Journal of Algebra and Related Topics
Vol. 5, No 2, (2017), pp 25-33

ALGEBRAIC ADJOINT OF THE POLYNOMIALS-POLYNOMIAL MATRIX MULTIPLICATION

R. ANDRIAMIFDISOA* AND H. RANDRIAMBOLASATA

ABSTRACT. This paper deals with a result concerning the algebraic dual of the linear mapping defined by the multiplication of polynomial vectors by a given polynomial matrix over a commutative field.

1. INTRODUCTION

Usually, people (including many mathematicians) think that the work of applied mathematicians is to apply some theory from fundamental mathematics in another area of speciality. In this paper, we follow the inverse method: after having studied practical applications, mainly from algebraic coding and algebraic systems theory, we have looked for the algebraic theories that are used within these applications.

Algebraic dynamical systems specialists, Willems ([13]), Oberst ([8]), Zerz ([14]) and, to some extend, Napp and Rocha ([7]), to name just a few, used *polynomial and matrix operators in the shifts*, which give *difference equations*, to define *discrete linear dynamical systems*.

Difference equations, involving polynomial operators in the shifts (a particular case of the matrix operator in the shifts) are also widely used in information and algebraic coding theory, especially with the

MSC(2010): Primary: 15A04; Secondary: 39A06
Keywords: Operator in the shifts, scalar product, algebraic adjoint.
Received: 14 November 2017, Accepted: 3 January 2018.
*Corresponding author.

Berlekamp-Massey algorithm and its variants ([4, 6, 11, 12]).

Even though the formulae used to define polynomial operator in the shifts (2.2) resembles to the usual vector-matrix multiplication, it is often stated without explanation. Moreover, it is somewhat frightening and discouraging for those who want study discrete linear dynamical systems.

In [2, 3], we gave explanations of the *polynomial operator in the shifts* and the *polynomial matrix operator in the shifts*, using categories and functors. Once again, the use of categories and functors may discourage those who are not familiar with these and moreover, not all of mathematicians does agree with the formalisms of these theories.

In this article, we use a much simpler approach: we will simply prove that the polynomial matrix operator in the shifts is the *algebraic adjoint* of the multiplication of polynomial vectors by the polynomial matrix, with respect to a *scalar product*. This is our main result.

The main objets of our study are polynomials, vectors and matrices of polynomials and vectors of power series over a commutative field.

In section 2, we introduce the notations and the properties we will need. Because the terminology "scalar product"is often stated without explanation, and its meaning sometimes varies, we end this section by the Proposition 2.1, which includes de definition of a scalar product and gives a particular case of scalar product, which we will need.

In section 3 we state and prove our main theorem, which is Theorem 3.1.

We hope that our result gives an explanation of the matrix operator in the shifts and provides a nice and elegant presentation of this operator. Moreover, we believe that our method permits the constructions of other interesting linear operators in algebra and interpretations of many existing ones, for example in algebraic dynamical systems with continuous time-set or involving $\mathbb{Z}$ as time-set.

2. PRELIMINARIES

Here, we recall the notations we used in [1, 2, 3] and [9]. We denote by $\mathbb{F}$ a commutative field. Let $r \geqslant 1$ be an integer, $X_1, \ldots, X_r$

and $Y_1, \dots, Y_r$ distinct letters, which we call *variables*. For the sake of simplicity, the letter X (resp. Y) will denote $X_1, \dots, X_r$ (resp. $Y_1, \dots, Y_r$). Let $\mathbb{N}$ be the set of positive integer. For a multi-index $\alpha = (\alpha_1, \dots, \alpha_r) \in \mathbb{N}^r$, we define X^α (resp. Y^α) by

$$X^\alpha = X_1^{\alpha_1} \cdots X_r^{\alpha_r} \text{ (resp. } Y^\alpha = Y_1^{\alpha_1} \cdots Y_r^{\alpha_r}).$$

Let $\mathbf{D} = \mathbb{F}[X_1, \dots, X_r] = \mathbb{F}[X]$ be the $\mathbb{F}$-vector space of the polynomials with the r variables $X_1, \dots, X_r$ and coefficients in $\mathbb{F}$. An element of $\mathbf{D}$ can be uniquely written as

$$d(X_1, \dots, X_r) = d(X) = \sum_{\alpha \in \mathbb{N}^r} d_\alpha X^\alpha$$

with $d_\alpha \in \mathbb{F}$ for all $\alpha \in \mathbb{N}^r$, where $d_\alpha = 0$ except for a finite number of α's.

Let $\mathbf{A} = \mathbb{F}[[Y_1, \dots, Y_r]] = \mathbb{F}[[Y]]$ be $\mathbb{F}$-vector space of the formal power series with the variables $Y_1, \dots, Y_r$ and coefficients in $\mathbb{F}$. An element of $\mathbf{A}$ can be uniquely written as

$$W(Y_1, \dots, Y_r) = W(Y) = \sum_{\alpha \in \mathbb{N}^r} W_\alpha Y^\alpha$$

where $W_\alpha \in \mathbb{F}$ for all $\alpha \in \mathbb{N}^r$.

For integers $k, l \geqslant 1$, the set of matrices with k rows and l columns with entries in $\mathbf{D}$ is denoted by $\mathbf{D}^{k,l}$. An element $R(X) \in \mathbf{D}^{k,l}$ is of the form

$$R(X) = (R_{ij}(X))_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l}$$

where $R_{ij}(X) \in \mathbf{D}$ for $i = 1, \dots, k$ and $j = 1, \dots, l$. For $l \in \mathbb{N}^*$, the notation $\mathbf{A}^l$ will be for the set of row of power series of $\mathbf{A}$ with l rows : an element $W(Y)$ of $\mathbf{A}^l$ is of the form

$$W(Y) = \begin{pmatrix} W_1(Y) \\ \vdots \\ W_l(Y) \end{pmatrix}$$

where $W_j(Y) \in \mathbf{A}$ for $j = 1, \dots, l$ and $\mathbf{D}^l$ is the set of column vector of polynomials of $\mathbf{D}$ with l columns. An element $d(X) \in \mathbf{D}^l$ is of the form

$$d(X) = (d_1(X), \dots, d_l(X))$$

where $d_j(X) \in \mathbf{D}$ for $j = 1, \dots, l$. The set $\mathbf{D}^l$ is an infinite-dimensional $\mathbb{F}$-vector space. A basis is given by the set

$$\{X^\alpha e_j^{(l)} \mid \alpha \in \mathbb{N}^r \text{ and } j = 1, \dots, l\}, \tag{2.1}$$

where $e_j^{(l)} = \underbrace{(0, \ldots, 0, 1, 0, \ldots, 0)}_{\text{1 at the } j\text{-th column}}$.

A polynomial $d(X) \in \mathbf{D}^l$ operates on a power series $W(Y) \in \mathbf{A}$ by the " polynomial operation in the shifts"

$$d(X) \circ W(Y) = \sum_{\beta} (\sum_{\alpha} d_\alpha W_{\alpha+\beta}) Y^\beta \in \mathbf{A},$$

([1, 2, 8, 9, 13, 14]) . Similarly, a matrix $R(X) \in \mathbf{D}^{k,l}$ operates on a column vector of power series $W(Y) = (W_1(Y), \ldots, W_l(Y))^T \in \mathbf{A}^l$ (where T is the transposition) by the "polynomial matrix operation in the shifts"

$$\begin{aligned} R(X) \circ W(Y) &= \begin{pmatrix} R_1(X) \circ W(Y) \\ \vdots \\ R_k(X) \circ W(Y) \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^l R_{1j}(X) \circ W_j(Y) \\ \vdots \\ \sum_j^l R_{kj}(X) \circ W_j(Y) \end{pmatrix} \in \mathbf{A}^k, \qquad (2.2) \\ &= \begin{pmatrix} \sum_{j=1}^l \sum_\beta (\sum_\alpha R_{1j\alpha} W_{j\beta}) Y^\beta \\ \vdots \\ \sum_{j=1}^l \sum_\beta (\sum_\alpha R_{kj\alpha} W_{j\beta}) Y^\beta \end{pmatrix} \in \mathbf{A}^k, \end{aligned}$$

where $R_i(X) = (R_{ij}(X)), i = 1, \ldots, k$ and $j = 1, \ldots, l$ are the rows of $R(X)$, with $R_{ij}(X) = \sum_\alpha R_{ij\alpha} X^{\alpha}$' ([1, 3, 8, 9, 13, 14]).

For the definition of a *scalar product* or a *bilinear form which is non-degenerate (non-singular) on the right*, we refer to [1, 2, 5, 8, 10, 9]. In our definition, the mapping has values in the field $\mathbb{F}$.

Proposition 2.1. *The* $\mathbb{F}$*-bilinear mapping*

$$\begin{aligned} &\langle -, - \rangle : \mathbf{D}^l \times \mathbf{A}^l \longrightarrow \mathbb{F}, \\ &(d(X), W(Y)) \longmapsto \langle d(X), W(Y) \rangle = \sum_{j=1}^l (\sum_{\alpha \in \mathbb{N}^r} d_{j\alpha} \cdot W_{j\alpha}) \qquad (2.3) \end{aligned}$$

is a scalar product.

Proof. Since it is obvious that the mapping in Proposition 2.1 is $\mathbb{F}$-bilinear, we will prove three properties :

(1) Let $d(X) = (d_1(X), \ldots, d_l(X)), b(X) = (b_1(X), \ldots, b_l(X)) \in \mathbf{D}^l$

such that $\langle d(X), W(Y)\rangle = \langle b(X), W(Y)\rangle$ for $W(Y) \in \mathbf{A}^l$. Fix $j \in \{1, \ldots, l\}$ and $\beta \in \mathbb{N}^r$ and take

$$W(Y) = \begin{pmatrix} 0 \\ \vdots \\ \delta_\beta \\ \vdots \\ 0 \end{pmatrix} \in \mathbf{A}^l \quad (\delta_\beta \text{ at the } j\text{-th row}).$$

Then

$$\begin{aligned} \langle d(X), W(Y)\rangle &= \sum_{\alpha \in \mathbb{N}^r} d_{j\alpha} W_{j\alpha} = d_{j\beta} \\ \langle b(X), W(Y)\rangle &= \sum_{\alpha \in \mathbb{N}^r} b_{j\alpha} W_{j\alpha} = b_{j\beta}. \end{aligned}$$

Hence $d_{j\beta} = b_{j\beta}$. Since this is true for $\beta \in \mathbb{N}^r$ we have $d_i(X) = b_j(X)$ for $j = 1, \ldots, l$. Thus $d(X) = b(X)$, i.e. the mapping

$$\begin{aligned} &\mathbf{D}^l \longrightarrow \mathbf{Hom}_{\mathbb{F}}(\mathbf{A}^l, \mathbb{F}) \\ &d(X) \longmapsto \begin{cases} \langle d(X), -\rangle : \mathbf{A}^l \longrightarrow \mathbb{F} \\ W(Y) \longmapsto \langle d(X), W(Y)\rangle \end{cases} \end{aligned} \tag{2.4}$$

is injective.

Now, let $W(Y), V(Y) \in \mathbf{A}^l$ such that $\langle -, W(Y)\rangle = \langle -, V(Y)\rangle$, i.e. $\langle d(X), W(Y)\rangle = \langle d(X), V(Y)\rangle$ for $d(X) \in \mathbf{D}^l$. Fix $j \in \{1, \ldots, l\}$ and $\beta \in \mathbb{N}^r$ and take $d(X) = (0, \ldots, 0, X^\beta, 0, \ldots, 0)$ (X^β at the j-th column). We get

$$\begin{aligned} \langle d(X), W(Y)\rangle &= W_{j\beta} \\ \langle d(X), V(Y)\rangle &= V_{j\beta}, \end{aligned}$$

i.e. $W_{j\beta} = V_{j\beta}$. Since it is true for $\beta \in \mathbb{N}^r$ and $j \in \{1, \ldots, \}$, we have $W_j = V_j$ for $j = 1, \ldots, l$. Thus $W(Y) = V(Y)$ and the, the mapping

$$\begin{aligned} &\mathbf{A}^l \longrightarrow \mathbf{Hom}_{\mathbb{F}}(\mathbf{D}^l, \mathbb{F}) \\ &W(Y) \longmapsto \begin{cases} \langle -, W(Y)\rangle : \mathbf{D}^l \longrightarrow \mathbb{F} \\ d(X) \longmapsto \langle d(X), W(Y)\rangle \end{cases} \end{aligned} \tag{2.5}$$

is also injective.

(2) Let $\psi \in \mathbf{Hom}_{\mathbb{F}}(\mathbf{D}^l, \mathbb{F})$. Take

$$W(Y) = \begin{pmatrix} W_1(Y) \\ \vdots \\ W_j(Y) \\ \vdots \\ W_l(Y) \end{pmatrix} \in \mathbf{A}^l$$

with $W_{j\alpha} = \psi(X^\alpha e_j^{(l)})$ for $j \in \{1, \ldots, l\}$ and $\alpha \in \mathbb{N}^r$. For $d(X) \in \mathbf{D}^l$, using the $\mathbb{F}$-basis of $\mathbf{D}^l$ in (2.1), write

$$d(X) = \sum_{j=1}^{l} \sum_{\alpha \in \mathbb{N}^r} d_\alpha X^\alpha e_j^{(l)}. \tag{2.6}$$

It follows that

$$\begin{aligned}
\psi(d(X)) &= \psi(\sum_{j=1}^{l} \sum_{\alpha \in \mathbb{N}^r} d_{\alpha j} X^\alpha e_j^{(l)}) \\
&= \sum_{j=1}^{l} \sum_{\alpha \in \mathbb{N}^r} d_{\alpha j} \psi(X^\alpha e_j^{(l)}) \\
&= \sum_{j=1}^{l} \sum_{\alpha \in \mathbb{N}^r} d_{\alpha j} W_{\alpha j} = \langle d(X), W(Y) \rangle.
\end{aligned}$$

Thus $\psi = \langle -, W(Y) \rangle$. Therefore, the mapping (2.5) is surjective and is an isomorphism of vector spaces (this is the *non-degeneracy on the right*). We have shown that the mapping is $\langle -, - \rangle$ bilinear form, non-degenerate on the right. $\square$

3. MAIN RESULT

Now, we state and prove our main theorem :

Theorem 3.1. *The $\mathbb{F}$-bilinear mapping*

$$\begin{aligned}
R(X) : \mathbf{A}^l &\longrightarrow \mathbf{A}^k, \\
W(Y) &\longmapsto R(X) \circ W(Y)
\end{aligned} \tag{3.1}$$

is the algebraic adjoint of the $\mathbb{F}$-linear mapping

$$\begin{aligned}
d(X) : \mathbf{D}^k &\longrightarrow \mathbf{D}^l, \\
d(X) &\longmapsto d(X)R(X)
\end{aligned} \tag{3.2}$$

according to the scalar product of Proposition 2.1. This means that the $\mathbb{F}$-linear mapping (3.1) is the only one from $\mathbf{A}^l$ to $\mathbf{A}^k$ which verifies

$$\langle d(X)R(X), W(Y) \rangle = \langle d(X), R(X) \circ W(Y) \rangle$$

for $d(X) \in \mathbf{D}^k$ and $W(Y) \in \mathbf{A}^l$.

Proof. Let $W(Y) \in \mathbf{A}^l, d(X) \in \mathbf{D}^k$ and $R(X) \in \mathbf{D}^{k,l}$, where, for $i = 1, \ldots, k$ and $j = 1, \ldots l$,

$$d_i(X) = \sum_{\alpha \in \mathbb{N}^r} d_{i\alpha} X^\alpha,$$

$$R_{ij}(X) = \sum_{\alpha \in \mathbb{N}^r} R_{ij\alpha} X^\alpha,$$

with $d_{i\alpha} = 0$ (resp. $R_{ij\alpha} = 0$) except for a finite number of α's. We denote by$(d(X)R(X))_j$ the j-th column of $d(X)R(X)$. Then

$$d(X)R(X) = (d(X)R(X))_{j=1,\ldots,l} \in \mathbf{D}^l$$

where

$$(d(X)R(X))_j = \sum_{i=1}^{k} d_i(X) R_{ij}(X) \tag{3.3}$$

for $j = 1, \ldots, l$. The formulae for polynomial multiplication gives

$$d_i(X) R_{ij}(X) = \sum_{\alpha,\beta \in \mathbb{N}^r} d_{i\alpha} R_{ij\beta} X^{\alpha+\beta} \tag{3.4}$$

for $i = 1, \ldots, k$ and $j = 1, \ldots, l$. Writing $\gamma = \alpha + \beta$, we then have

$$d_i(X) R_{ij}(X) = \sum_{\alpha,\gamma \in \mathbb{N}^r, \alpha \leqslant_+ \gamma} d_{i\alpha} R_{ij(\gamma-\alpha)} X^\gamma \tag{3.5}$$

(where, $\alpha = (\alpha, \ldots, \alpha_r) \leqslant_+ \gamma = (\gamma_1, \ldots, \gamma_r)$ means that $\alpha_i \leqslant \gamma_i$ for $i = 1, \ldots, r$) so that for $i = 1, \ldots, k, j = 1, \ldots, l$ and $\gamma \in \mathbb{N}^r$, the coefficient of X^γ in the polynomial $d_i(X)R_{ij}(X)$ is

$$[d_i(X) R_{ij}(X)]_\gamma = \sum_{\alpha \in \mathbb{N}^r, \alpha \leqslant_+ \gamma} d_{i\alpha} R_{ij(\gamma-\alpha)}.$$

Now, we are ready to calculate the scalar product $\langle d(X)R(X), W(Y) \rangle$. We have

$$\begin{aligned} d(X)R(X) &= (d(X)R(X))_{j=1,\ldots,l} \in \mathbf{D}^l \\ &= (\sum_{i=1}^{k} d_i(X) R_{i1}(X), \ldots, \sum_{i=1}^{k} d_i(X) R_{il}(X)). \end{aligned}$$

Using (3.5), we get

$$d(X)R(X) = (\sum_{i=1}^{k} \sum_{\alpha,\gamma \in \mathbb{N}^r, \alpha \leqslant_+ \gamma} d_{i\alpha} R_{i1(\gamma-\alpha)} X^\gamma, \ldots, \sum_{i=1}^{k} \sum_{\alpha,\gamma \in \mathbb{N}^r, \alpha \leqslant_+ \gamma} d_{i\alpha} R_{il(\gamma-\alpha)} X^\gamma). \tag{3.6}$$

Proposition 2.1 gives

$$\langle d(X)R(X), W(Y)\rangle = \sum_{j=1}^{l}(\sum_{\gamma\in\mathbb{N}^r}[(d(X)R(X))_j]_\gamma \cdot W_{j\gamma}).$$

By (3.6), for $j = 1, \dots, l$ and $\gamma \in \mathbb{N}^r$, we have

$$[(d(X)R(X))_j]_\gamma = \sum_{i=1}^{k}\sum_{\alpha\in\mathbb{N}^r, \alpha\leqslant_+\gamma} d_{i\alpha}R_{ij(\gamma-\alpha)},$$

so that

$$\langle d(X)R(X), W(Y)\rangle = \sum_{j=1}^{l}(\sum_{\alpha\in\mathbb{N}^r,\gamma\in\mathbb{N}^r,\alpha\leqslant_+\gamma}\sum_{i=1}^{k} d_{i\alpha}R_{ij(\gamma-\alpha)} \cdot W_{j\gamma}), \quad (3.7)$$

and

$$\begin{aligned}\langle d(X), R(X)\circ W(Y)\rangle &= \sum_{i=1}^{k}(\sum_{\alpha\in\mathbb{N}^r} d_{i\alpha}\cdot[(R(X)\circ W(Y))_j]_\alpha) \\ &= \sum_{j=1}^{l}(\sum_{\alpha,\beta\in\mathbb{N}^r}\sum_{i=1}^{k} d_{i\alpha}R_{ij\beta}W_{j(\alpha+\beta)}).\end{aligned} \quad (3.8)$$

Comparing (3.7) and (3.8), this latter with the indices change $\gamma = \alpha+\beta$, we have

$$\langle d(X)R(X), W(Y)\rangle = \langle d(X), R(X)\circ W(Y)\rangle.$$

Now, suppose that we have a **D**-linear mapping $f : \mathbf{A}^l \longrightarrow \mathbf{A}^k$ such that for $d(X) \in \mathbf{D}^k$ and $W(Y) \in \mathbf{A}^l$,

$$\langle d(X)R(X), W(Y)\rangle = \langle d(X), f(W(Y))\rangle,$$

i.e.

$$\langle d(X), R(X)\circ(W(Y)\rangle = \langle d(X), f(W(Y))\rangle$$

Using the notations in (2.5), we then have

$$\langle -, R(X)\circ W(Y)\rangle = \langle -, g(W(Y))\rangle.$$

By the injectivity of the mapping in (2.5), it follows that $R(X)\circ W(Y)) = g(W(Y))$. It follows that g is the same as the mapping defined by $R(X)$ in (3.1). Therefore, there is one algebraic adjoint only. □

Acknowledgments

The authors would like to thank the referees for careful reading.

References

[1] R. Andriamifidisoa, *Systèmes Dynamiques Linéaires Discrets et Codes Algébriques*, Thèse de Doctorat, Université d'Antananarivo, 2002.

[2] R. Andriamifidisoa and J. Andrianjanahary, *Polynomial Operators in the Shifts in Discrete Algebraic Dynamical Systems*, British Journal of Mathematics and Computer Science, (2) **6** (2015), 119-128.

[3] R. Andriamifidisoa, *Action of a Polynomial Matrix on a Vector of Power Series*, British Journal of Mathematics and Computer Science, (4) **16** (2016), 1-8.

[4] M. Kuijper, *Berlekamp-Massey Algorithm, error-correstion, keystream and modeling, Dynamical Systems, Control, Coding, Computer Vision*, Springer, 1999.

[5] S. Lang, *Algebra*, Springer, Revised Third Edition, 2003.

[6] J. Massey, *Shift-Register Synthesis and BCH Decoding*, IEEE Trans. IT, (1) **15** (1969), 122-127.

[7] D. Napp and P. Rocha, *Strongly Autonomous Interconnections and Stabilization of 2D Behaviors*, Asian J. Control, (2) **12**, 127-135, 2010.

[8] U. Oberst, *Multidimensional Constant Linear Systems*, Acta Appl. Math., **20** (1990), 1-175.

[9] H. Randriambolasata, *Systèmes Dynamiques Algebriques et Décodage des Codes Reed-Solomon*, Mémoire de Master II, Université d'Antananarivo, 2017.

[10] L. Schwarz, *Analyse, Topologie générale et analyse fonctionnelle*, Hermann, EDITEURS DES SCIENCES ET DES ARTS, 1993.

[11] S. Sakata, *Extension of the Berlekamp-Massey Algorithm to N Dimensions*, Inform. and Comput., **84** (1990), 207-239.

[12] K. Saints and C. Heegard, *Algebraic-geometric codes and multidimensional cyclic codes : A unified theory and algorithms for decoding using Groebner bases*, IEEE Trans. IT, (6) **41** (1995), 1733-1751.

[13] J.C. Willems, *Models for Dynamics*, Dynamics Reported, **2** (1989), 171 - 296.

[14] E. Zerz, *Behavioral systems theory: a survey*, Int. J. Appl. Math. Comput. Sci., (3) **18** (2008), 265-270.

R. Andriamifidisoa
Department of Mathematics and Computer Science, Faculty of Sciences, University of Antananarivo, Antananarivo, Madagascar.
Email: `rmw278@yahoo.fr`

H. Randriambolasata
Laboratoire de Grandes Déviations et d'Algèbre Appliquée, Department of Mathematics and Computer Science, University of Antananarivo, Antananarivo, Madagascar.
Email: `sosorandriambolasata@gmail.com`