{aligned}$$

Actually, the input-output behaviour of system (1) is completely defined by its **generating series** ([4] p.12), which is a noncommutative formal power series in the variables  $x_0, \dots, x_n$ :

$$g = h|_{q(0)} + \sum_{\nu \geq 0} \sum_{j_0, \dots, j_\nu \geq 0}^n \left( A_{j_0} \dots A_{j_\nu} h|_{q(0)} \right) x_{j_\nu} \dots x_{j_0} \quad (3)$$

Recall that a formal power series in the noncommutative variables  $x_0, \dots, x_n$  is a mapping  $g$  from the free monoid  $X^*$  generated by  $X = \{x_0, \dots, x_n\}$  into  $\mathbb{R}$ , denoted by  $w \rightarrow (g, w)$ , for any **word** (= element of  $X^*$ )  $w$ , including the empty word, denoted by 1. The formal series  $g$  will also be denoted by

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

The set of formal series is denoted by  $\mathbb{R}\langle\langle X \rangle\rangle$ . Following [5], we give a definition, inspired by (3). First, let us say that a (commutative) formal series in

$\mathbb{R}[[q]] = \mathbb{R}[[q_1, \dots, q_d]]$  (where the  $q_i$ 's are commutative variables) is **convergent** if it converges in a neighborhood of 0; similarly, we say that a **formal vector field**, that is, an operator of  $\mathbb{R}[[q]]$  of the form<sup>2</sup>

$$A = \sum_{1 \leq k \leq d} \theta_k(q_1, \dots, q_d) \frac{\partial}{\partial q_k}$$

where the  $\theta_k$  are in  $\mathbb{R}[[q]]$ , is **convergent**, if the  $\theta_k$ 's are convergent formal series. Because of the reverse order in (3) of the  $A$ 's and the  $x$ 's, we let the formal vector fields operate at the right of the formal series.

**Definition 1.** A formal series  $g \in \mathbb{R}\langle\langle X \rangle\rangle$  is **produced differentially** if there exists an integer  $d$ , an homomorphism  $\mu$  from the free monoid into the multiplicative monoid of the endomorphisms of  $\mathbb{R}[[q]]$  such that  $\mu x$  is a formal vector field for any  $x$  in  $X$ , a convergent formal series  $h$  in  $\mathbb{R}[[q]]$  such that

$$\forall w \in X^*, \quad (g, w) = h(\mu w)|_0$$

(that is,  $(g, w)$  is the constant term of the series which is the image of  $h$  under the operator  $\mu w$ ).

We call the couple  $(\mu, h)$  a **differential representation** of  $g$ , of **dimension**  $d$ .

It is now obvious that if  $g$  is the generating series of system (1), then it is produced differentially (take local coordinates around  $q(0)$  in (3)). Conversely, if a series  $g$  is produced differentially, then one may associate to it a system of type (1), whose generating series is  $g$ . Thus, **the study of differential representations of series is equivalent to the study of local realizations of systems like (1)**.

Before stating the main result, we need some notations. Denote by  $\mathbb{R}\langle X \rangle$  the set of noncommutative **polynomials**, that is, formal series having only a finite number of nonzero coefficients. Then  $\mathbb{R}\langle\langle X \rangle\rangle$  is isomorphic to the dual of  $\mathbb{R}\langle X \rangle$  (because  $\mathbb{R}\langle X \rangle \simeq \mathbb{R}^{X^*}$  and  $\mathbb{R}\langle\langle X \rangle\rangle \simeq \mathbb{R}^{X^*}$ , as vector spaces), with duality

$$\begin{aligned} \mathbb{R}\langle\langle X \rangle\rangle \times \mathbb{R}\langle X \rangle &\rightarrow \mathbb{R} \\ (S, P) &\mapsto (S, P) = \sum_{w \in X^*} (S, w)(P, w) \end{aligned}$$

The set  $\mathbb{R}\langle X \rangle$  possesses an associative product, which extends linearly the concatenation of words in  $X^*$ . Thus, the algebra  $\mathbb{R}\langle X \rangle$  acts naturally at the left and at the right of  $\mathbb{R}\langle\langle X \rangle\rangle$ , in the following way

$$\begin{aligned} S \circ P &= \sum_{w \in X^*} (S, Pw)w \\ P \circ S &= \sum_{w \in X^*} (S, wP)w \end{aligned} \tag{4}$$

---

<sup>2</sup>A formal vector field may also be defined as a derivation of the algebra  $\mathbb{R}[[q]]$ , which is continuous for the usual topology of  $\mathbb{R}[[q]]$ .

These two actions are associative (that is,  $S \circ PQ = (S \circ P) \circ Q$  and  $PQ \circ S = P \circ (Q \circ S)$ ) and commute each to another (that is  $P \circ (S \circ Q) = (P \circ S) \circ Q$ ).

We denote by  $L\langle X \rangle$  the Lie algebra generated by the elements of  $X$ : an element of  $L\langle X \rangle$  is called a **Lie polynomial**.

**Definition 2.** The **Lie rank** of a formal series  $g \in \mathbb{R}\langle\langle X \rangle\rangle$  is the dimension of the vector space

$$\{P \circ g \mid P \in L\langle X \rangle\}$$

We say that a formal series  $g \in \mathbb{R}\langle\langle X \rangle\rangle$  satisfies to the **convergence hypothesis** (C) if: for any Lie polynomials  $P_1, \dots, P_q$ , there exist constants  $\alpha$  and  $C$  such that

$$\forall i_1, \dots, i_q \in \mathbb{N}, \quad |(g, P_1^{i_1} \dots P_q^{i_q})| \leq \alpha C^{i_1 + \dots + i_q} i_1! \dots i_q! \quad (\text{C})$$

Note that one may replace  $i_1! \dots i_q!$  by  $(i_1 + \dots + i_q)!$ , because these numbers satisfy to

$$i_1! \dots i_q! \leq (i_1 + \dots + i_q)! \leq q^{i_1 + \dots + i_q} i_1! \dots i_q!$$

Now, we can state the following fundamental result.

**Theorem** (Fliess [5]). A series  $g \in \mathbb{R}\langle\langle X \rangle\rangle$  is differentially produced if and only if its Lie rank is finite and if it satisfies to the convergence hypothesis. In this case, its Lie rank  $d$  is equal to the smallest dimension of all its differential representations. If  $(\mu, h)$  and  $(\mu', h')$  are two differential representations of dimension  $d$  of  $g$  (with the same  $\mathbb{R}[[q]]$ ), then there exists a continuous and convergent<sup>3</sup> automorphism of  $\mathbb{R}[[q]]$  such that  $h' = \phi(h)$  and  $\phi(k\mu w) = \phi(k)\mu'w$  for any word  $w$  and any series  $k$  in  $\mathbb{R}[[q]]$ .

Note that the fact that  $\phi$  is bijection is equivalent to the well-known Jacobian condition

$$\left| \frac{\partial \phi(q_j)}{\partial q_i}(0) \right| \neq 0$$

The third part of this paper is devoted to the proof of the theorem. We need before some definition and results.

On  $\mathbb{R}\langle\langle X \rangle\rangle$  is defined another product, the **shuffle**, which is associative and commutative and which will be important in the sequel; this is not a surprise, as the shuffle intervenes already for systems of the form (1): indeed, by Fliess ([4] prop. II.4), if two systems admit the generating series  $g_1$  and  $g_2$ , then the system whose output is the product of the outputs of these two systems admits as generating series the shuffle of  $g_1$  and  $g_2$ .

If  $w$  is a word of length  $|w| = p$  ( $w = y_1 \dots y_p$ ,  $y_i \in X$ ) and  $I \subset \{1, \dots, p\}$ , denote by  $w|I$  the word  $y_{i_1} \dots y_{i_r}$ , with  $I = \{i_1 < \dots < i_r\}$ . Then the shuffle  $u \star v$  of two words  $u$  and  $v$  is defined as

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

---

<sup>3</sup>that is, for any  $q_i$ ,  $\phi(q_i)$  is convergent and without constant term.

where the sum is extended to all partitions  $(I, J)$  of  $(1, \dots, |u| + |v|)$  with  $\text{Card}(I) = |u|$ ,  $\text{Card}(J) = |v|$  and where the word  $w(I, J)$ , of length  $|u| + |v|$ , is defined by

$$w(I, J)|I = u, \quad w(I, J)|J = v$$

Note that there are  $\binom{|u|+|v|}{|u|}$  such words.

**Example.**  $y_1 y_2 \star y_2 y_3 = 2y_1 y_2^2 y_3 + y_1 y_2 y_3 y_2 + y_2 y_1 y_2 y_3 + y_2 y_1 y_3 y_2 + y_2 y_3 y_1 y_2$ .

The shuffle  $S \star T$  of two series in  $\mathbb{R}\langle\langle X \rangle\rangle$  is then defined by

$$S \star T = \sum_{u, v \in X^*} (S, u)(T, v) u \star v$$

(extension by linearity and continuity). **From now on, we denote  $S \star T$  simply by  $ST$ :** there will be no ambiguity because we consider here only the shuffle structure of  $\mathbb{R}\langle\langle X \rangle\rangle$ <sup>4</sup>. However,  $\mathbb{R}\langle X \rangle$  will be considered with its concatenation structure.

**Lemma 1.** *Let  $c_p : \mathbb{R}\langle X \rangle \rightarrow \mathbb{R}\langle X \rangle^{\otimes p}$  be the concatenation homomorphism defined by*

$$c_p(x) = x \otimes 1 \cdots \otimes 1 + 1 \otimes x \cdots \otimes 1 + 1 \otimes 1 \cdots \otimes x$$

*For any series  $S_1, \dots, S_p$  in  $\mathbb{R}\langle\langle X \rangle\rangle$  and any polynomial  $P$  one has*

$$(S_1 \cdots S_p, P) = (S_1 \otimes \cdots \otimes S_p, c_p(P))$$

*where the duality between  $\mathbb{R}\langle\langle X \rangle\rangle$  and  $\mathbb{R}\langle X \rangle$  is extended to  $\mathbb{R}\langle\langle X \rangle\rangle^{\otimes p}$  and  $\mathbb{R}\langle X \rangle^{\otimes p}$ , that is*

$$(S_1 \otimes \cdots \otimes S_p, P_1 \otimes \cdots \otimes P_p) = (S_1, P_1) \cdots (S_p, P_p)$$

*Proof.* It is enough to prove the lemma when the  $S$ 's and the  $P$ 's are words; in this case, it is a simple consequence of the definition of the shuffle.  $\square$

**Lemma 2.** *If  $P$  is a Lie polynomial, then*

$$c_p(P) = P \otimes 1 \cdots \otimes 1 + 1 \otimes P \cdots \otimes 1 + 1 \otimes 1 \cdots \otimes P$$

*Proof.* This is true if  $P = x \in X$ . Moreover, if it is true for  $P$  and  $Q$ , then also for  $[P, Q] = PQ - QP$ , as is easily verified. So, the lemma follows.  $\square$

We shall use the following classical result.

**Theorem** (Poincaré-Birkhoff-Witt). *Let  $P_1, \dots, P_n, \dots$  be a basis of  $L\langle X \rangle$ . Then the polynomials*

$$P_{i_1}^{j_1} \cdots P_{i_r}^{j_r}, \quad r \geq 0, \quad i_1, \dots, i_r, j_1, \dots, j_r \geq 1, \quad i_1 < \cdots < i_r$$

*form a basis of  $\mathbb{R}\langle X \rangle$ .*

For a proof, see [8], corollary C p. 92.

---

<sup>4</sup> $\mathbb{R}\langle\langle X \rangle\rangle$  possesses also the noncommutative product which extends the concatenation of words.

### 3 Proof of theorem

**a)** Let  $g$  be a series having the differential representation  $(\mu, g)$  of dimension  $d$ . We show that the Lie rank of  $g$  is  $\leq d$  and that  $g$  satisfies (C). For the first assertion, we do as in [5] II.a. Let  $T_i$  ( $1 \leq i \leq d$ ) be the series

$$T_i = \sum_w \frac{\partial(h\mu w)}{\partial q_i} \Big|_0 w$$

Let  $P$  be a Lie element. We extend  $\mu : X^* \rightarrow \text{End}(\mathbb{R}[[q]])$  to an algebra homomorphism from  $\mathbb{R}\langle X \rangle$  into  $\text{End}(\mathbb{R}[[q]])$ . Then  $\mu(P)$  is a continuous derivation (because derivations form a Lie algebra) of  $\mathbb{R}[[q]]$ , hence

$$\begin{aligned} (P \circ S, w) &= (S, wP) = h\mu(wP)|_0 = (h\mu w)\mu P|_0 \\ &= \left[ \sum_{1 \leq i \leq d} \frac{\partial(h\mu w)}{\partial q_i} (q_i \mu P) \right] \Big|_0 = \sum_i (T_i, w) (q_i \mu P) \Big|_0 \end{aligned}$$

Thus  $P \circ S = \sum_i (q_i \mu P)|_0 T_i$  is a linear combination of  $T_1, \dots, T_d$ .

We show now that  $g$  satisfies to (C)<sup>5</sup>. By assumption, the series  $h$  and  $q_i \mu x_j$  ( $1 \leq i \leq d$ ,  $0 \leq j \leq n$ ) are convergent in a neighborhood of 0. We thus may find constants  $\alpha$  and  $C$  such these series are all bounded by the same series

$$f = \alpha \sum_r C^r q^r = \alpha(1 - Cq)^{-1}$$

in the sense that the coefficient of  $q_1^{i_1} \dots q_d^{i_d}$  is bounded by  $\alpha C^{i_1 + \dots + i_d}$ . It is then easily shown that  $h\mu w$  ( $w$  of length  $p$ ) is bounded by the series  $f\Delta P$ , where  $\Delta$  is the differential operator

$$\Delta = d \frac{\alpha}{1 - Cq} \frac{\partial}{\partial q}$$

A simple computation shows that

$$f\Delta^p = \frac{\alpha(d\alpha C)^p 1 \cdot 3 \cdots (2p-1)}{(1 - Cq)^{2p+1}}$$

Hence, we obtain

$$|(g, w)| = |hw_w|_0 \leq f\Delta^p|_0 = \frac{\alpha(d\alpha C)^p (2p)!}{2^p p!}$$

As  $\binom{2p}{p}$  is bounded by  $2^p$ , we obtain

$$|(g, w)| \leq \alpha(2d\alpha C)^p p!$$

---

<sup>5</sup>We follow Gröbner [6], chap. 1.

Now let  $P_1, \dots, P_q$  be Lie polynomials,  $y_1, \dots, y_q$  new letters and  $g' \in \mathbb{R}\langle\langle y_1, \dots, y_q \rangle\rangle$  the series having the differential representation  $(\mu', h)$  with  $\mu' y_i = \mu P_i$ . The previous paragraph implies that if  $w$  is a word of length  $p$  in the  $y$ 's, then one has an inequality of the form

$$|(g', w)| \leq \beta D^p p!$$

which proves (C), in view of the remark following the definition of (C).

**b)** We come now to the converse, which is the essential part of the theorem. Let  $g$  be a series of Lie rank  $d$  and which satisfies to the convergence hypothesis.

Let  $L_0 = \{P \in L\langle X \rangle \mid P \circ g = 0\}$ . By assumption,  $L_0$  is of finite codimension  $d$  in  $L\langle X \rangle$ . Moreover, it is a sub-Lie-algebra of  $L\langle X \rangle$ . Let  $P_1, \dots, P_n, \dots$  be a basis of  $L\langle X \rangle$  such that  $P_{d+1}, \dots, P_n, \dots$  is a basis of  $L_0$ . Let  $S_1, \dots, S_d$  the series defined by  $(S_i, P_j) = \delta_{i,j}$  and  $(S_i, P_{i_1}^{j_1} \dots P_{i_r}^{j_r}) = 0$  if  $r = 0$  or if  $j_1 + \dots + j_r \geq 2$  (use the P-B-W theorem). Then

$$g = \sum_{i_1, \dots, i_d \geq 0} \frac{(g, P_1^{i_1} \dots P_d^{i_d})}{i_1! \dots i_d!} S_1^{i_1} \dots S_d^{i_d} \quad (1)$$

Note that the  $S_i$ 's have zero constant term, which ensures that the sum is well-defined. In fact, we shall prove a more general result.

**Proposition 1.** *Let  $L_0$  be a sub-Lie-algebra of  $L\langle X \rangle$  of codimension  $d$ . Let  $P_1, \dots, P_d$  be a basis of  $L\langle X \rangle$  modulo  $L_0$  and  $S_1, \dots, S_d$  series without constant term such that  $(S_i, P_j) = \delta_{i,j}$  and which vanish on the left ideal  $J = \mathbb{R}\langle X \rangle L_0$ . Then*

$$J^\perp = \{S \mid (S, P) = 0, \forall P \in J\} = \mathbb{R}[[S_1, \dots, S_d]]$$

Moreover, any  $S \in \mathbb{R}[[S_1, \dots, S_d]]$  has a unique expression as series in the  $S_i$ 's.

*Proof.* **1)** We show that  $J^\perp$  contains  $\mathbb{R}[[S_1, \dots, S_d]]$ . As  $J^\perp$  is closed for the usual topology of  $\mathbb{R}\langle\langle X \rangle\rangle$  and closed for the operation  $T \rightarrow T \circ P$  ( $P \in \mathbb{R}\langle X \rangle$ ), because  $J$  is a left ideal, it is enough to show that it is also closed for the shuffle. Let  $S, T$  in  $J^\perp$  : it suffices to show that  $(ST) \circ W$  vanishes on  $L_0$  for any word  $w$  (it will imply that  $ST$  vanishes on  $X^* L_0$ , hence on  $J$ ).

**Lemma 3.**  *$T \rightarrow T \circ x$  is a derivation for the shuffle.*

By the lemma (which is well-known),  $(ST) \circ w$  is a linear combination of series of the form  $(S \circ u)(T \circ v)$ . As  $S, T$  vanish on  $J$ , we obtain that  $S \circ u, T \circ v$  vanish on  $L_0$ .

**Lemma 4.** *Let  $i > j$ ,  $T_1, \dots, T_i$  series without constant term and  $Q_1, \dots, Q_j$  be Lie polynomials. Then*

$$(T_1 \dots T_i, Q_1 \dots Q_j) = 0$$

*Proof.* The lemma follows from Lemmas 1 and 2: write that  $(T_1 \dots T_i, Q_1 \dots Q_j) = (T_1 \otimes \dots \otimes T_i, c_i(Q_1 \dots Q_j))$  and note that  $c_i(Q_1 \dots Q_j)$ , which is the product from 1 to  $j$  of

$$Q_\ell \otimes 1 \dots \otimes 1 + 1 \otimes Q_\ell \dots \otimes 1 + 1 \otimes 1 \dots \otimes Q_\ell$$

is a sum of tensors each of which has a 1 as factor; as  $(T_k, 1) = 0$ , we obtain Lemma 4.  $\square$

By this lemma, the shuffle of two series which vanish on  $L_0$  is still vanishing on  $L_0$ . Hence each  $(S \circ u)(T \circ v)$  vanishes on  $L_0$ , and so does also  $(ST) \circ w$ .

**2)** We prove that  $J^\perp \subset \mathbb{R}[[s_1, \dots, S_d]]$ . Let  $S \in J^\perp$ . We have to find coefficients  $a_{i_1, \dots, i_d}$  such that

$$S = \sum_{i_1, \dots, i_d} a_{i_1, \dots, i_d} S_1^{i_1} \dots S_d^{i_d} \quad (2)$$

For  $I = (i_1, \dots, i_d)$ , let  $a(I) = a_{i_1, \dots, i_d}$ ,  $S(I) = S_1^{i_1} \dots S_d^{i_d}$ ,  $P(I) = P_1^{i_1} \dots P_d^{i_d}$ ,  $|I| = i_1 + \dots + i_d$  and  $I! = i_1! \dots i_d!$ . By the P-B-W theorem, we have to show that both sides of (2) have the same value on any polynomial of the form

$$P_1^{i_1} \dots P_r^{i_r}, \quad r \geq 0, \quad 1 \leq i_1 < \dots < i_r, \quad 1 \leq j_1, \dots, j_r$$

But, if  $r > d$ , then this polynomial is in  $J$ , hence both sides map it to zero. Hence, we have to find coefficients  $a(I)$  such that

$$\forall J, \quad (S, P(J)) = \sum_I a(I) (S(I), P(J)) \quad (3)$$

**Lemma 5.** (i) If  $|I| > |J|$  or if  $|I| = |J|$  and  $I \neq J$ , then  $(S(I), P(J)) = 0$   
(ii)  $(S(I), P(I)) = |I|!$

*Proof.* If  $|I| > |J|$ , use Lemma 4. Otherwise, use Lemmas 1 and 2 to prove that

$$(T_1 \dots T_n, Q_1 \dots Q_n) = \sum_{\sigma \in \mathfrak{S}_n} (T_1, Q_{\sigma(1)}) \dots (T_n, Q_{\sigma(n)})$$

which is true for any series  $T_i$  without constant term and any Lie polynomials  $Q_j$ .  $\square$

Lemma 5 shows that (3) is a triangular system of linear equations in the  $a$ 's, with  $I!$  on the diagonal. Hence, it admits one and only one solution, which proves the proposition.  $\square$

(1) is proved by using the fact that in this case one has:  $|I| < |J|$  implies  $(S(I), P(J)) = 0$  (use Lemmas 1 and 2).

(1) gives almost the differential representation of  $g$ . Indeed,  $g$  is given in (1) as a commutative series in  $S_1, \dots, S_d$ , and by Proposition 1,  $\mathbb{R}[[S_1, \dots, S_d]]$  is isomorphic to an algebra of commutative formal power series in  $d$  variables. We have to define  $\mu$  and  $h$ . We let  $h = g$  and define  $\mu w$  ( $w \in X^*$ ) as  $T \rightarrow T \circ w$ .



By Lemma 3,  $\mu x$  is a continuous derivation, which maps  $\mathbb{R}[[S_1, \dots, S_d]]$  into itself (by the proposition). Moreover

$$(g, w) = (g \circ w, 1) = (h\mu w, 1)$$

and the constant term of  $h\mu w$  is also the constant term of  $\mu w$  when expressed as a series in the  $S_i$ 's (because the latter are without constant term). We still have to show that the operators  $\mu x$  are convergent. The series  $P_1 \circ g, \dots, P_d \circ g$  being linearly independent, we may find polynomials  $Q_1, \dots, Q_d$  such that

$$(P_i \circ g, Q_j) = \delta_{i,j}$$

Let  $T_1, \dots, T_d$  be defined by

$$T_i = g \circ Q_i - (g, Q_i) \quad (4)$$

The  $T_i$ 's are without constant term, vanish on  $J$  and we have

$$(T_i, P_j) = (g \circ Q_i, P_j) = (g, Q_i P_j) = (P_j \circ g, Q_i) = \delta_{j,i}$$

Hence by the proposition

$$\mathbb{R}[[T_1, \dots, T_d]] = J^\perp = \mathbb{R}[[S_1, \dots, S_d]]$$

As for  $g$ , we have relations of the form

$$T_j = \sum_I \frac{(T_j, P(I))}{I!} S(I) \quad (5)$$

Moreover by (4), the  $T_j$ 's satisfy to the convergence hypothesis. Thus, by (5), the  $T_j$ 's may be written as convergent series in the  $S_i$ 's. We use now the following classical result.

**Theorem** (of implicit functions). *Let  $t_1, \dots, t_d$  convergent series in  $\mathbb{R}[[s_1, \dots, s_d]]$  without constant term and such that  $\mathbb{R}[[s]] = \mathbb{R}[[t]]$ . Then each  $s_i$  may be written as a convergent series in  $t_1, \dots, t_d$ .*

By this theorem, each  $S_i$  is a convergent series in  $T_1, \dots, T_d$ . As previously, the series

$$T_j \mu x = T_j \circ x$$

satisfy to (C) and are thus convergent series in the  $S_i$ 's; hence, they are also convergent series when expressed as series in the  $T_i$ 's. All this shows that  $(\mu, h)$  is a differential representation of  $g$ .

c) Now, let  $g$  be a series of Lie rank  $d$  and  $(\mu, h)$  be a differential representation of dimension  $d$  of  $g$ . We use the notations of paragraph b).

**Lemma 6.** *The mapping  $\eta : \mathbb{R}[[q]] \rightarrow \mathbb{R}\langle\langle X \rangle\rangle$  which maps  $k$  onto  $\sum_w (k\mu w|_0) w$  is a continuous homomorphism (for the shuffle), such that for any word  $w$  one has  $\eta(k\mu w) = \eta(k) \circ w$ .*

*Proof.* This lemma is a simple consequence of [4] prop. III. 1.  $\square$

**Lemma 7.** *The mapping  $\theta : \mathbb{R}\langle\langle X \rangle\rangle \rightarrow \mathbb{R}\langle\langle X \rangle\rangle$  which maps  $S$  onto  $\sum_I \frac{(S, P(I))}{I!} S(I)$  is a continuous shuffle homomorphism.*

*Proof.* In order to prove this lemma, note that if  $S_1, \dots, S_n, \dots$  are the series which are the elements of the dual basis of the P-B-W basis constructed on  $P_1, \dots, P_n, \dots$ , which correspond to  $P_1, \dots, P_n, \dots$  then  $\mathbb{R}\langle\langle X \rangle\rangle = \mathbb{R}[[S_1, \dots, S_n, \dots]]$  and the mapping of Lemma 7 is just a projection:  $S_1 \rightarrow S_1, \dots, S_d \rightarrow S_d, S_n \rightarrow 0$  if  $n > d$ .  $\square$

By Lemma 6,  $\eta(\mathbb{R}[[q]])$  contains  $g = \eta(h)$  and is closed for the operations  $T \rightarrow T \circ w$ . Hence, it contains the  $T_i$ 's defined by (4), hence also  $\mathbb{R}[[T_i]] = \mathbb{R}[[S_i]]$ . As the restriction of  $\theta$  to  $\mathbb{R}[[S_i]]$  is the identity, the mapping  $\phi = \theta \circ \eta : \mathbb{R}[[q]] \rightarrow \mathbb{R}[[S_i]]$  is surjective. As it is a continuous homomorphism from an algebra of formal power series in  $d$  commutative variables into another,  $\phi$  is also injective. We deduce that  $\eta$  is also a bijection  $\mathbb{R}[[q]] \rightarrow \mathbb{R}[[S_i]]$ : first,  $\eta$  is injective (otherwise  $\phi = \theta \circ \eta$  is not); moreover we may find series  $k_1, \dots, k_d$  in  $\mathbb{R}[[q]]$  such that  $q_i \rightarrow k_i$  is a continuous automorphism of  $\mathbb{R}[[q]]$  and such that  $\phi(k_i) = S_i$ . As  $\eta(\mathbb{R}[[q]])$  contains  $\mathbb{R}[[S_i]]$  and  $\mathbb{R}[[q]] = \mathbb{R}[[k_i]]$ , we have that  $S_i$  is a series in the  $\eta(k_i)$ 's:  $S_i = s(\eta(k_1), \dots, \eta(k_d))$ .

Apply  $\theta$ : then  $S_i = \theta(S_i) = s(S_1, \dots, S_d)$ , which shows that  $s$  has only the term  $S_i$ , hence  $S_i = \eta(k_i)$ . This shows that  $\eta(\mathbb{R}[[q]]) = \eta(\mathbb{R}[[k_i]]) = \mathbb{R}[[\eta(k_i)]] = \mathbb{R}[[S_i]]$  and  $\eta$  is a bijection as claimed.

We still have to prove the assertions about convergence (we have already seen that any differential representation of dimension  $d$  of  $g$  is isomorphic to the one defined by  $S_1, \dots, S_d$ ). By assumption, the series  $g$  and the operators  $T \rightarrow T \circ x$  of  $\mathbb{R}[[S_i]]$  are convergent when expressed as series in the  $\eta(q_i)$ 's (as  $h$  and  $\mu x$  are convergent, when expressed in the  $q_i$ 's). Hence the series  $T_i$  of (4) are convergent in the  $\eta(q_i)$ 's. Hence  $\eta$  is a convergent isomorphism from  $\mathbb{R}[[q]]$  onto  $\mathbb{R}[[T_i]]$ . This ends the proof of the theorem.

## References

- [1] P. d'Alessandro, A. Isidori, A. Ruberti: Realization and structure theory of bilinear systems, Siam J. Control 12 (1974) 517-535.
- [2] R.W. Brockett: On the algebraic structure of bilinear systems, In: Theory and Application of Variable Structure Systems (Mohler, Ruberti, ed.), Acad. Press (1972) 153-168.
- [3] M. Fliess: Sur la réalisation des systèmes dynamiques bilinéaires, C.R. Acad. Sci. Paris A 277 (1973) 923-926.

- [4] M. Fliess: Fonctionnelles causales non linéaires et indéterminées non commutatives, Bull. Soc. Math. France 109 (1981) 3-40.
- [5] M. Fliess: Réalisation locale des systèmes non linéaires, algèbres de Lie filtrées transitives et séries génératrices non commutatives, Invent. Math. 71 (1983) 521-537.
- [6] W. Gröbner: Die Lie Reihen und ihre Anwendungen, Berlin, VEB Deutscher Verlag der Wissenschaften (1967).
- [7] R. Hermann, A.J. Krener: Nonlinear controllability and observability, IEEE Trans. Automat. Control 22 (1977) 728-740.
- [8] J.E. Humphreys: Introduction to Lie algebras and representation theory, Springer Verlag (1980).
- [9] B. Jakubczyk: Existence and uniqueness of realizations of nonlinear systems, SIAM J. Control Optimiz 18 (1980) 455-471.
- [10] R.E. Kalman: Mathematical description of linear dynamical systems, SIAM J. Control 1 (1963) 152-162.
- [11] M. Lothaire, Combinatorics on words, Addison Wesley (1983).
- [12] H.J. Sussmann: Minimal realizations and canonical forms for bilinear systems, J. Franklin Inst. 301 (1976) 593-604.
- [13] H.J. Sussmann: Existence and uniqueness of minimal realizations of nonlinear systems, Math. Systems Theory 10 (1977) 263-284.