On algebraic simplifications of linear functional systems

Thomas Cluzeau[1] and Alban Quadrat[2]

[1] XLIM (UMR CNRS 6172), DMI, CANSO Project, Université de Limoges, ENSIL, 16 Rue d'Atlantis, Parc Ester Technopole, 87068 Limoges Cedex, France
cluzeau@ensil.unilim.fr

[2] INRIA Sophia Antipolis, APICS Project, 2004 Route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex, France
Alban.Quadrat@sophia.inria.fr

Introduction

Given a linear functional system coming from mathematical physics, applied mathematics, engineering sciences or control theory, it is often interesting to simplify the equations of the system before studying its structural properties and using numerical analysis methods.

In the case of linear ordinary differential systems of the form $\dot{x} = A(t)\,x$, where A is a $n \times n$ matrix with entries in the field $\mathbb{Q}(t)$ of rational functions, i.e., $A \in \mathbb{Q}(t)^{n\times n}$, the computer algebra community has developed algorithms for *reducing* (resp., *decomposing*) such systems. Here, reducing (resp., decomposing) the system means finding an invertible change of variables $x = P(t)\,y$ such that the new differential system for y writes $\dot{y} = B(t)\,y$, where $B(t)$ has a block-triangular (resp., a block-diagonal) form. One kind of algorithms to perform this task is based on an object called the *eigenring* of the system $\dot{x} = A(t)\,x$. The eigenring is the ring of matrices $P \in \mathbb{Q}(t)^{n\times n}$ which commute with the derivation $\nabla = \frac{d}{dt}\,I_n - A(t)$, namely, $P\,\nabla = \nabla\,P$, which is equivalent to $\dot{P}(t) = A(t)\,P(t) - P(t)\,A(t)$. If one can find an *idempotent* P in the eigenring, namely, $P^2 = P$, then one can decompose the system $\dot{x} = A(t)\,x$. For more details, we refer the reader to [1, 16, 19] and references therein.

The eigenring approach has been extended to linear (q-)difference systems (see, e.g., [1]) and most recently to algebraic integrable connections (see [16, 20] and references therein). This approach is restricted to the so-called class of *D-finite* linear functional systems ([2]) since it is based on the property that the latter systems are finite-dimensional vector spaces over the base field k. Unfortunately, this approach cannot be extended to the main classes of linear functional systems (e.g., ordinary/partial differential equations, time-delay equations, difference equations) appearing in applied mathematics, mathematical physics, engineering sciences and control theory as they are generally not D-finite.

If we consider linear systems of ordinary differential/difference equations with constant coefficients, the *Smith canonical form* can be used to determine an equivalent system defined by decoupled scalar equations: here again, this technique simplifies the study of the original system. The influence of the Smith form has been particularly evident in the control theory community where it has played an important role in the so-called *polynomial approach* pioneered by Rosenbrock, Kučera, Kailath and others. For more details, we refer to [10, 12, 18] and references therein. A generalization of the Smith canonical form to (left/right) principal ideal domains exists and is usually called the *Jacobson canonical form* ([8, 15]). However, once again, Smith and Jacobson canonical forms do not exist for the main classes of linear functional systems coming from applied mathematics, mathematical physics, engineering sciences or control theory as, for instance, they do not exist for linear systems of partial differential equations or differential time-delay equations.

Starting from these observations and trying to fill the gap, in [5, 6], we have studied the factorization and decomposition problems for a larger class of linear functional systems (determined, over-determined, under-determined) within a *constructive homological algebra approach*. Using the concept of Ore algebras of functional operators (e.g., ordinary/partial differential operators, shift operators, time delay-operators), we have developed in [5, 6] algorithms for computing morphisms between finitely presented left modules over an Ore algebra and idempotent endomorphisms of a finitely presented left module over an Ore algebra. Then, we have given three theorems (recalled hereafter) concerning the factorization, reduction and decomposition of linear functional systems. Note that, as in the eigenring approach, idempotents are crucial for the decomposition problem. Finally, these results naturally find applications in control theory (i.e., study of structural properties, study of the Monge problem and its applications to optimal control, decoupling problems), engineering sciences (e.g., algebraic pre-conditioner to numerical analysis methods) and mathematical physics (e.g., search for quadratic conservation laws). For some applications, see [5, 6].

The purpose of this paper is to give a survey on the main theoretical results developed in [5, 6] based on a constructive homological algebra approach. See [7] for an implementation of those results in the OreMorphisms package.

1 Notations and Problems

In this paper, we denote by D a non-commutative ring, $R \in D^{q \times p}$ a $q \times p$ matrix with entries in D and $\mathrm{GL}_p(D)$ the *general linear group* of units of the ring $D^{p\times p}$, i.e., $\mathrm{GL}_p(D) = \{U \in D^{p\times p} \mid \exists\, V \in D^{p\times p} : U\,V = V\,U = I_p\}$. Given $R \in D^{q\times p}$, the latter results are related to the following three problems:

1. *Factorization problem*: Find two matrices $L \in D^{q\times r}$ and $S \in D^{r\times p}$ such that we have the factorization $R = L\,S$.
2. *Reduction problem*: Find two matrices $U \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $\overline{R} = V\,R\,U^{-1} \in D^{q\times p}$ has a block-triangular form.
3. *Decomposition problem*: Find two matrices $U \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $\overline{R} = V\,R\,U^{-1} \in D^{q\times p}$ has a block-diagonal form.

In what follows, we shall focus on a particular type of non-commutative polynomial rings called *Ore algebras* of functional operators (e.g., differential operators, time-delay operators, shift operators) over which the existence of *Gröbner bases* is ensured for any *admissible term order*. For a precise definition of an Ore algebra, we refer the reader to [2, 3, 4, 15] or [6, Definition 2.1] and to [2, 13] and the references therein for the concepts of Gröbner bases and admissible term orders. To achieve these conditions, which allow us to constructively work over the ring D, it is sufficient to assume that the Ore algebra D further satisfies the technical hypotheses of [6, Proposition 2.1]. In practice, these conditions are not too restrictive since they are satisfied for the common Ore algebras that we encounter in many examples coming from applied mathematics, mathematical physics, engineering sciences or control theory as, for instance, rings of differential operators, of differential time-delay operators or of shift operators. The reader, unfamiliar with non-commutative polynomial rings, can replace everywhere the Ore algebra D by the commutative polynomial ring $k[x_1, \ldots, x_n]$ with coefficients in a field k (e.g., $k = \mathbb{Q}$).

2 Morphisms and Galois transformations

We recall that the definition of a *left D-module M* is the same as the one of a k-vector space but where the field k is replaced by a ring D and the coefficients of D act on the left on the elements of M, namely, for all m_1, $m_2 \in M$ and for all a_1, $a_2 \in D$, we have $a_1\,m_1 + a_2\,m_2 \in M$ (see, e.g., [17]).

Let D be a non-commutative Ore algebra of functional operators, $\mathcal{F}$ a left D-module and $R \in D^{q\times p}$ a matrix. Then, the *abelian group*, namely, the $\mathbb{Z}$-module, defined by $\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\}$ is called a *linear functional system* or a *behaviour* and $\mathcal{F}$ the *signal space* (see, e.g., [3]).

Within the *algebraic analysis* approach to mathematical systems theory ([11, 14]), the *finitely presented left D-module* $M = D^{1\times p}/(D^{1\times q}\,R)$ is associated with the linear system $\ker_{\mathcal{F}}(R.)$, where $D^{1\times p}$ denotes the left D-module formed by row vectors of length p with entries in D.

Let us introduce a few definitions (see, e.g., [17]).

Definition 1. Let M and M' be two left D-modules. We call *D-morphism* $f : M \longrightarrow M'$, a left D-linear application from M to M', namely:

$$\forall\, m_1,\, m_2 \in M,\ \forall\, a_1,\, a_2 \in D:\ f(a_1\, m_1 + a_2\, m_2) = a_1\, f(m_1) + a_2\, f(m_2).$$

We denote by $\hom_D(M, M')$ the abelian group of D-morphisms from M to M'. If $M' = M$, then $\hom_D(M, M)$ is also denoted by $\mathrm{end}_D(M)$ and an element of $\mathrm{end}_D(M)$ is called a *D-endomorphism* of M.

If D is a commutative ring and M and M' are two D-modules, then the abelian group $\hom_D(M, M')$ inherits a D-module structure. However, if D is a non-commutative ring and M and M' are two left D-modules, then $\hom_D(M, M')$ has only an abelian group structure. If D is a k-algebra, where k is a field included in the center $Z(D) = \{a \in D \,|\, \forall\, b \in D,\ a\, b = b\, a\}$ of the ring D, then $\hom_D(M, M')$ can be endowed with a k-vector space structure. We note that $\mathrm{end}_D(M)$ is a non-commutative ring for the addition and the composition of endomorphisms. The unity of $\mathrm{end}_D(M)$ is id_M. It is called the *D-endomorphism ring* of M. For more details, see, e.g., [17].

Let us now describe the left D-module M in terms of generators and relations. We denote by $\{e_j\}_{j=1,\ldots,p}$ (resp., $\{f_i\}_{i=1,\ldots,q}$) the standard basis of the *free* left D-module $D^{1\times p}$ (resp., $D^{1\times q}$), namely, e_j (resp., f_i) is the row vector of $D^{1\times p}$ (resp., $D^{1\times q}$) defined by 1 at the j^{th} (resp., i^{th}) position and 0 elsewhere, and $\pi : D^{1\times p} \longrightarrow M$ the D-morphism sending an element $\lambda \in D^{1\times p}$ to its residue class $\pi(\lambda)$ in the quotient left D-module $M = D^{1\times p}/(D^{1\times q}\, R)$. For all $i = 1, \ldots, q$, we have $f_i\, R \in (D^{1\times q}\, R)$, a fact implying that $\pi(f_i\, R) = 0$ and, by D-linearity, we then get:

$$\forall\, i = 1, \ldots, q, \quad \pi(f_i\, R) = \pi\left(\sum_{j=1}^{p} R_{ij}\, e_j\right) = \sum_{j=1}^{p} R_{ij}\, \pi(e_j) = 0. \tag{1}$$

Moreover, using the fact that π is surjective, for all $m \in M$, there exists an element $a = (a_1, \ldots, a_p) \in D^{1\times p}$ such that $m = \pi(a) = \sum_{j=1}^{p} a_j\, \pi(e_j)$, proving that the left D-module M is finitely generated by $\{\pi(e_j)\}_{j=1,\ldots,p}$ and its generators $\pi(e_j)$'s satisfy the relations (1) and their left D-linear combinations.

The following result explains why the finitely presented left D-module $M = D^{1\times p}/(D^{1\times q}\, R)$ plays an important role in mathematical systems theory.

Theorem 1 ([11, 14]). *Let D be a ring, $\mathcal{F}$ a left D-module, $R \in D^{q\times p}$ a matrix, $M = D^{1\times p}/(D^{1\times q}\, R)$ the left D-module finitely presented by R and $\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\}$ the corresponding linear functional system. Then, the morphism of abelian groups*

$$\begin{aligned} \psi : \ker_{\mathcal{F}}(R.) &\longrightarrow \hom_D(M, \mathcal{F}), \\ \eta &\longmapsto \psi(\eta) \end{aligned}$$

– where $f = \psi(\eta)$ is the D-morphism defined by $f(\pi(e_i)) = \eta_i$, for $i = 1, \ldots, p$ and $\eta = (\eta_1, \ldots, \eta_p)^T$ – is an isomorphism, i.e., we have:

$$\ker_{\mathcal{F}}(R.) \cong \hom_D(M, \mathcal{F}).$$

Theorem 1 shows that the linear functional system $\ker_{\mathcal{F}}(R.)$ only depends on the finitely presented left D-module M and on the left D-module $\mathcal{F}$ ([11]).

The main tool that we use to handle the three previously stated problems is the study of D-morphisms between finitely presented left D-modules. The next proposition, classical in homological algebra (see, e.g., [17]), will play a fundamental role in what follows.

Proposition 1 ([6]). *Let $R \in D^{q \times p}$ and $R' \in D^{q' \times p'}$ be two matrices with entries in a ring D, $M = D^{1 \times p}/(D^{1 \times q}\, R)$ and $M' = D^{1 \times p'}/(D^{1 \times q'}\, R')$ two finitely presented left D-modules and the projections $\pi : D^{1 \times p} \longrightarrow M$ and $\pi' : D^{1 \times p'} \longrightarrow M'$. A morphism $f \in \hom_D(M, M')$ is then defined by*

$$\forall\, m = \pi(\lambda) \in M,\ \lambda \in D^{1 \times p} :\ f(m) = \pi'(\lambda\, P),$$

where $P \in D^{p \times p'}$ is a matrix such that there exists $Q \in D^{q \times q'}$ satisfying:

$$R\, P = Q\, R'. \tag{2}$$

The pair of matrices (P, Q) is defined up to a homotopy equivalence*, namely, if we denote by $R'_2 \in D^{r' \times q'}$ a matrix satisfying*

$$\ker_D(.R') \triangleq \{\mu \in D^{1 \times q'} \mid \mu\, R' = 0\} = D^{1 \times r'}\, R'_2,$$

then, for all $Z \in D^{p \times q'}$ and $Z' \in D^{q \times r'}$, the matrices defined by

$$\begin{cases} \overline{P} = P + Z\, R', \\ \overline{Q} = Q + R\, Z + Z'\, R'_2, \end{cases} \tag{3}$$

satisfy the relation $R\, \overline{P} = \overline{Q}\, R'$ and define the same D-morphism f.

Proposition 1 can easily be understood if we first note that, contrary to k-vector spaces, a left D-module M is generally not free, i.e., M does not admit a basis. Hence, a D-linear application from a left D-module M to a left D-module M' is generally not defined by the matrix obtained by sending the elements of a basis of M to elements of M'. However, as we have previously seen, $\{\pi(e_j)\}_{j=1,\ldots,p}$ (resp., $\{\pi'(e'_k)\}_{k=1,\ldots,p'}$) forms a family of generators of M (resp., M') and a D-morphism $f \in \hom_D(M, M')$ sends the generators of M to certain elements of M', i.e., we have $f(\pi(e_j)) = \sum_{k=1}^{p'} P_{jk}\, \pi'(e'_k)$, $j = 1, \ldots, p$, where the P_{jk}'s are elements of D which must satisfy the relations coming from the fact that $f(0) = 0$, i.e., f must send the relations $\sum_{j=1}^{p} R_{ij}\, \pi(e_j) = 0$, $i = 1, \ldots, q$, between the generators $\pi(e_j)$'s of M to 0, i.e., for $i = 1, \ldots, q$, by D-linearity, we have:

$$f\left(\sum_{j=1}^{p} R_{ij}\,\pi(e_j)\right) = \sum_{j=1}^{p} R_{ij}\,f(\pi(e_j)) = \sum_{j=1}^{p} R_{ij}\,\left(\sum_{k=1}^{p'} P_{jk}\,\pi'(e'_k)\right)$$
$$= \pi'\left(\sum_{k=1}^{p'}\left(\sum_{j=1}^{p} R_{ij}\,P_{jk}\right)\,e'_k\right) = 0,$$

and thus, $(\sum_{j=1}^{p} R_{ij}\,P_{j1},\ldots,\sum_{j=1}^{p} R_{ij}\,P_{jp'}) \in D^{1\times q'}\,R'$, i.e., there exists a row vector $Q_i \in D^{1\times q'}$ such that $(\sum_{j=1}^{p} R_{ij}\,P_{j1},\ldots,\sum_{j=1}^{p} R_{ij}\,P_{jp'}) = Q_i\,R'$. Hence, we obtain $R\,P = Q\,R'$, where $Q = (Q_1^T \ldots Q_q^T)^T \in D^{q\times q'}$.

We can easily check that the P_{jk}'s are not uniquely defined as, if we also have $f(\pi(e_j)) = \sum_{k=1}^{p'} \overline{P}_{jk}\,\pi'(e'_k)$, then we get

$$\forall\, j = 1,\ldots,p, \quad \sum_{k=1}^{p'} (\overline{P}_{jk} - P_{jk})\,\pi'(e'_k) = 0 = \pi'\left(\sum_{k=1}^{p'} (\overline{P}_{jk} - P_{jk})\,e'_k\right),$$

and thus, the row vector $\overline{P}_{j\bullet} - P_{j\bullet} = (\overline{P}_{j1} - P_{j1},\ldots,\overline{P}_{jp'} - P_{jp'})$ belongs to $D^{1\times q'}\,R'$, i.e., there exists $Z_j \in D^{1\times q'}$ satisfying $\overline{P}_{j\bullet} - P_{j\bullet} = Z_j\,R'$. Hence, we obtain $\overline{P} - P = Z\,R'$, where $Z = (Z_1^T \ldots Z_p^T)^T \in D^{p\times q'}$. Finally, if we denote by $R'_2 \in D^{r'\times q'}$ a matrix generating $\ker_D(.R') = \{\lambda \in D^{1\times q'} \mid \lambda\,R' = 0\}$, i.e. $\ker_D(.R') = D^{1\times r'}\,R'_2$, and $Z' \in D^{q\times r'}$ is any arbitrary matrix, then we get

$$R\,\overline{P} = R\,P + R\,Z\,R' = Q\,R' + R\,Z\,R' = (Q + R\,Z)\,R' = (Q + R\,Z + Z'\,R'_2)\,R',$$

which proves that we have $R\,\overline{P} = \overline{Q}\,R'$, with the notation $\overline{Q} = Q + R\,Z + Z'\,R'_2$.

One of the main interests of computing $\hom_D(M, M')$ is the following corollary of Proposition 1 which is a straightforward consequence of (2).

Corollary 1 ([6]). *Let $\mathcal{F}$ be a left D-module, $R \in D^{q\times p}$, $R' \in D^{q'\times p'}$ and the corresponding two linear functional systems:*

$$\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\}, \quad \ker_{\mathcal{F}}(R'.) = \{\eta' \in \mathcal{F}^{p'} \mid R'\,\eta' = 0\}.$$

Then, an element $f \in \hom_D(M, M')$ defined by matrices $P \in D^{p\times p'}$ and $Q \in D^{q\times q'}$ satisfying (2) induces the following morphism of abelian groups:

$$f^\star : \ker_{\mathcal{F}}(R'.) \longrightarrow \ker_{\mathcal{F}}(R.)$$
$$\eta' \longmapsto \eta = P\,\eta'.$$

By Corollary 1, we obtain that the abelian group $\hom_D(M, M')$ defines transformations sending the solutions of the second system to those of the first one, i.e., defines a *morphism of behaviours*. In particular, if $M' = M$, then the elements of the D-endomorphism ring $\mathrm{end}_D(M)$ of M define internal transformations of $\ker_{\mathcal{F}}(R.)$, i.e., *Galois-like transformations*. We refer the reader to [6] for applications of the Galois transformations to the computation of quadratic conservation laws of linear systems of partial differential equations.

Moreover, in the next section, we shall see that the endomorphism ring $\mathrm{end}_D(M)$ allows us to factorize, reduce and decompose the left D-module M and its corresponding linear functional system $\ker_{\mathcal{F}}(R.)$.

3 Computations of D-morphisms

Let first study $\hom_D(M, M')$ when D is a commutative ring. As, in this particular case, $\hom_D(M, M')$ is a D-module, we can characterize this D-module by means of generators and relations.

Definition 2. The *Kronecker product* of $E \in D^{q\times p}$ and $F \in D^{r\times s}$ is the matrix defined by:

$$E \otimes F = \begin{pmatrix} E_{11}\, F & \dots & E_{1p}\, F \\ \vdots & & \vdots \\ E_{q1}\, F & \dots & E_{qp}\, F \end{pmatrix} \in D^{(q\, r)\times(p\, s)}.$$

Using the Kronecker product, we have the simple but useful lemma.

Lemma 1. *Let D be a commutative ring and $U \in D^{a\times b}$, $V \in D^{b\times c}$ and $W \in D^{c\times d}$. Then, we have*

$$U\, V\, W = (V_{1\bullet} \dots V_{b\bullet})\, (U^T \otimes W),$$

where $V_{i\bullet}$ denotes the i^{th} row of the matrix V.

With the notations of Proposition 1, we get:

$$\begin{cases} R\, P = R\, P\, I_{p'} = (P_{1\bullet} \dots P_{p\bullet})\, (R^T \otimes I_{p'}), \\ Q\, R' = I_q\, Q\, R' = (Q_{1\bullet} \dots Q_{q\bullet})\, (I_q \otimes R'). \end{cases}$$

Hence, the computation of the matrices $P \in D^{p\times p'}$ and $Q \in D^{q\times q'}$ satisfying (2) is reduced to the computation of a set of generators of the D-module:

$$\ker_D \left(. \begin{pmatrix} R^T \otimes I_{p'} \\ -I_q \otimes R' \end{pmatrix} \right) = \left\{ \lambda \in D^{1\times(p\, p' + q\, q')} \mid \lambda \begin{pmatrix} R^T \otimes I_{p'} \\ -I_q \otimes R' \end{pmatrix} = 0 \right\}. \quad (4)$$

If D is a *noetherian ring*, namely, if every ideal of D is finitely generated as a D-module, then the previous D-module is finitely generated and even finitely presented (see, e.g., [17]). In particular, when D is a commutative polynomial ring over a *computational field* k (e.g., $k = \mathbb{Q}, \mathbb{F}_p$) (see, e.g., [2, 13]), the kernel defined by (4) can be obtained by means of a Gröbner basis computation. For more details, see, e.g., [3, 4, 6, 13] and the references therein.

The complete algorithm for computing generators of $\hom_D(M, M')$ based on this method is given in [6, Algorithm 2.1]. The relations between these generators can be obtained using the method described in [6, Remark 2.3].

Example 1. We consider a fluid in a tank satisfying Saint-Venant's equations and subjected to a one-dimensional horizontal move ([9]):

$$\begin{cases} y_1(t-2\,h) + y_2(t) - 2\,\dot{u}(t-h) = 0, \\ y_1(t) + y_2(t-2\,h) - 2\,\dot{u}(t-h) = 0. \end{cases} \tag{5}$$

Let $D = \mathbb{Q}\,[\partial, \delta]$ be the commutative polynomial ring of differential time-delay operators with rational constant coefficients (i.e., $\partial f(t) = \dot{f}(t)$, $\delta f(t) = f(t-h)$), the system matrix of (5) defined by

$$R = \begin{pmatrix} \delta^2 & 1 & -2\,\partial\,\delta \\ 1 & \delta^2 & -2\,\partial\,\delta \end{pmatrix} \in D^{2\times 3}. \tag{6}$$

and the corresponding finitely presented D-module $M = D^{1\times 3}/(D^{1\times 2}\,R)$.

Applying the previous algorithm to the matrix R, we obtain that $\mathrm{end}_D(M)$ is generated by the D-endomorphisms f_{e_1}, f_{e_2}, f_{e_3} and f_{e_4} defined by $f_\alpha(\pi(\lambda)) = \pi(\lambda\, P_\alpha)$, for all $\lambda \in D^{1\times 3}$, where

$$P_\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & 2\,\alpha_3\,\partial\,\delta \\ \alpha_2 + 2\,\alpha_4\,\partial & \alpha_1 - 2\,\alpha_4\,\partial & 2\,\alpha_3\,\partial\,\delta \\ \alpha_4\,\delta & -\alpha_4\,\delta & \alpha_1 + \alpha_2 + \alpha_3\,(\delta^2+1) \end{pmatrix},$$

$$Q_\alpha = \begin{pmatrix} \alpha_1 - 2\,\alpha_4\,\partial & \alpha_2 + 2\,\alpha_4\,\partial \\ \alpha_2 & \alpha_1 \end{pmatrix},$$

$\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in D^{1\times 4}$ and $\{e_j\}_{j=1,\ldots,4}$ denotes the standard basis of $D^{1\times 4}$. We can check that the generators $\{f_{e_i}\}_{i=1,\ldots,4}$ of the D-module $\mathrm{end}_D(M)$ satisfy the following D-linear relations:

$$(\delta^2 - 1)\, f_{e_4} = 0, \quad \delta^2\, f_{e_1} + f_{e_2} - f_{e_3} = 0, \quad f_{e_1} + \delta^2\, f_{e_2} - f_{e_3} = 0. \tag{7}$$

Let us consider the D-module $\mathcal{F} = C^\infty(\mathbb{R})$ and the linear system $\ker_{\mathcal{F}}(R.) = \{\eta = (y_1, y_2, u)^T \in \mathcal{F}^3 \mid R\,\eta = 0\}$ defined by (5). Then, every $f_\alpha \in \mathrm{end}_D(M)$ defines the D-morphism $f_\alpha^\star : \ker_{\mathcal{F}}(R.) \longrightarrow \ker_{\mathcal{F}}(R.)$, $f_\alpha^\star(\eta) = P_\alpha\,\eta$, i.e., defines a Galois transformation of the differential time-delay system $\ker_{\mathcal{F}}(R.)$.

A complete description of the non-commutative ring $\mathrm{end}_D(M)$ is given by the knowledge of the expressions of the compositions $f_{e_i} \circ f_{e_j}$ in the family of generators $\{f_{e_k}\}_{k=1,\ldots,4}$ for $i, j = 1, \ldots, 4$:

$$\begin{cases} f_{e_1} \circ f_{e_i} = f_{e_i} \circ f_{e_1} = f_{e_i}, \\ f_{e_2} \circ f_{e_2} = f_{e_1}, \\ f_{e_2} \circ f_{e_3} = f_{e_3} \circ f_{e_2} = f_{e_3}, \\ f_{e_2} \circ f_{e_4} = 2\,\partial\, f_{e_1} - 2\,\partial\, f_{e_2} + f_{e_4}, \\ f_{e_4} \circ f_{e_2} = -f_{e_4}, \end{cases} \quad \begin{cases} f_{e_3} \circ f_{e_3} = (\delta^2+1)\, f_{e_3}, \\ f_{e_3} \circ f_{e_4} = 2\,\partial\, f_{e_1} - 2\,\partial\, f_{e_2} + 2\, f_{e_4}, \\ f_{e_4} \circ f_{e_3} = 0, \\ f_{e_4} \circ f_{e_4} = -2\,\partial\, f_{e_4}. \end{cases} \tag{8}$$

In other words, we get the following *multiplication table* where $f_{e_c} \circ f_{e_r}$ means that we compose an element in the first column by an element in the first row:

$f_{e_c} \circ f_{e_r}$	f_{e_1}	f_{e_2}	f_{e_3}	f_{e_4}
f_{e_1}	f_{e_1}	f_{e_2}	f_{e_3}	f_{e_4}
f_{e_2}	f_{e_2}	f_{e_1}	f_{e_3}	$2\,\partial\, f_{e_1} - 2\,\partial\, f_{e_2} + f_{e_4}$
f_{e_3}	f_{e_3}	f_{e_3}	$(\delta^2+1)\, f_{e_3}$	$2\,\partial\, f_{e_1} - 2\,\partial\, f_{e_2} + 2\, f_{e_4}$
f_{e_4}	f_{e_4}	$-f_{e_4}$	0	$-2\,\partial\, f_{e_4}$

If we denote by $D < f_{e_1}, f_{e_2}, f_{e_3}, f_{e_4} >$ the *free* D-*algebra* (i.e., the non-commutative polynomial ring with coefficients in D) defined by the f_{e_i}'s and

$$I =< (\delta^2-1)\, f_{e_4}, \delta^2\, f_{e_1} + f_{e_2} - f_{e_3}, f_{e_1} + \delta^2\, f_{e_2} - f_{e_3}, \ldots, f_{e_4} \circ f_{e_4} + 2\,\partial\, f_{e_4} >$$

the two-sided ideal of $D < f_{e_1}, f_{e_2}, f_{e_3}, f_{e_4} >$ generated by the polynomials obtained from the identities (7) and (8), then we get that:

$$\mathrm{end}_D(M) = D < f_{e_1}, f_{e_2}, f_{e_3}, f_{e_4} > /I.$$

The previous quotient of a non-commutative polynomial algebra can be studied by means of non-commutative Gröbner bases ([13]) as discussions with V. Levandovskyy (Aachen University) have recently demonstrated. This promising approach will be developed in the future.

When D is a non-commutative k-algebra, the computation of the abelian group $\hom_D(M, M')$ is more complicated and we can generally only compute the morphisms of $\hom_D(M, M')$ which are defined by means of a matrix P with a fixed total order in the functional operators ∂_i and a fixed degree in x_i for the numerators and denominators of the polynomial/rational coefficients. As this issue is not crucial for the rest of the paper, we shall not detail this point here and we refer to [6, Algorithm 2.2] for a complete algorithm computing morphisms in the non-commutative case. Note that we can easily study $\hom_D(M, M')$ when it is a finite-dimensional k-vector space and a k-basis of $\hom_D(M, M')$ is known (see [6, 16, 20] and references therein). In particular, it is the case when M and M' are two left *holonomic* modules over the ring $A_n(k)$ of differential operators with coefficients in $k[x_1, \ldots, x_n]$ or D-*finite* linear functional systems ([2, 16, 20]) such as, for instance, $B_n(k)$-*finite* linear systems, where $B_n(k)$ denotes the ring of differential operators with coefficients in $k(x_1, \ldots, x_n)$ (see [6, 16, 20] and references therein).

4 Factorization, reduction and decomposition problems

If $f \in \hom_D(M, M')$, then we can define the following left D-modules:

$$\begin{cases} \ker f = \{m \in M \mid f(m) = 0\}, \\ \mathrm{im}\, f = \{m' \in M' \mid \exists\, m \in M :\; m' = f(m)\}, \end{cases} \qquad \begin{cases} \mathrm{coim}\, f = M/\ker f \\ \mathrm{coker}\, f = M'/\mathrm{im}\, f. \end{cases}$$

We now give three main theorems of [6]. Each of them corresponds to one of the three problems given in Section 1.

Theorem 2 ([6] - Factorization problem). *Let us consider $R \in D^{q\times p}$, $M = D^{1\times p}/(D^{1\times q}\, R)$ and $f \in \mathrm{end}_D(M)$ defined by $P \in D^{p\times p}$ and $Q \in D^{q\times q}$ satisfying $R\,P = Q\,R$. Let $S \in D^{r\times p}$ and $T \in D^{r\times q}$ be two matrices such that:*

$$\ker_D\left(.\begin{pmatrix} P \\ R \end{pmatrix}\right) = D^{1\times r}\,(S \quad -T).$$

Then, we have the following inclusion of left D-modules $(D^{1\times q}\, R) \subseteq (D^{1\times r}\, S)$, which proves the existence of a factorization of the matrix R of the form

$$R = L\,S, \tag{9}$$

for a certain matrix $L \in D^{q\times r}$. In particular, if $\mathcal{F}$ is a left D-module, from (9), we then have $\ker_{\mathcal{F}}(S.) \subseteq \ker_{\mathcal{F}}(R.)$.

Moreover, we have:

1. $\ker f = (D^{1\times r}\, S)/(D^{1\times q}\, R)$. *Hence, f is injective iff there exists a matrix $F \in D^{r\times q}$ such that $S = F\,R$.*
2. $\mathrm{coim}\, f = D^{1\times p}/(D^{1\times r}\, S)$. *Hence, $f = 0$ iff the matrix S admits a left-inverse $X \in D^{p\times r}$, namely, $X\,S = I_p$.*
3. $\mathrm{im}\, f = (D^{1\times (p+q)}\,(P^T \quad R^T)^T)/(D^{1\times q}\, R)$.
4. $\mathrm{coker}\, f = D^{1\times p}/(D^{1\times (p+q)}\,(P^T \quad R^T)^T)$. *Hence, f is surjective iff the matrix $(P^T \quad R^T)^T$ admits a left-inverse $(X_1 \quad X_2) \in D^{p\times (p+q)}$, i.e., we have $X_1\,P + X_2\,R = I_p$.*

We refer the reader to [3] for constructive algorithms which factorize and compute left-inverses over certain classes of Ore algebras and their implementations in the library OreModules ([4]).

The second result gives conditions for the existence of a reduction of R.

Theorem 3 ([6] - Reduction problem). *Let us consider $R \in D^{q\times p}$, $M = D^{1\times p}/(D^{1\times q}\, R)$ and $f \in \mathrm{end}_D(M)$ defined by $P \in D^{p\times p}$ and $Q \in D^{q\times q}$ satisfying $R\,P = Q\,R$. If the left D-modules $\ker_D(.P)$, $\mathrm{coim}_D(.P)$, $\ker_D(.Q)$ and $\mathrm{coim}_D(.Q)$ are respectively free of rank m, $p-m$, l, $q-l$, then there exist matrices $U_1 \in D^{m\times p}$, $U_2 \in D^{(p-m)\times p}$, $V_1 \in D^{l\times q}$ and $V_2 \in D^{(q-l)\times q}$ such that $U = (U_1^T \quad U_2^T)^T \in \mathrm{GL}_p(D)$, $V = (V_1^T \quad V_2^T)^T \in \mathrm{GL}_q(D)$ and*

$$\overline{R} = V\,R\,U^{-1} = \begin{pmatrix} V_1\,R\,W_1 & 0 \\ V_2\,R\,W_1 & V_2\,R\,W_2 \end{pmatrix} \in D^{q\times p},$$

where $U^{-1} = (W_1 \quad W_2)$, $W_1 \in D^{p\times m}$ and $W_2 \in D^{p\times (p-m)}$.

In particular, the full row rank matrix U_1 (resp., U_2, V_1, V_2) defines a basis of the free D-module $\ker_D(.P)$ (resp., $\mathrm{coim}_D(.P)$, $\ker_D(.Q)$, $\mathrm{coim}_D(.Q)$), i.e.,

$$\begin{cases} \ker_D(.P) = D^{1\times m}\, U_1, \\ \mathrm{coim}_D(.P) = \kappa(D^{1\times (p-m)}\, U_2), \\ \ker_D(.Q) = D^{1\times l}\, V_1, \\ \mathrm{coim}_D(.Q) = \rho(D^{1\times (q-l)}\, V_2), \end{cases}$$

where $\kappa : D^{1\times p} \longrightarrow \mathrm{coim}_D(.P) = D^{1\times p}/\ker_D(.P)$ *denotes the canonical projection and similarly with* $\rho : D^{1\times q} \longrightarrow \mathrm{coim}_D(.Q) = D^{1\times q}/\ker_D(.Q)$.

The last result gives conditions for the existence of a decomposition of R.

Theorem 4 ([6] - Decomposition problem). *Let us consider* $R \in D^{q\times p}$, $M = D^{1\times p}/(D^{1\times q}\, R)$ *and* $f \in \mathrm{end}_D(M)$ *an idempotent endomorphism of* M *defined by two idempotent matrices* $P \in D^{p\times p}$ *and* $Q \in D^{q\times q}$, *namely, they satisfy* $R\,P = Q\,R$, $P^2 = P$ *and* $Q^2 = Q$. *If the left* D*-modules* $\ker_D(.P)$, $\mathrm{im}_D(.P) = \ker_D(.(I_p - P))$, $\ker_D(.Q)$ *and* $\mathrm{im}_D(.Q) = \ker_D(.(I_q - Q))$ *are respectively free of rank* m, $p-m$, l, $q-l$, *then there exist four matrices* $U_1 \in D^{m\times p}$, $U_2 \in D^{(p-m)\times p}$, $V_1 \in D^{l\times q}$ *and* $V_2 \in D^{(q-l)\times q}$ *such that*

$$U = (U_1^T \quad U_2^T)^T \in \mathrm{GL}_p(D), \quad V = (V_1^T \quad V_2^T)^T \in \mathrm{GL}_q(D),$$

and

$$\overline{R} = V\,R\,U^{-1} = \begin{pmatrix} V_1\,R\,W_1 & 0 \\ 0 & V_2\,R\,W_2 \end{pmatrix} \in D^{q\times p},$$

where $U^{-1} = (W_1 \quad W_2)$, $W_1 \in D^{p\times m}$ *and* $W_2 \in D^{p\times(p-m)}$.

In particular, the full row rank matrix U_1 *(resp.,* U_2, V_1, V_2*) defines a basis of the free* D*-module* $\ker_D(.P)$, *(resp.,* $\mathrm{im}_D(.P)$, $\ker_D(.Q)$, $\mathrm{im}_D(.Q)$*) of rank* m *(resp.,* $p-m$, l, $q-l$*). In other words, we have:*

$$\begin{cases} \ker_D(.P) = D^{1\times m}\,U_1, \\ \mathrm{im}_D(.P) = D^{1\times(p-m)}\,U_2, \\ \ker_D(.Q) = D^{1\times l}\,V_1, \\ \mathrm{im}_D(.Q) = D^{1\times(q-l)}\,V_2. \end{cases}$$

Finally, if $\mathcal{F}$ *is a left* D*-module, then we obtain the following decomposition of the linear functional system* $\ker_{\mathcal{F}}(R.)$*:*

$$\ker_{\mathcal{F}}(R.) \cong \ker_{\mathcal{F}}(V_1\,R\,W_1.) \oplus \ker_{\mathcal{F}}(V_2\,R\,W_2.).$$

Example 2. If we consider again Example 1, then we can check that the D-endomorphism $f = \frac{1}{2}\,(f_{e_1} + f_{e_2})$ is defined by the following matrices:

$$P = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad Q = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

The corresponding factorization of the matrix R defined by (6) is given by:

$$R = L\,S, \quad L = \begin{pmatrix} \delta^2 & 1 \\ 1 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & -1 & 0 \\ 0 & \delta^2 + 1 & -2\,\partial\,\delta \end{pmatrix}.$$

Moreover, as the entries of P and Q belong to the field $\mathbb{Q}$, using linear algebraic techniques, we can easily compute bases of the free D-modules $\ker_D(.P)$, $\mathrm{coim}_D(.P)$, $\ker_D(.Q)$ and $\mathrm{coim}_D(.Q)$ and we get:

$$U_1 = (1 \quad -1 \quad 0), \quad U_2 = \begin{pmatrix} 0 \; 1 \; 0 \\ 0 \; 0 \; 1 \end{pmatrix}, \quad V_1 = (1 \quad -1), \quad V_2 = (0 \quad 1).$$

Forming $U = (U_1^T \quad U_2^T)^T \in \mathrm{GL}_3(D)$ and $V = (V_1^T \quad V_2^T)^T \in \mathrm{GL}_2(D)$, we obtain the following reduction of the matrix R:

$$\overline{R} = V\, R\, U^{-1} = \begin{pmatrix} \delta^2 - 1 & 0 & 0 \\ 1 & \delta^2 + 1 & -2\,\partial\,\delta \end{pmatrix}.$$

Using (8), we can easily check that f is an idempotent of $\mathrm{end}_D(M)$ defined by two idempotent matrices P and Q, i.e., $P^2 = P$ and $Q^2 = Q$. By means of linear algebra, we can compute bases of the free D-modules $\mathrm{im}_D(.P) = \ker_D(.(I_3 - P))$ and $\mathrm{im}_D(.Q) = \ker_D(.(I_2 - Q))$ and we obtain:

$$X_2 = \begin{pmatrix} 1 \; 1 \; 0 \\ 0 \; 0 \; 1 \end{pmatrix}, \quad Y_2 = (1 \quad 1).$$

Forming $X = (U_1^T \quad X_2^T)^T \in \mathrm{GL}_3(D)$ and $Y = (V_1^T \quad Y_2^T)^T \in \mathrm{GL}_2(D)$, we finally obtain the following decomposition of the matrix R:

$$\overline{\overline{R}} = Y\, R\, X^{-1} = \begin{pmatrix} \delta^2 - 1 & 0 & 0 \\ 0 & \delta^2 + 1 & -4\,\partial\,\delta \end{pmatrix}.$$

We refer the reader to [6, 7] for more results and examples coming from control theory, mathematical physics and engineering sciences.

Conclusion

In this paper, we have recalled the main theoretical results of [5, 6] on the factorization, reduction and decomposition problems of linear functional systems. The theorems given in Section 4 have been implemented in the OreMorphisms package ([7]) and can be used to decompose the main linear differential time-delay systems appearing in the literature of control theory ([6, 7]). However theoretical difficult questions are still open on the way of getting a general algorithmic test which checks whether or not a finitely presented left D-module M is (completely) decomposable or simple. The algebraic structure of the endomorphism ring $\mathrm{end}_D(M)$ needs to be investigated in more details. In particular, the study of the *regular elements* of $\mathrm{end}_D(M)$ (namely, $f \in \mathrm{end}_D(M)$ such that there exists $g \in \mathrm{end}_D(M)$ satisfying $f \circ g \circ f = f$) and the idempotents of $\mathrm{end}_D(M)$ will be pursued in the future.

References

1. M. A. Barkatou, "On the reduction of matrix pseudo-linear equations", *Technical Report RR 1040*, Rapport de Recherche de l'Institut IMAG, 2001.
2. F. Chyzak, B. Salvy, "Non-commutative elimination in Ore algebras proves multivariate identities", *J. Symbolic Comput.*, 26 (1998), 187-227.
3. F. Chyzak, A. Quadrat, D. Robertz, "Effective algorithms for parametrizing linear control systems over Ore algebras", *Appl. Algebra Engrg. Comm. Comput.*, 16 (2005), 319-376.
4. F. Chyzak, A. Quadrat, D. Robertz, "OreModules: A symbolic package for the study of multidimensional linear systems", in the book *Applications of Time-Delay Systems*, J. Chiasson and J.-J. Loiseau (Eds.), Lecture Notes in Control and Inform. Sci. (LNCIS) 352, Springer, 233-264.
5. T. Cluzeau, A. Quadrat, "Using morphism computations for factoring and decomposing general linear functional systems", in the proceedings of *Mathematical Theory of Networks and Systems (MTNS)*, Kyoto (Japan), 20-24/07/06.
6. T. Cluzeau, A. Quadrat, "Factoring and decomposing a class of linear functional systems", *Linear Algebra Appl.*, 428 (2008), 324-381.
7. T. Cluzeau, A. Quadrat, "OreMorphisms: A homological algebraic package for factoring, reducing and decomposing linear functional systems", *Topics in Time-Delay Systems: Analysis, Algorithms and Control*, J.-J. Loiseau, W. Michiels, S.-I. Niculescu, R. Sipahi (Eds.), Lecture Notes in Control and Inform. Sci. (LNCIS), Springer (2008).
8. P. M. Cohn, *Free rings and their Relations*, LMS Monographs 19, Academic Press, 2^{nd} edition, 1985.
9. F. Dubois, N. Petit, P. Rouchon, "Motion planning and nonlinear simulations for a tank containing a fluid", in the proceedings of the *European Control Conference (ECC)*, Karlsruhe (Germany), 1999.
10. T. Kailath, *Linear Systems*, Englewood Cliffs: Prentice-Hall 1980.
11. M. Kashiwara, *Algebraic Study of Systems of Partial Differential Equations*, Master Thesis, Tokyo Univ. 1970, Mémoire de la Société Mathématiques de France 63 (1995) (English translation).
12. V. Kučera, *Discrete Linear Control*, Wiley, 1979.
13. V. Levandovskyy, *Non-commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation*, Ph.D. Thesis, University of Kaiserslautern (Germany), 2005.
14. B. Malgrange, "Systèmes à coefficients constants", *Séminaire Bourbaki*, 1962/1963, 1-11.
15. J. C. McConnell, J. C. Robson, *Noncommutative Noetherian Rings*, American Mathematical Society, 2000.
16. M. van der Put, M. F. Singer, *Galois theory of linear differential equations*, Grundlehren der mathematischen Wissenschaften, 328, Springer, 2003.
17. J. J. Rotman, *An Introduction to Homological Algebra*, Academic Press, 1979.
18. H. H. Rosenbrock, *State Space and Multivariable Theory*, Wiley, 1970.
19. M. F. Singer, "Testing reducibility of linear differential operators: a group theoretic perspective", *Appl. Algebra Engrg. Comm. Comput.*, 7 (1996), 77-104.
20. M. Wu, *On Solutions of Linear Functional Systems and Factorization of Modules over Laurent-Ore Algebras*, PhD thesis of the Chinese Academy of Sciences (China) and the University of Nice-Sophia Antipolis (France), 2005.