ARTICLE IN PRESS

Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Symbolic Computation ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Computation of bases of free modules over the Weyl algebras

Alban Quadrat[a,*], Daniel Robertz[b]

[a] *INRIA Sophia Antipolis, APICS project, 2004 Route des Lucioles BP 93, 06902 Sophia Antipolis Cedex, France*
[b] *Lehrstuhl B für Mathematik, RWTH - Aachen, Templergraben 64, 52056 Aachen, Germany*

Received 15 February 2007; accepted 10 June 2007

Abstract

A well-known result due to J.T. Stafford asserts that a stably free left module M over the Weyl algebras $D = A_n(k)$ or $B_n(k)$ – where k is a field of characteristic 0 – with $\text{rank}_D(M) \geq 2$ is free. The purpose of this paper is to present a new constructive proof of this result as well as an effective algorithm for the computation of bases of M. This algorithm, based on the new constructive proofs [Hillebrand, A., Schmale, W., 2001. Towards an effective version of a theorem of Stafford. J. Symbolic Comput. 32, 699–716; Leykin, A., 2004. Algorithmic proofs of two theorems of Stafford. J. Symbolic Comput. 38, 1535–1550] of J.T. Stafford's result on the number of generators of left ideals of D, performs Gaussian elimination on the formal adjoint of the presentation matrix of M. We show that J.T. Stafford's result is a particular case of a more general one asserting that a stably free left D-module M with $\text{rank}_D(M) \geq \text{sr}(D)$ is free, where $\text{sr}(D)$ denotes the stable rank of a ring D. This result is constructive if the stability of unimodular vectors with entries in D can be tested. Finally, an algorithm which computes the left projective dimension of a general left D-module M defined by means of a finite free resolution is presented. It allows us to check whether or not the left D-module M is stably free.

Keywords: Stably free modules; Free modules; Computation of bases; Projective dimension; Stafford's results; Monge problem; Flat multidimensional linear systems; Weyl algebras

1. Introduction

A famous result in non-commutative algebra, due to J.T. Stafford, states that any left ideal of the Weyl algebras $D = A_n(k)$ or $B_n(k)$ of partial differential operators in $\partial_1 = \partial/\partial x_1, \ldots,$

* Corresponding author. Tel.: +33 4 92 38 76 42; fax: +33 4 92 38 78 58.
E-mail addresses: Alban.Quadrat@sophia.inria.fr (A. Quadrat), daniel@momo.math.rwth-aachen.de (D. Robertz).

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2007.06.005

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

$\partial_n = \partial/\partial x_n$ with coefficients in $k[x_1, \ldots, x_n]$ or $k(x_1, \ldots, x_n)$, where k is a field of characteristic 0, is generated by two elements of D. See Stafford (1978) for more details. Two constructive proofs of this result recently appeared in the literature of symbolic computation (Hillebrand and Schmale, 2001; Leykin, 2004). A well-known consequence of J.T. Stafford's result is that every stably free left D-module M (cf. Definition 2) with $\mathrm{rank}_D(M) \geq 2$ is free (Stafford, 1978). As noticed in Gago-Vargas (2003), the recent results of Hillebrand and Schmale (2001), Leykin (2004) now allow us to pay more attention to constructive versions of this last result, i.e., to the computation of bases of stably free left D-modules which are not isomorphic to left ideals of D. In particular, following the non-constructive proof given by J.T. Stafford, an algorithm has been obtained in Gago-Vargas (2003). However, we feel that this algorithm is rather involved and the purpose of this paper is to give a simple algorithm which is essentially nothing but the Gaussian elimination performed on the formal adjoint of a *minimal presentation matrix* of the stably free left D-module M. By minimal presentation matrix of a stably free left D-module M, we mean a matrix $R \in D^{q\times p}$ which admits a right-inverse $S \in D^{p\times q}$, i.e. $R\,S = I_q$, and satisfies $M \cong D^{1\times p}/(D^{1\times q}\,R)$, where $D^{1\times p}$ denotes the left D-module formed by the row vectors of length p with entries in D. Simplifying a result of Gago-Vargas (2003), we give an algorithm which computes such a minimal presentation matrix of a left D-module M defined by means of a finite free resolution. In particular, this algorithm allows us to compute the left projective dimension of any left D-module M defined by a finite free resolution. Implementations of all these algorithms have recently been realized in the package STAFFORD (Quadrat and Robertz, 2005–2007) based on the OREMODULES library (Chyzak et al., 2007). See also Chyzak et al. (2005) for more details and examples. Hence, using the fact that we can also constructively check whether or not a stably free ideal is principal, i.e., free, this implementation allows us to compute bases of free left D-modules.

More generally, it is known that a stably free left module M over a ring D with $\mathrm{rank}_D(M) \geq \mathrm{sr}(D)$ is free, where $\mathrm{sr}(D)$ denotes the *stable rank* of D (see Definition 33). We present a general algorithm which computes bases of free left D-modules. This algorithm was inspired by a result of Lombardi (2005) obtained for commutative rings. If the stability of unimodular vectors with entries in D (cf. Definition 33) can be effectively checked, then the algorithm becomes constructive. We note that J.T. Stafford's result on the number of generators of left ideals of the Weyl algebras (Stafford, 1978) shows that $\mathrm{sr}(A_n(k)) = 2$ and $\mathrm{sr}(B_n(k)) = 2$, where k is a field of characteristic 0.

We have recently given in Chyzak et al. (2005) some constructive algorithms which check whether or not finitely presented left modules over some classes of Ore algebras have some torsion elements or are torsion-free, reflexive or projective (cf. Definition 2). These algorithms have been implemented in OREMODULES (Chyzak et al., 2007). In systems theory, this previous classification of modules allows us to check whether or not an underdetermined linear system over an Ore algebra of functional operators is parametrizable, admits a parametrization which is also parametrizable or admits a chain of n successive parametrizations. These results have some applications in mathematical physics where it is interesting to know whether some field equations derive from some potentials, and in control theory where this problem is also called the image representation problem of behaviours (Chyzak et al., 2005; Polderman and Willems, 1998; Pommaret, 2001; Pommaret and Quadrat, 1998, 2004; Wood, 2000; Zerz, 2006). However, apart from some special situations, we were not able to give in Chyzak et al. (2005) and Pommaret and Quadrat (1998, 1999a) constructive algorithms which check whether or not a finitely presented left module over an Ore algebra is stably free or free. Hence, the results obtained in this paper allow us to extend the previous classification of linear systems over Ore algebras in terms of the algebraic properties of the associated module. In particular, we shall illustrate the interpretation of freeness and stably freeness in the system-theoretic language. The concept of a flat linear system over an Ore algebra developed in the literature (Fliess et al., 1995; Mounier, 1995; Pommaret, 2001; Pommaret and Quadrat, 1998) corresponds to the fact that the module associated with the system is free (Chyzak et al., 2005). A basis of the module then corresponds to a so-called *flat output* of the system. Hence, the algorithms presented in this paper allow us to compute flat outputs of some classes of multidimensional linear systems over Ore algebras.

The problem of recognizing whether or not an underdetermined (linear) system of partial differential equations (PDEs) can be (injectively) parametrized by means of arbitrary functions constitutes the so-called *Monge problem*, which was particularly studied by J. Hadamard and E. Goursat. We refer the reader to Hadamard (1901), Goursat (1930), Zervos (1932) and Janet (1971) for more historical details and for the main contributions of G. Darboux, D. Hilbert and E. Cartan in the case of nonlinear systems of ordinary differential equations. Hence, combining the results developed in this paper with the ones given in Chyzak et al. (2005) and Pommaret and Quadrat (1998, 1999a) gives constructive solutions to the Monge problem for the case of linear systems of PDEs with polynomial or rational coefficients. To finish, we quote the last paragraph of E. Goursat's introduction of his paper (Goursat, 1930): "Ces résultats sont encore bien particuliers. J'espère cependant qu'ils pourront contribuer à appeler l'attention de quelques jeunes mathématiciens sur un sujet difficile et bien peu étudié" ("These results are still particular. However I hope they can contribute to drawing some young mathematicians' attention to a difficult subject which has not been thoroughly studied so far"). We hope that this paper will contribute to attracting more attention to this challenging problem.

The plan of the paper is the following. In Section 2, we recall some useful notations, definitions and results on the duality between systems and modules. In particular, we give general characterizations of stably free and free modules which will be useful in the rest of the paper, and their system-theoretic interpretations. In Section 3, we give an algorithm which computes the left projective dimension of a left D-module. This algorithm is then used to compute a minimal presentation matrix of a stably free module. Finally, the problem of the constructive computation of bases of free modules is studied in Section 4 and a general algorithm is presented. We show how this algorithm can be made effective using the recent results of Hillebrand and Schmale (2001) and Leykin (2004).

2. A module-theoretic classification of linear systems

Let us consider a non-commutative ring D, a left D-module $\mathcal{F}$ and a $q \times p$ matrix R with entries in D, i.e., $R \in D^{q \times p}$. Then, we can define the *system* or *behaviour* (Oberst, 1990; Polderman and Willems, 1998; Pommaret and Quadrat, 2003; Wood, 2000)

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

which is naturally associated with the *finitely presented* left D-module (Rotman, 1979):

$$M = D^{1\times p}/(D^{1\times q}\,R).$$

Indeed, we recall that if we apply the contravariant left exact functor $\hom_D(\cdot, \mathcal{F})$ to the following *finite presentation* of M

$$\begin{array}{ccccccc} D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{\pi} & M & \longrightarrow & 0, \\ \lambda = (\lambda_1, \ldots, \lambda_q) & \longmapsto & \lambda\,R & & & & \end{array} \tag{1}$$

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

namely, (1) is an *exact sequence* and π denotes the canonical projection onto M sending elements of $D^{1\times p}$ to their residue classes in M, we then obtain the exact sequence

$$\begin{array}{cccl} \mathcal{F}^q & \xleftarrow{R.} & \mathcal{F}^p & \longleftarrow \hom_D(M,\mathcal{F}) \longleftarrow 0, \\ R\,\eta & \longleftarrow & \eta = (\eta_1,\ldots,\eta_p)^T & \end{array}$$

where $\hom_D(M,\mathcal{F})$ denotes the abelian group of left D-morphisms from M to $\mathcal{F}$. For more details, see, e.g., Lam (1999) and Rotman (1979). This implies the following important isomorphism of abelian groups (Malgrange, 1962):

$$\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\} \cong \hom_D(M,\mathcal{F}). \tag{2}$$

See Chyzak et al. (2005), Oberst (1990), Pommaret and Quadrat (2003), Wood (2000) and the references therein for more details. In particular, (2) gives an intrinsic characterization of the $\mathcal{F}$-solutions of a linear system over D. It only depends on two objects:

(1) The finitely presented left D-module M representing the equations of the system.
(2) The left D-module $\mathcal{F}$ which is the functional space in which we seek the solutions.

If D is now a ring of functional operators (e.g., differential operators, time-delay operators, difference operators), then the issue of understanding which functional space $\mathcal{F}$ is suitable for a particular linear system has been studied for a long time in functional analysis and still is a very active subject. It does not seem that constructive algebra and symbolic computation can propose new methods for handling this functional analysis problem. However, they are useful for classifying $\hom_D(M,\mathcal{F})$ by means of the algebraic properties of M. Indeed, a large classification of the properties of modules is developed in homological algebra. See, e.g., Lam (1999) and Rotman (1979). Before recalling a part of the standard classification, let us introduce the concept of an *Ore ring*.

Definition 1 (*McConnell and Robson, 2000*). A ring D is said to be a *left Ore ring* if, for all $a_1, a_2 \in D \setminus \{0\}$, there exist $b_1, b_2 \in D \setminus \{0\}$ such that $b_1\,a_1 = b_2\,a_2$.

We now recall a few definitions. See, e.g., Lam (1999), McConnell and Robson (2000) and Rotman (1979).

Definition 2. Let D be a domain which is a left Ore ring and M a finitely generated left D-module. Then, we have:

(1) M is *free* if it is isomorphic to $D^{1\times r}$ for a certain $r \in \mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$.
(2) M is *stably free* if there exist $r, s \in \mathbb{Z}_{\geq 0}$ such that we have $M \oplus D^{1\times s} \cong D^{1\times r}$.
(3) M is *projective* if there exist a left D-module N and $r \in \mathbb{Z}_{\geq 0}$ such that

$$M \oplus N \cong D^{1\times r}.$$

(4) M is *reflexive* if the canonical map defined by

$$\varepsilon_M : M \longrightarrow \hom_D(\hom_D(M,D),D), \quad \varepsilon_M(m)(f) = f(m),$$

for all $m \in M$ and for all $f \in \hom_D(M,D)$, is an isomorphism, where $\hom_D(M,D)$ denotes the right D-module of all D-morphisms from M to D.
(5) M is *torsion-free* if the left submodule of M defined by

$$t(M) = \{m \in M \mid \exists\, 0 \neq P \in D : \; P\,m = 0\}$$

is the zero module. $t(M)$ is called the *torsion submodule* of M and the elements of $t(M)$ are the *torsion elements* of M.
(6) M is *torsion* if $t(M) = M$, i.e., every element of M is a torsion element.

Constructive algorithms which check whether or not a finitely presented left module M over certain classes of *Ore algebras* (see Definition 4) is respectively torsion-free, reflexive or projective were given in Chyzak et al. (2005) and Pommaret and Quadrat (1999a). These algorithms have been implemented in the library OREMODULES (Chyzak et al., 2007).

With a little abuse of language, we say that a behaviour $\mathcal{B} = \ker_{\mathcal{F}}(R.)$ is *torsion-free* (resp., *reflexive, projective, stably free, free*) if the finitely presented left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$ is torsion-free (resp., reflexive, projective, stably free, free).

Let us recall some important results concerning the notions given in Definition 2.

Theorem 3. (1) *(Rotman, 1979) Let D be a domain which is a left Ore ring and M a finitely generated left D-module. Then, we have the following implications among the above concepts:*

$$\textit{free} \Rightarrow \textit{stably free} \Rightarrow \textit{projective} \Rightarrow \textit{reflexive} \Rightarrow \textit{torsion-free}.$$

(2) *(McConnell and Robson, 2000; Rotman, 1979) If D is a* left hereditary ring *– namely, every left ideal of D is a projective left D-module – then every finitely generated torsion-free left D-module is projective.*

(3) *If D is a* left principal ideal domain *– namely, every left ideal of D is principal – then every finitely generated torsion-free left D-module is free.*

(4) *(Rotman, 1979, Theorem 4.59) (Quillen–Suslin theorem) Every projective module over a commutative polynomial ring with coefficients in a field is free.*

See also Lam (1999). We refer the reader to Fabiańska and Quadrat (2007) for an implementation of the Quillen–Suslin theorem and its applications to systems theory.

We define the concept of an Ore algebra which will play an important role.

Definition 4. (1) (McConnell and Robson, 2000) Let A be a domain with a unit 1 which is also a k-algebra, where k is a field. The *skew polynomial ring* $A[\partial;\sigma,\delta]$ is the non-commutative ring consisting of all polynomials in ∂ with coefficients in A obeying the commutation rule

$$\forall a \in A, \quad \partial\, a = \sigma(a)\,\partial + \delta(a), \tag{3}$$

where σ is a *k-algebra endomorphism of A*, namely, $\sigma : A \to A$ satisfies

$$\forall a,\, b \in A, \quad \sigma(1) = 1, \quad \sigma(a+b) = \sigma(a) + \sigma(b), \quad \sigma(a\,b) = \sigma(a)\,\sigma(b),$$

and δ is a *σ-derivation of A*, namely, $\delta : A \to A$ satisfies

$$\forall a,\, b \in A, \quad \delta(a+b) = \delta(a) + \delta(b), \quad \delta(a\,b) = \sigma(a)\,\delta(b) + \delta(a)\,b.$$

(2) (Chyzak and Salvy, 1998; McConnell and Robson, 2000) Let $A = k[x_1,\ldots,x_n]$ be a commutative polynomial ring over a field k (if $n = 0$ then $A = k$). Then, the iterated skew polynomial ring $D = A[\partial_1;\sigma_1,\delta_1]\ldots[\partial_m;\sigma_m,\delta_m]$ is called an *Ore algebra* if the σ_i's and δ_j's commute for $1 \le i,\, j \le m$ and satisfy the following conditions:

$$\forall j < i, \quad \sigma_i(\partial_j) = \partial_j, \quad \delta_i(\partial_j) = 0.$$

We note that $A[\partial;\mathrm{id}_A,0]$ is the commutative polynomial ring in ∂ with coefficients in A. Let us give some important examples of *Ore algebras* and related algebras.

Example 5. (1) The *Weyl algebra* $A_n(k)$ is the Ore algebra defined by

$$A_n(k) = k[x_1,\ldots,x_n][\partial_1;\sigma_1,\delta_1]\ldots[\partial_n;\sigma_n,\delta_n], \quad \sigma_i = \mathrm{id}_{k[x_1,\ldots,x_n]}, \quad \delta_i = \frac{\partial}{\partial x_i},$$

$i = 1, \ldots, n$, where k denotes a field. Equivalently, $A_n(k)$ can be defined as the non-commutative polynomial ring in the $2\,n$ variables x_i and ∂_j, $1 \leq i, j \leq n$, with coefficients in k, satisfying the following commutation relations:

$$x_i\, x_j = x_j\, x_i, \quad \partial_i\, \partial_j = \partial_j\, \partial_i, \quad \partial_i\, x_j = x_j\, \partial_i + \delta_{ij}, \quad 1 \leq i, j \leq n,$$

where δ_{ij} is defined by $\delta_{ij} = 1$ if $i = j$ and 0 otherwise.

In what follows, we shall use the notation $A_1(k) = k[t]\left[\frac{\mathrm{d}}{\mathrm{d}t}; \mathrm{id}_{k[t]}, \frac{\mathrm{d}}{\mathrm{d}t}\right]$. If k is a field of characteristic 0, then we can prove that $A_1(k)$ is a left hereditary ring (McConnell and Robson, 2000, Proposition 7.5.8).

By extension, we can define the k-algebra

$$B_n(k) = k(x_1, \ldots, x_n)[\partial_1; \sigma_1, \delta_1] \ldots [\partial_n; \sigma_n, \delta_n]$$

of differential operators with rational coefficients, where σ_i and δ_i are defined as previously. $B_1(k)$ is a left principal ideal domain (McConnell and Robson, 2000, Theorem 1.3.9 (ii)).

(2) The Ore algebra of differential time-delay operators with polynomial coefficients is defined by $A_1(k)[\partial_2; \sigma_2, \delta_2]$, where $\delta_2 = 0$ and $\sigma_2(a(t)) = a(t-1)$ for all $a \in k[t]$ and $\sigma_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) = \frac{\mathrm{d}}{\mathrm{d}t}$.

Similarly, we can define the k-algebra $B_1(k)[\partial_2; \sigma_2, \delta_2]$ with the same σ_2 and δ_2.

(3) The Ore algebra of shift operators with polynomial coefficients is defined by

$$k[x_1, \ldots, x_n][\partial_1; \sigma_1, \delta_1] \ldots [\partial_n; \sigma_n, \delta_n], \quad \delta_i = 0, \quad i = 1, \ldots, n,$$

and, $\forall a \in k[x_1, \ldots, x_n]$, $\sigma_i(a(x_1, \ldots, x_n)) = a(x_1, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_n)$.

Similarly, we can define the k-algebra $k(x_1, \ldots, x_n)[\partial_1; \sigma_1, \delta_1] \ldots [\partial_n; \sigma_n, \delta_n]$ with the same σ_i and δ_i as were defined before.

See Chyzak and Salvy (1998), Levandovskyy (2005) and the references therein for other algebras of functional operators.

Remark 6. Let k be a field, $A = k[x_1, \ldots, x_n]$ the commutative polynomial ring and $D = A[\partial_1; \sigma_1, \delta_1] \ldots [\partial_m; \sigma_m, \delta_m]$ an Ore algebra. Then

$$B = \{x_1^{i_1} \cdots x_n^{i_n}\, \partial_1^{j_1} \cdots \partial_m^{j_m} \mid (i_1, \ldots, i_n) \in (\mathbb{Z}_{\geq 0})^n, (j_1, \ldots, j_m) \in (\mathbb{Z}_{\geq 0})^m\} \tag{4}$$

is a k-vector space basis of D.

The next proposition allows us to effectively work in certain classes of Ore algebras.

Proposition 7 (*Kredel, 1993; Chyzak and Salvy, 1998*). *Let k be a computable field (e.g., $k = \mathbb{Q}$, $\mathbb{F}_p$), $A = k[x_1, \ldots, x_n]$ the polynomial ring with n indeterminates over the field k and $A[\partial_1; \sigma_1, \delta_1] \ldots [\partial_m; \sigma_m, \delta_m]$ an Ore algebra satisfying the conditions*

$$\sigma_i(x_j) = a_{ij}\, x_j + b_{ij}, \quad \delta_i(x_j) = c_{ij}, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n, \tag{5}$$

for certain $a_{ij} \in k \setminus \{0\}$, $b_{ij} \in k$, $c_{ij} \in A$. Let $\prec$ be an admissible term order, i.e., a total order on the set B of terms given in (4) with 1 as least element and such that $t\,u \prec t\,v$ for all $t \in B$ whenever $u \prec v$ for $u, v \in B$. If the $\prec$-greatest term u in each non-zero c_{ij} satisfies $u \prec x_j\,\partial_i$, then a non-commutative version of Buchberger's algorithm terminates for this admissible term order and its result is a Gröbner basis with respect to this order.

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

See also Levandovskyy (2005) and the references therein for more results. For more historical details concerning Buchberger's algorithm, we refer the reader to Buchberger (2006). See also Janet (1929) for the development of Janet bases in the study of PDEs.

Proposition 7 holds for the Ore algebras defined in Example 5. Moreover, we can prove that the Ore algebras satisfying the hypotheses of Proposition 7 are *left/right noetherian domains*, namely, rings over which every left/right ideal is finitely generated as a left/right module. In particular, this condition implies that D is a left/right Ore domain and has *invariant basis number* (IBN), namely, the property that two bases of a finitely generated free left/right D-module F have the same cardinality (Lam, 1999; McConnell and Robson, 2000). We call this cardinality the *rank* of the free left/right D-module F and denote it by $\mathrm{rank}_D(F)$.

We recall the concept of an *involution* (see, e.g., Lam (1999)).

Definition 8. (1) An *involution* of D is a k-linear map $\theta : D \longrightarrow D$ satisfying:

(a) $\forall P_1,\ P_2 \in D$: $\theta(P_1\, P_2) = \theta(P_2)\,\theta(P_1)$.

(b) $\theta \circ \theta = \mathrm{id}_D$.

(2) If $R \in D^{q\times p}$, then we define $\theta(R) = (\theta(R_{ij}))^T \in D^{p\times q}$.

Let us give some involutions of the Ore algebras defined in Example 5.

Example 9. (1) If D is a commutative k-algebra, then $\theta = \mathrm{id}_D$ is an involution.

(2) If $D = A_n(k)$ or $B_n(k)$, then we can define the following involution:

$$\theta(\partial_i) = -\partial_i, \quad \theta(x_i) = x_i, \quad i = 1, \ldots, n, \quad \forall a \in k, \quad \theta(a) = a.$$

(3) If D is the Ore algebra of differential time-delay operators defined in (2) of Example 5, then an involution θ of D is defined by

$$\theta\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) = \frac{\mathrm{d}}{\mathrm{d}t}, \quad \theta(\partial_2) = \partial_2, \quad \theta(t) = -t, \quad \forall a \in k, \quad \theta(a) = a.$$

(4) If D is the Ore algebra of shift operators defined in (3) of Example 5, then an involution θ of D is defined by

$$\theta(\partial_i) = \partial_i, \quad \theta(x_i) = -x_i, \quad i = 1, \ldots, n, \quad \forall a \in k, \quad \theta(a) = a.$$

See Chyzak et al. (2005), Levandovskyy (2005) for more details. If $D = A_n(k)$ or $B_n(k)$, θ is the involution defined in (2) of Example 9 and $R \in D^{q\times p}$, then $\theta(R) \in D^{p\times q}$ is usually called the *formal adjoint* of R (see Pommaret and Quadrat (1998)). In what follows, when the involution θ of D is clearly defined, we shall also denote $\theta(R)$ by $\widetilde{R}$.

We are now in position to state some interesting results.

Theorem 10 (*Chyzak et al., 2005; Pommaret and Quadrat, 1999a*). *Let D be an Ore algebra which satisfies the hypotheses of Proposition 7 and admits an involution θ. Let us suppose that the global dimension $n = \mathrm{gld}(D)$ of D is finite (see Section 3), $M = D^{1\times p}/(D^{1\times q}\, R)$ the left D-module finitely presented by R and $\widetilde{N} = D^{1\times q}/(D^{1\times p}\,\theta(R))$ the left D-module finitely presented by $\theta(R)$. Then, we have:*

(1) $t(M) \cong \mathrm{ext}^1_D(\widetilde{N}, D)$.

(2) *M is torsion-free iff* $\mathrm{ext}^1_D(\widetilde{N}, D) = 0$.

(3) *M is reflexive iff* $\mathrm{ext}^i_D(\widetilde{N}, D) = 0$ *for* $i = 1, 2$.

(4) *M is projective iff* $\mathrm{ext}^i_D(\widetilde{N}, D) = 0$ *for* $i = 1, \ldots, n$.

We refer the reader to Rotman (1979) for the definition of the extension modules $\mathrm{ext}^i_D(\widetilde{N}, D)$. Algorithms for computing $\mathrm{ext}^i_D(\widetilde{N}, D)$ are given in Chyzak et al. (2005) and they have been implemented in OREMODULES (Chyzak et al., 2007). See also Levandovskyy (2005). Hence, we can constructively check whether or not the left D-module M admits torsion elements or is torsion-free, reflexive or projective. See Chyzak et al. (2005, 2007) for explicit examples coming from mathematical physics and control theory.

Let us introduce a few more definitions (see, e.g., Lam (1999), Rotman (1979)).

Definition 11. (1) A left D-module $\mathcal{F}$ is called *injective* if the left exact contravariant functor $\hom_D(\cdot\,, \mathcal{F})$ transforms exact sequences of left D-modules into exact sequences of abelian groups.
(2) A left D-module $\mathcal{F}$ is called *cogenerator* if $\hom_D(M, \mathcal{F}) = 0$ implies that $M = 0$.

We can prove that an injective cogenerator left D-module $\mathcal{F}$ exists for every ring D (Rotman, 1979). The reader only needs to keep in mind the following explicit examples.

Example 12. (1) If Ω is an open convex subset of $\mathbb{R}^n$, then the space $C^\infty(\Omega)$ (resp., $\mathcal{D}'(\Omega)$) of smooth functions (resp., distributions) on Ω is an injective cogenerator module over the ring $k[\partial_1; \sigma_1, \delta_1] \ldots [\partial_n; \sigma_n, \delta_n]$ of differential operators with coefficients in $k = \mathbb{R}$ or $\mathbb{C}$ (Malgrange, 1962; Oberst, 1990).
(2) (Zerz, 2006) If $\mathcal{F}$ denotes the set of all functions that are smooth on $\mathbb{R}$ except for a finite number of points, then $\mathcal{F}$ is an injective cogenerator left $B_1(\mathbb{R})$-module.

We have the following interpretation of the classification of modules given in Definition 2 in terms of parametrizability of the behaviour $\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\}$.

Theorem 13 (*Chyzak et al., 2005; Pommaret and Quadrat, 1999a*). *Let D be an Ore algebra which satisfies the hypotheses of Theorem 10 and $\mathcal{F}$ an injective cogenerator left D-module. Let us set $q_1 = p$. Then, we have the following results:*

(1) *There exists $Q_1 \in D^{q_1 \times q_2}$ such that we have the exact sequence*

$$\mathcal{F}^q \xleftarrow{R.} \mathcal{F}^{q_1} \xleftarrow{Q_1.} \mathcal{F}^{q_2},$$

iff the left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$ is torsion-free.
(2) *There exist $Q_1 \in D^{q_1 \times q_2}$ and $Q_2 \in D^{q_2 \times q_3}$ such that we have the exact sequence*

$$\mathcal{F}^q \xleftarrow{R.} \mathcal{F}^{q_1} \xleftarrow{Q_1.} \mathcal{F}^{q_2} \xleftarrow{Q_2.} \mathcal{F}^{q_3},$$

iff the left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$ is reflexive.
(3) *There exists a chain of n successive parametrizations of* $\ker_{\mathcal{F}}(R.)$, *i.e., there exist $Q_i \in D^{q_i \times q_{i+1}}$, for $i = 1, \ldots, n$, such that we have the exact sequence*

$$\mathcal{F}^q \xleftarrow{R.} \mathcal{F}^{q_1} \xleftarrow{Q_1.} \mathcal{F}^{q_2} \xleftarrow{Q_2.} \mathcal{F}^{q_3} \xleftarrow{Q_3.} \cdots \xleftarrow{Q_{n-1}.} \mathcal{F}^{q_n} \xleftarrow{Q_n.} \mathcal{F}^{q_{n+1}}, \tag{6}$$

iff the left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$ is projective.

We note that the constructive verification of the vanishing of the $\mathrm{ext}^i_D(\widetilde{N}, D)$ allows us to explicitly compute the matrices Q_i as shown in Chyzak et al. (2005), Pommaret and Quadrat (1999a). Therefore, over a large class of algebras of functional operators, which are useful in engineering sciences, the previous results give us a constructive way to compute parametrizations of underdetermined linear systems (Chyzak et al., 2005; Pommaret and Quadrat, 1998).

See Chyzak et al. (2007, 2005), Pommaret and Quadrat (1998, 1999b,a, 2003) and Quadrat and Robertz (2005) for applications of these results in control theory and mathematical physics.

We point out that if $\mathcal{F}$ is any left D-module, then the exact sequences given in Theorem 13 will generally only be complexes, whereas they are exact if $\mathcal{F}$ is an injective left D-module and M is respectively a torsion-free, reflexive or projective left D-module. For instance, if $\mathcal{F}$ is not an injective left D-module but M is a torsion-free left D-module, then we have that $Q_1\,\mathcal{F}^{q_2} \subseteq \ker_{\mathcal{F}}(R.)$, i.e., we can generate a family of $\mathcal{F}$-solutions of the system $R\,\eta = 0$, which is sometimes enough for the applications in engineering sciences.

Finally, if $M = D^{1\times p}/(D^{1\times q}\,R)$ is a projective left D-module, where D satisfies the hypotheses of Theorem 13, then (6) is always an exact sequence without any assumption about the left D-module $\mathcal{F}$. This result follows from the fact that the left exact contravariant functor $\hom_D(\cdot, \mathcal{F})$ transforms long *split exact sequences* of left D-modules into long split exact sequences of abelian groups (see, e.g., Rotman (1979)).

The papers Chyzak et al. (2005) and Pommaret and Quadrat (1998, 1999a) have mainly left open the question of recognizing whether a finitely presented left module M over an Ore algebra is stably free or free. The purpose of this paper is to give some general answers to these questions. In particular, an algorithm for the computation of bases of free modules over some algebras will be presented in Section 4.

Let us state a useful result concerning the relationship between projective and stably free modules first due to J.-P. Serre for commutative rings.

Proposition 14 (*McConnell and Robson, 2000, Proposition 11.1.6*). *Let D be a non-commutative ring having invariant basis number. Then, a finitely generated projective left D-module M is stably free iff M admits a finite free resolution.*

We also have the following interesting proposition.

Proposition 15 (*McConnell and Robson, 2000, Corollary 12.3.3*). *If*

$$D = A[\partial_1; \sigma_1, \delta_1] \ldots [\partial_m; \sigma_m, \delta_m]$$

is an Ore algebra where σ_i is an automorphism for $i = 1, \ldots, m$, then every finitely generated projective left D-module is stably free.

In particular, Proposition 15 holds for the class of Ore algebras defined in Proposition 7. Hence, the verification of the vanishing of $\mathrm{ext}^i_D(\widetilde{N}, D)$, for $i = 1, \ldots, n$, checks whether or not a finitely presented left D-module M is stably free when D satisfies the hypotheses given in Proposition 7.

We have the following straightforward lemma characterizing stably free modules.

Lemma 16 (*McConnell and Robson, 2000, Proposition 11.1.7*). *A left D-module M is stably free iff there exists a matrix $R \in D^{q\times p}$ which admits a right-inverse $S \in D^{p\times q}$, i.e., $R\,S = I_q$, and satisfies $M \cong D^{1\times p}/(D^{1\times q}\,R)$.*

Let us now give a characterization of free modules in terms of matrices.

Lemma 17. *Let D be a left noetherian domain and $M = D^{1\times p}/(D^{1\times q}\,R)$ a finitely presented left D-module. Then, M is a free left D-module iff there exist $Q \in D^{p\times m}$ and $T \in D^{m\times p}$ satisfying $M \cong D^{1\times p}\,Q$ and $T\,Q = I_m$.*

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

Proof. $\Rightarrow$ The fact that D is a left noetherian domain implies that the concept of rank of a free left D-module is well defined. Hence, using the fact that M is a finitely generated module over a left noetherian domain, there exists an isomorphism $\phi : M \longrightarrow D^{1\times m}$, where $\mathrm{rank}_D(M) = m$. Therefore, we get the exact sequence

$$D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.Q} D^{1\times m} \longrightarrow 0, \tag{7}$$

where Q is the matrix which represents the D-morphism $\phi \circ \pi$ with respect to the canonical bases of $D^{1\times p}$ and $D^{1\times m}$, and $\pi : D^{1\times p} \longrightarrow M$ denotes the canonical projection onto M (see (1)). Finally, the exact sequence (7) ends with the free left D-module $D^{1\times m}$, and thus, it splits (Rotman, 1979). Therefore, there exists $T \in D^{m\times p}$ such that $T\,Q = I_m$.

$\Leftarrow$ If Q satisfies $M \cong D^{1\times p}\,Q$ and $T\,Q = I_m$, then we obtain $M \cong D^{1\times p}\,Q = D^{1\times m}$ as $D^{1\times p}\,Q \subseteq D^{1\times m}$ and, for all $\lambda \in D^{1\times m}$, we have $\lambda = (\lambda\,T)\,Q \in D^{1\times p}\,Q$, which shows $D^{1\times m} \subseteq D^{1\times p}\,Q$. $\square$

Let us give a system-theoretic interpretation of free modules. If M is a free left module over a left noetherian domain D, then, by Lemma 17, we get the split exact sequence (7). If $\mathcal{F}$ is any left D-module, then, by applying the left exact contravariant functor $\hom_D(\cdot\,,\mathcal{F})$ to (7) and using the fact that $\hom_D(\cdot\,,\mathcal{F})$ transforms split exact sequences of left D-modules into split exact sequences of abelian groups (Rotman, 1979), we obtain the split exact sequence

$$\mathcal{F}^q \xleftarrow{R.} \mathcal{F}^p \xleftarrow{Q.} \mathcal{F}^m \longleftarrow 0.$$

Therefore, for every $\eta \in \mathcal{F}^p$ satisfying $R\,\eta = 0$, there exists a unique $\xi \in \mathcal{F}^m$ such that $\eta = Q\,\xi$. In particular, ξ is then given by $\xi = T\,\eta$ where $T \in D^{m\times p}$ is a left-inverse of Q, i.e., $T\,Q = I_m$. Hence, the system $\ker_{\mathcal{F}}(R.)$ admits the *injective parametrization* $Q. : \mathcal{F}^m \longrightarrow \mathcal{F}^p$. Such a behaviour $\ker_{\mathcal{F}}(R.)$ is said to be *flat* in the control theory literature (Fliess et al., 1995) and ξ is called a *flat output* of $\ker_{\mathcal{F}}(R.)$. The class of flat systems has been shown to have important applications in control theory and, in particular, for the motion planning, tracking and optimal control problems. We refer the reader to Chyzak et al. (2005), Fliess et al. (1995), Pommaret and Quadrat (2004) and the references therein for more details and illustrations. An important issue in the theory of flat systems is being able to recognize whether a system is flat and, if so, computing a flat output. In a module-theoretic language, it means being able to check whether or not a finitely presented left D-module M is free and, if so, computing a basis of M. The results that we shall present in the following sections will give some constructive answers for some Ore algebras.

Let us consider a stably free left D-module M and the corresponding stably free behaviour $\hom_D(M, \mathcal{F})$. Using Lemma 16, we can always suppose that M is defined by a matrix $R \in D^{q\times p}$ which admits a right-inverse $S \in D^{p\times q}$, i.e., $M = D^{1\times p}/(D^{1\times q}\,R)$ and $R\,S = I_q$. The next result gives a system-theoretic interpretation of stably free modules.

Proposition 18 (*Quadrat and Robertz, 2005*). *Let $R \in D^{q\times p}$ be a matrix which admits a right-inverse $S \in D^{p\times q}$, i.e., $R\,S = I_q$, the stably free left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$ and $\pi : D^{1\times p} \longrightarrow M$ the canonical projection.*

(1) *If we define $R' = (R \quad 0) \in D^{q\times(p+q)}$, then we have the split exact sequence*

$$0 \longrightarrow D^{1\times q} \underset{.S'}{\overset{.R'}{\rightleftarrows}} D^{1\times(p+q)} \underset{.T'}{\overset{.Q'}{\rightleftarrows}} D^{1\times p} \longrightarrow 0 \tag{8}$$

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

with the following definitions for $S' \in D^{(p+q)\times q}$, $T' \in D^{p\times(p+q)}$, $Q' \in D^{(p+q)\times p}$:

$$S' = \begin{pmatrix} S \\ -I_q \end{pmatrix}, \quad T' = (I_p \quad S), \quad Q' = \begin{pmatrix} I_p - S\,R \\ R \end{pmatrix}. \tag{9}$$

Equivalently, we have the following Bézout identities:

$$\begin{pmatrix} R' \\ T' \end{pmatrix} (S' \quad Q') = I_{p+q}, \quad (S' \quad Q') \begin{pmatrix} R' \\ T' \end{pmatrix} = I_{p+q}.$$

(2) *Let us consider the D-morphism $\kappa : D^{1\times(p+q)} \longrightarrow D^{1\times(p+q)}/(D^{1\times q}\,R')$ defined by*

$$\kappa((\lambda_1, \ldots, \lambda_{p+q})) = (\pi(\lambda_1, \ldots, \lambda_p), \lambda_{p+1}, \ldots, \lambda_{p+q}).$$

(a) *We have $M \oplus D^{1\times q} \cong D^{1\times p}$, i.e., $M \oplus D^{1\times q}$ is a free left D-module with a basis defined by $\{\kappa(T'_i)\}_{1\le i\le p}$, where T'_i denotes the ith row of T'.*

(b) *If $\mathcal{F}$ is a left D-module, then we have the following equality:*

$$\mathcal{B}' = \left\{(\eta^T \quad \zeta^T)^T \in \mathcal{F}^{p+q} \mid R\,\eta = 0\right\} = Q'\,\mathcal{F}^p.$$

Moreover, for all $\zeta \in \mathcal{F}^q$ and $\eta \in \mathcal{F}^p$ such that $R\,\eta = 0$, there exists a unique $\xi \in \mathcal{F}^p$, defined by $\xi = \eta + S\,\zeta$, satisfying:

$$\begin{cases} \eta = (I_p - S\,R)\,\xi, \\ \zeta = R\,\xi. \end{cases}$$

The free behaviour $\mathcal{B}' \cong \mathcal{B} \oplus \mathcal{F}^q$ projects onto the stably free behaviour $\mathcal{B}$ under the projection $\mathcal{F}^{p+q} \longrightarrow \mathcal{F}^p$ defined by $(\eta^T \quad \zeta^T)^T \longmapsto \eta^T$.

We refer the reader to Quadrat and Robertz (2005) for different examples, applications of Proposition 18 in control theory and relations with the blowing up of singularities.

3. Shortest free resolutions and projective dimensions

The purpose of this section is to give a constructive algorithm which computes the left projective dimension $\mathrm{lpd}_D(M)$ of a left D-module M defined by means of a finite free resolution. In particular, this algorithm can be used for the Ore algebras D defined in Proposition 15, and thus, for the class of Ore algebras defined in Proposition 7. This result simplifies one obtained in Gago-Vargas (2003). Finally, we shall use this algorithm in order to test whether or not M is stably free and to compute a shortest free resolution of M which will be of crucial importance in Section 4 for the computation of bases of free left D-modules.

Let us start by recalling the concept of a *projective* and a *free resolution*.

Definition 19 (*Rotman, 1979*). A *projective resolution* of a left D-module M is an exact sequence of the form

$$\ldots \xrightarrow{\delta_{m+1}} P_m \xrightarrow{\delta_m} P_{m-1} \xrightarrow{\delta_{m-1}} P_{m-2} \xrightarrow{\delta_{m-2}} \cdots \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} M \longrightarrow 0, \tag{10}$$

where the left D-modules P_i are projective. Moreover, if the P_i's are free, then (10) is called a *free resolution* of M. Finally, if the P_i's are finitely generated free left D-modules and $P_{m+1} = 0$ for a certain $m \in \mathbb{Z}_{\ge 0}$, then (10) is called a *finite free resolution* of M.

As a free left D-module is projective (see Theorem 3), we obtain that a free resolution is also a projective one. The next proposition will play an important role in what follows.

Proposition 20. *Let us consider a projective resolution of a left D-module M:*

$$0 \longrightarrow P_m \xrightarrow{\delta_m} P_{m-1} \xrightarrow{\delta_{m-1}} P_{m-2} \xrightarrow{\delta_{m-2}} P_{m-3} \xrightarrow{\delta_{m-3}} \cdots \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} M \longrightarrow 0. \quad (11)$$

If $m \geq 2$ and there exists a D-morphism $\sigma_m : P_{m-1} \longrightarrow P_m$ such that $\sigma_m \circ \delta_m = \mathrm{id}_{P_m}$, then we have the following projective resolution of M:

$$0 \to P_{m-1} \xrightarrow{\tau_{m-1}} P_{m-2} \oplus P_m \xrightarrow{\tau_{m-2}} P_{m-3} \xrightarrow{\delta_{m-3}} P_{m-4} \xrightarrow{\delta_{m-4}} \cdots \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} M \to 0, \quad (12)$$

with the notation

$$\tau_{m-1} = \begin{pmatrix} \delta_{m-1} \\ \sigma_m \end{pmatrix}, \qquad \tau_{m-2} = (\delta_{m-2} \quad 0).$$

Proof. Using the fact that (11) is a complex at P_{m-2}, i.e., $\delta_{m-2} \circ \delta_{m-1} = 0$, we obtain $\tau_{m-2} \circ \tau_{m-1} = \delta_{m-2} \circ \delta_{m-1} = 0$, which proves that $\mathrm{im}\,\tau_{m-1} \subseteq \ker \tau_{m-2}$.

Let us now prove $\ker \tau_{m-2} \subseteq \mathrm{im}\,\tau_{m-1}$. We consider $(a \quad b)^T \in \ker \tau_{m-2}$. Then, we have $a \in P_{m-2}$, $b \in P_m$ and $\tau_{m-2}((a \quad b)^T) = \delta_{m-2}(a) = 0$. Since (11) is exact at P_{m-2}, there exists $c \in P_{m-1}$ such that $a = \delta_{m-1}(c)$. Now, let us define

$$d = (\mathrm{id}_{P_{m-1}} - \delta_m \circ \sigma_m \quad \delta_m)\,(c \quad b)^T = c - (\delta_m \circ \sigma_m)(c) + \delta_m(b) \in P_{m-1}.$$

Then, the image of d under τ_{m-1} is

$$\begin{pmatrix} \delta_{m-1}(c) - \delta_{m-1}(\delta_m(\sigma_m(c))) + \delta_{m-1}(\delta_m(b)) \\ \sigma_m(c) - ((\sigma_m \circ \delta_m) \circ \sigma_m)(c) + (\sigma_m \circ \delta_m)(b) \end{pmatrix} = \begin{pmatrix} \delta_{m-1}(c) \\ \sigma_m(c) - \sigma_m(c) + b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix},$$

which shows that $(a \quad b)^T \in \mathrm{im}\,\tau_{m-1}$, and thus, we have $\ker \tau_{m-2} \subseteq \mathrm{im}\,\tau_{m-1}$, which proves the exactness of (12) at $P_{m-2} \oplus P_m$.

Let us compute $\ker \tau_{m-1}$. If $d \in \ker \tau_{m-1}$, then we have $\tau_{m-1}(d) = 0$, i.e., $\delta_{m-1}(d) = 0$ and $\sigma_m(d) = 0$. Now, let us consider the short exact sequence

$$0 \longrightarrow P_m \xrightarrow{\delta_m} P_{m-1} \xrightarrow{\delta_{m-1}} \mathrm{im}\,\delta_{m-1} \longrightarrow 0. \quad (13)$$

Using the existence of $\sigma_m : P_{m-1} \longrightarrow P_m$ satisfying $\sigma_m \circ \delta_m = \mathrm{id}_{P_m}$, we obtain that (13) splits, i.e., there exists a D-morphism $\kappa_{m-1} : \mathrm{im}\,\delta_{m-1} \longrightarrow P_{m-1}$ such that the identity $\mathrm{id}_{P_{m-1}} = \delta_m \circ \sigma_m + \kappa_{m-1} \circ \delta_{m-1}$ holds. Hence, we have

$$d = \delta_m(\sigma_m(d)) + \kappa_{m-1}(\delta_{m-1}(d)) = 0,$$

which proves that τ_{m-1} is an injective D-morphism.

Finally, we have $\mathrm{im}\,\tau_{m-2} = \tau_{m-2}(P_{m-2} \oplus P_m) = \delta_{m-2}(P_{m-2}) = \mathrm{im}\,\delta_{m-2} = \ker \delta_{m-3}$ as (11) is exact at P_{m-3}. Hence, we obtain that (12) is exact at P_{m-3}, and thus, (12) is an exact sequence. □

We note that Proposition 20 simplifies a result obtained in Gago-Vargas (2003) by, on the one hand, explicating the morphisms in (11) and, on the other hand, giving a simple and direct proof. We have the following straightforward corollary of Proposition 20.

Corollary 21. *Let us consider a finite free resolution of a left D-module M:*

$$0 \longrightarrow D^{1\times p_m} \xrightarrow{.R_m} D^{1\times p_{m-1}} \xrightarrow{.R_{m-1}} \cdots \xrightarrow{.R_2} D^{1\times p_1} \xrightarrow{.R_1} D^{1\times p_0} \xrightarrow{\delta_0} M \longrightarrow 0. \quad (14)$$

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

(1) *If $m \geq 3$ and there exists $S_m \in D^{p_{m-1} \times p_m}$ such that $R_m S_m = I_{p_m}$, then we have the following finite free resolution of M:*

$$0 \to D^{1 \times p_{m-1}} \xrightarrow{.T_{m-1}} D^{1 \times (p_{m-2}+p_m)} \xrightarrow{.T_{m-2}} D^{1 \times p_{m-3}} \xrightarrow{.R_{m-3}} \cdots \xrightarrow{.R_1} D^{1 \times p_0} \xrightarrow{\delta_0} M \to 0, \tag{15}$$

where $T_{m-1} \in D^{p_{m-1} \times (p_{m-2}+p_m)}$, $T_{m-2} \in D^{(p_{m-2}+p_m) \times p_{m-3}}$ are defined by

$$T_{m-1} = (R_{m-1} \quad S_m), \quad T_{m-2} = \begin{pmatrix} R_{m-2} \\ 0 \end{pmatrix}.$$

(2) *If $m = 2$ and there exists $S_2 \in D^{p_1 \times p_2}$ such that $R_2 S_2 = I_{p_2}$, then we have the following finite presentation of M:*

$$0 \longrightarrow D^{1 \times p_1} \xrightarrow{.T_1} D^{1 \times (p_0+p_2)} \xrightarrow{\tau_0} M \longrightarrow 0, \tag{16}$$

with the notation

$$T_1 = (R_1 \quad S_2) \in D^{p_1 \times (p_0+p_2)}, \quad \tau_0 = \begin{pmatrix} \delta_0 \\ 0 \end{pmatrix}.$$

Remark 22. In case 2 of Corollary 21, we obtain the following isomorphism:

$$M = D^{1 \times p_0}/(D^{1 \times p_1} R_1) \cong \operatorname{coker}_D(.T_1) = D^{1 \times (p_0+p_2)}/(D^{1 \times p_1} T_1).$$

In terms of equations, the left D-module M is defined by $R_1 z = 0$, whereas $\operatorname{coker}_D(.T_1)$ is defined by $R_1 y_1 + S_2 y_2 = 0$. Applying R_2 on the left of the last system, we then have $(R_2 R_1) y_1 + (R_2 S_2) y_2 = 0$ and using the facts that $R_2 R_1 = 0$ and $R_2 S_2 = I_{p_2}$, we finally obtain $y_2 = 0$, and thus, $R_1 y_1 = 0$. Hence, the D-morphisms ϕ and ψ defined by

$$\begin{array}{rcll} \phi : M & \longrightarrow & \operatorname{coker}_D(.T_1) & \\ z_i & \longmapsto & y_{1i}, & i = 1, \ldots, p_0, \end{array} \qquad \begin{array}{rcll} \psi : \operatorname{coker}_D(.T_1) & \longrightarrow & M & \\ y_{1i} & \longmapsto & z_i, & i = 1, \ldots, p_0, \\ y_{2j} & \longmapsto & 0, & j = 1, \ldots, p_2, \end{array}$$

satisfy $\phi \circ \psi = \mathrm{id}$ and $\psi \circ \phi = \mathrm{id}$, i.e., ϕ is an isomorphism and $\phi^{-1} = \psi$.

Let us illustrate Corollary 21.

Example 23. Let us consider the Weyl algebra $D = A_3(\mathbb{Q})$ and the matrix

$$R_1 = \begin{pmatrix} \frac{1}{2} x_2 \partial_1 & x_2 \partial_2 + 1 & x_2 \partial_3 + \frac{1}{2} \partial_1 \\ -\frac{1}{2} x_2 \partial_2 - \frac{3}{2} & 0 & \frac{1}{2} \partial_2 \\ -\partial_1 - \frac{1}{2} x_2 \partial_3 & -\partial_2 & -\frac{1}{2} \partial_3 \end{pmatrix} \in D^{3 \times 3},$$

which defines the system $R_1 \xi = 0$ of the infinitesimal transformations of the Lie pseudogroup defined by the contact transformations (see Example V.1.84 in Pommaret (2001)). Using OreModules (Chyzak et al., 2007), we obtain the following free resolution of the left D-module $M = D^{1 \times 3}/(D^{1 \times 3} R_1)$:

$$0 \longrightarrow D \xrightarrow{.R_2} D^{1 \times 3} \xrightarrow{.R_1} D^{1 \times 3} \xrightarrow{\delta_0} M \longrightarrow 0,$$

where $R_2 = (\partial_2 \quad -(\partial_1 + x_2 \partial_3) \quad x_2 \partial_2 + 2) \in D^{1 \times 3}$. We easily check that the matrix $S_2 = (-x_2 \quad 0 \quad 1)^T$ is a right-inverse of R_2, and thus, by Corollary 21, we obtain the following finite free resolution of M:

$$0 \longrightarrow D^{1 \times 3} \xrightarrow{.T_1} D^{1 \times 4} \xrightarrow{\tau_0} M \longrightarrow 0, \tag{17}$$

where the matrix T_1 is defined by

$$T_1 = \begin{pmatrix} \frac{1}{2}\,x_2\,\partial_1 & x_2\,\partial_2 + 1 & x_2\,\partial_3 + \frac{1}{2}\,\partial_1 & -x_2 \\ -\frac{1}{2}\,x_2\,\partial_2 - \frac{3}{2} & 0 & \frac{1}{2}\,\partial_2 & 0 \\ -\partial_1 - \frac{1}{2}\,x_2\,\partial_3 & -\partial_2 & -\frac{1}{2}\,\partial_3 & 1 \end{pmatrix}.$$

We recall the definitions of the *left projective dimension* of a left D-module M and the *left global dimension* of a ring D (McConnell and Robson, 2000; Rotman, 1979).

Definition 24. (1) Let M be a left D-module. Then, we call the *left projective dimension* of M, denoted by $\mathrm{lpd}_D(M)$, the smallest $n \in \mathbb{Z}_{\geq 0}$ such that there exists a projective resolution of M of the form

$$0 \longrightarrow P_n \xrightarrow{\delta_n} P_{n-1} \xrightarrow{\delta_{n-1}} \cdots \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} M \longrightarrow 0. \qquad (18)$$

If no such finite projective resolution exists, then we set $\mathrm{lpd}_D(M) = +\infty$.

(2) The *left global dimension* of D, denoted by $\mathrm{lgld}(D)$, is the supremum of $\mathrm{lpd}_D(M)$ over all the left D-modules M.

The right projective dimension of a right D-module M and the right global dimension $\mathrm{rgld}(D)$ of D are defined similarly. If D is a left and right noetherian ring, then we have $\mathrm{lgld}(D) = \mathrm{rgld}(D)$ (see, e.g., 7.1.11 of McConnell and Robson (2000)). Then, $\mathrm{lgld}(D)$ is called *global dimension* of D and is denoted by $\mathrm{gld}(D)$.

Example 25. (1) (McConnell and Robson, 2000, Theorem 7.5.8 (iii)) If k is a field of characteristic 0, then $\mathrm{lgld}(A_n(k)) = \mathrm{rgld}(A_n(k)) = n$.

(2) (McConnell and Robson, 2000, Theorem 7.4.4) If k is a field of characteristic 0, then we have $\mathrm{lgld}(B_n(k)) = \mathrm{rgld}(B_n(k)) = n$.

(3) If k is a field of characteristic 0 and D denotes the Ore algebra of differential time-delay operators defined in (2) of Example 5, then $\mathrm{lgld}(D) = \mathrm{rgld}(D) = 2$.

(4) If k is a field of characteristic 0 and D denotes the first (resp., second) Ore algebra of shift operators defined in (3) of Example 5, then $\mathrm{lgld}(D) = \mathrm{rgld}(D) = 2\,n$ (resp., $\mathrm{lgld}(D) = \mathrm{rgld}(D) = n$).

The following proposition will allow us to develop an algorithm which computes the projective dimension of modules defined by means of finite free resolutions.

Proposition 26 (*Lam, 1999, Proposition 5.11*). *Let M be a left D-module. If $n \geq 1$, then we have $\mathrm{lpd}_D(M) = n$ iff there exists a finite projective resolution of M as* (18) *where δ_n is* non-split, *namely, there exists no D-morphism $\tau_n : P_{n-1} \longrightarrow P_n$ such that $\tau_n \circ \delta_n = \mathrm{id}_{P_n}$.*

Following Gago-Vargas (2003), we obtain Algorithm 1 for the computation of the left projective dimension of a left D-module $M = D^{1\times p_0}/(D^{1\times p_1}\,R_1)$.

Algorithm 1. • **Input:** A left D-module M defined by a finite free resolution (14).

• **Output:** The left projective dimension $\mathrm{lpd}_D(M)$ of M.

(1) Set $j = m$ and $T_j = R_m$.

(2) Check whether or not T_j admits a right-inverse S_j over D.

(a) If no right-inverse of T_j exists, then $\mathrm{lpd}_D(M) = j$ and stop the algorithm.

(b) If there exists a right-inverse S_j of T_j and

(i) if $j = 1$, then we have $\text{lpd}_D(M) = 0$ and stop the algorithm;
(ii) if $j = 2$, then compute (16);
(iii) if $j \geq 3$, then compute (15).

(3) Return to step (2) with $j \leftarrow j - 1$.

Proof of correctness. Let (14) be the last projective resolution constructed using Algorithm 1. We have $m \geq 1$. If R_m does not admit a right-inverse, then Algorithm 1 returns m, which is correct by Proposition 26. If R_m admits a right-inverse when the algorithm stops, then we have $m = 1$ and the result is $\text{lpd}_D(M) = 0$, which is correct because M is then presented by the split short exact sequence (16) showing that M is a direct summand of a free left D-module, and hence projective. □

Remark 27. We refer the reader to Chyzak et al. (2005) for the description of a constructive algorithm which checks whether or not a matrix over certain classes of Ore algebras admits a right-inverse and to Chyzak et al. (2007) for an implementation in OreModules. Algorithm 1 has recently been implemented in OreModules and it can be applied by means of the command ProjectiveDimension(Rat).

Example 28. We consider again Example 23. We check that the matrix T_1 defined in (17) does not admit a right-inverse. Hence, we obtain that $\text{lpd}_D(M) = 1$.

We are now in position to define the concept of a *shortest free resolution*.

Definition 29. We call a *shortest free resolution* of M the last free resolution obtained using Algorithm 1, namely, a finite free resolution of M of the form (14) which satisfies that either $m = 1$ and R_1 admits a right-inverse or the last matrix R_m of the free resolution does not admit a right-inverse.

We recall an interesting result.

Proposition 30 (*Chyzak et al., 2005, Proposition 8*). *If we denote by*

$$D = A[\partial_1; \sigma_1, \delta_1] \ldots [\partial_m; \sigma_m, \delta_m]$$

an Ore algebra where σ_i is an automorphism for $i = 1, \ldots, m$, then every finitely generated left D-module admits a finite free resolution of length less than or equal to $\text{lgld}(D) + 1$.

Proposition 30 shows that every finitely generated left module over the Ore algebra D defined previously admits a finite free resolution. In particular, if we can compute Gröbner bases over D, then we can obtain finite free resolutions (Chyzak et al., 2005). We then arrive at the following important remark.

Remark 31. If D satisfies the hypothesis of Proposition 7, then, using the fact that any finite free resolution (14) of a stably free left D-module $M = D^{1\times p_0}/(D^{1\times p_1} R_1)$ splits (Rotman, 1979), Algorithm 1 gives us a constructive way to compute $R \in D^{q\times p}$ which admits a right-inverse $S \in D^{p\times q}$ and satisfies $M \cong D^{1\times p}/(D^{1\times q} R)$ (see Lemma 16). Such a matrix R, which will be called *minimal presentation matrix* of M, can be obtained in OreModules by using the command ShortestFreeResolution for certain classes of Ore algebras. See Chyzak et al. (2007) for more details and examples.

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

Let us illustrate Remark 31 by means of an explicit example.

Example 32. Let us consider $D = A_1(\mathbb{Q})$ and the left D-module $M = D^{1\times 2}/(D^{1\times 2}\, R_1)$, where the matrix R_1 is defined by

$$R_1 = \begin{pmatrix} -t^2 & t\,\frac{d}{dt} - 1 \\ -t\,\frac{d}{dt} - 2 & \frac{d^2}{dt^2} \end{pmatrix} \in D^{2\times 2}.$$

We can check that M has the following free resolution:

$$0 \longrightarrow D \xrightarrow{.R_2} D^{1\times 2} \xrightarrow{.R_1} D^{1\times 2} \xrightarrow{\delta_0} M \longrightarrow 0, \quad R_2 = \begin{pmatrix} \frac{d}{dt} & -t \end{pmatrix} \in D^{1\times 2}.$$

Moreover, the matrix $S_2 = \begin{pmatrix} t & \frac{d}{dt} \end{pmatrix}^T$ is a right-inverse of R_2. Hence, if we denote by $T_1 = (R_1 \quad S_2)$, then, by Corollary 21, we obtain the finite free resolution of M:

$$0 \longrightarrow D^{1\times 2} \xrightarrow{.T_1} D^{1\times 3} \xrightarrow{\tau_0} M \longrightarrow 0. \tag{19}$$

We finally check that T_1 admits the following right-inverse S_1 defined by

$$S_1 = \begin{pmatrix} 0 & -1 & \frac{d}{dt} \\ -1 & 0 & -t \end{pmatrix}^T \in D^{3\times 2}.$$

Therefore, the exact sequence (19) splits, and thus, M is a stably free left D-module of rank 1, (19) is a shortest free resolution of M and T_1 is a minimal presentation matrix.

4. Computation of bases of free modules

In what follows, we shall consider a left noetherian domain D. In particular, this condition implies that D is a left Ore domain and has invariant basis number. The rank of a free left D-module F is then well defined (see Section 2). By extension, the rank of a finitely generated stably free left D-module M satisfying $M \oplus D^{1\times s} \cong D^{1\times r}$ is $r - s$.

4.1. *The general case*

The purpose of this section is to give a general algorithm which computes bases of free left D-modules based on the concept of *stable rank* (McConnell and Robson, 2000).

Definition 33. (1) A column vector $v \in D^m$ is called *unimodular* if v admits a left-inverse $w = (w_1 \ \dots \ w_m) \in D^{1\times m}$, i.e., if we have $w\, v = \sum_{i=1}^n w_i\, v_i = 1$. We denote by $U_c(m, D)$ the set of all unimodular columns of length m over D.

(2) A unimodular column $v = (v_1 \ \dots \ v_m)^T \in U_c(m, D)$ is called *stable* (*reducible*) if there exist $a_1, \dots, a_{m-1} \in D$ such that $v' = (v_1 + a_1\, v_m \ \dots \ v_{m-1} + a_{m-1}\, v_m)^T$ is unimodular, i.e., we have $v' \in U_c(m-1, D)$.

(3) We say that l *is in the stable range of* ${}_D D$ (i.e., D as a left D-module), if, for every $m > l$, every unimodular column $v \in U_c(m, D)$ is stable.

(4) The least positive integer l in the stable range of ${}_D D$ is called the *stable rank of* ${}_D D$. It is denoted by $\mathrm{sr}({}_D D)$. If no such integer exists, then we set $\mathrm{sr}({}_D D) = +\infty$.

We note that the stable rank is sometimes also called the *stable range* in algebra.

Similar definitions hold for *unimodular rows*. If we denote by $U_r(m, D)$ the set of unimodular rows of length m with entries in D, then we can similarly define the stable rank $\mathrm{sr}(D_D)$ of D_D (i.e., D as a right D-module).

Proposition 34 (*McConnell and Robson, 2000, Proposition 11.3.4*). $\mathrm{sr}({}_D D) = \mathrm{sr}(D_D)$.

Hence, in what follows, we shall only write $\mathrm{sr}(D)$ instead of $\mathrm{sr}({}_D D)$ or $\mathrm{sr}(D_D)$.

Example 35. We have the following results as regards the stable rank:

(1) If D is a principal ideal domain, then $\mathrm{sr}(D) \leq 2$ (e.g., $\mathrm{sr}(\mathbb{Z}) = 2$; if k is a field, then $\mathrm{sr}(k[x]) = 2$). If K is a *differential field* (e.g., $K = \mathbb{Q}(t)$) (Pommaret, 2001), then $\mathrm{sr}(K[\frac{\mathrm{d}}{\mathrm{d}t}; \mathrm{id}, \frac{\mathrm{d}}{\mathrm{d}t}]) \leq 2$.
(2) (McConnell and Robson, 2000, Corollary 5.10 (i)) $\mathrm{sr}(\mathbb{R}[x_1, \ldots, x_n]) = n + 1$.
(3) (Stafford, 1978) If k is a field containing $\mathbb{Q}$, then we have $\mathrm{sr}(A_n(k)) = 2$.
(4) (Stafford, 1978) Under the same hypothesis as in (3), we have $\mathrm{sr}(B_n(k)) = 2$.

Definition 36. The *elementary group* $E(m, D)$ is the subgroup of

$$\mathrm{GL}(m, D) = \{U \in D^{m\times m} \mid \exists\, V \in D^{m\times m} :\ U\,V = V\,U = I_m\}$$

which is generated by matrices of the form $I_m + r\,E_{ij}$, where $r \in D$, $i \neq j$ and E_{ij} denotes the matrix defined by 1 in the (i, j)-position and 0 elsewhere.

Example 37 (*McConnell and Robson, 2000, 11.3.5*). Upper and lower triangular matrices with 1 on the diagonal belong to the elementary group.

We can now state the following useful proposition.

Proposition 38. *If v is a stable element of $U_c(m, D)$, then there exists $E \in E(m, D)$ such that*

$$E\,v = (1\ 0\ \ldots\ 0)^T.$$

Proof. Let $v = (v_1\ \ \ldots\ \ v_m)^T$ be a stable element of $U_c(m, D)$. Then there exist elements $a_1, \ldots, a_{m-1} \in D$ such that

$$v' = (v_1{+}a_1\,v_m \quad v_2{+}a_2\,v_m \quad v_3{+}a_3\,v_m \quad \ldots \quad v_{m-1}{+}a_{m-1}\,v_m)^T \in U_c(m{-}1, D). \tag{20}$$

Now, let us denote by $v'_i = v_i + a_i\,v_m$, for $i = 1, \ldots, m-1$, and

$$E_1 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{m-1} \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix} \in E(m, D). \tag{21}$$

Then, we easily check that we have $E_1\,v = (v'_1\ \ v'_2\ \ldots\ v'_{m-1}\ v_m)^T$.

Using the fact that $v' \in U_c(m-1, D)$, then there exist $b_1, \ldots, b_{m-1} \in D$ such that

$$\sum_{i=1}^{m-1} b_i\,v'_i = 1.$$

Hence, multiplying both sides of the previous expression by $v'_1 - 1 - v_m$, then we get

$$\sum_{i=1}^{m-1} (v'_1 - 1 - v_m)\,(b_i\, v'_i) = v'_1 - 1 - v_m. \tag{22}$$

If we now define $v''_i = (v'_1 - 1 - v_m)\, b_i$, for $i = 1, \ldots, m-1$, and

$$E_2 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ v''_1 & v''_2 & v''_3 & \ldots & v''_{m-1} & 1 \end{pmatrix} \in E(m, D), \tag{23}$$

then we have $E_2\,(v'_1\ \ldots\ v'_{m-1}\ v_m)^T = (v'_1\ \ldots\ v'_{m-1}\ v'_1 - 1)^T$. Moreover, if we define

$$E_3 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & -1 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix} \in E(m, D), \tag{24}$$

then we easily check that we have $E_3\,(v'_1\ \ldots\ v'_{m-1}\ v'_1 - 1)^T = (1\ v'_2\ \ldots\ v'_{m-1}\ v'_1 - 1)^T$.

Finally, if we define

$$E_4 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ -v'_2 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -v'_{m-1} & 0 & 0 & \ldots & 1 & 0 \\ -v'_1 + 1 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix} \in E(m, D), \tag{25}$$

then we obtain $E_4\,(1\ v'_2\ \ldots\ v'_{m-1}\ v'_1 - 1)^T = (1\ 0\ \ldots\ 0)^T$. Hence, the matrix defined by $E = E_4\, E_3\, E_2\, E_1 \in E(m, D)$ satisfies $E\,(v_1\ \ldots\ v_m)^T = (1\ 0\ \ldots\ 0)^T$. □

We sum up the constructive proof of Proposition 38 in the next algorithm.

Algorithm 2. • **Input:** A stable element $v = (v_1\ \ldots\ v_m)^T$ of $U_c(m, D)$.
• **Output:** An elementary matrix $E \in D^{m\times m}$ such that $E\,v = (1\ 0\ \ldots\ 0)^T$.

(1) Compute $a_1, \ldots, a_{m-1} \in D$ satisfying condition (20).
(2) Compute the matrix E_1 given in (21).
(3) Compute $b_1, \ldots, b_{m-1} \in D$ satisfying $\sum_{i=1}^{m-1} b_i\, v'_i = 1$, where v'_i denotes the ith component of the vector $E_1\, v$, $i = 1, \ldots, m-1$, and define $v''_i = (v'_1 - 1 - v_m)\, b_i \in D$, $i = 1, \ldots, m-1$.
(4) Define the matrices E_2, E_3, E_4 given by (23)–(25).
(5) Return the product $E = E_4\, E_3\, E_2\, E_1$.

Let us illustrate Proposition 38 on an example.

Example 39. Let us consider the Weyl algebra $D = A_3(\mathbb{Q})$ and the column vector $v = (\partial_1 + x_3 \quad \partial_2 \quad \partial_3)^T$. We can easily check that $w = (\partial_3 \quad 0 \quad -(\partial_1 + x_3))$ is a left-inverse of v, i.e., $v \in U_c(3, D)$. Moreover, the vector $v' = (\partial_1 + x_3 \quad \partial_2 + \partial_3)^T$ admits a left-inverse $w' = (\partial_2 + \partial_3 \quad -(\partial_1 + x_3))$, which shows that v' is unimodular, and thus, v is stable. Hence, by Proposition 38, there exists a matrix $E \in E(3, D)$ such that $E\, v = (1 \quad 0 \quad 0)^T$. Let us compute such a matrix E following Algorithm 2.

The unimodular vector v' shows that we can take $a_1 = 0$ and $a_2 = 1$. If we define

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

we then obtain $E_1\, v = (\partial_1 + x_3 \quad \partial_2 + \partial_3 \quad \partial_3)^T$. We check that we have the Bézout identity:

$$(\partial_2 + \partial_3)\,(\partial_1 + x_3) - (\partial_1 + x_3)\,(\partial_2 + \partial_3) = 1.$$

If we define $v''_1 = (\partial_1 + x_3 - 1 - \partial_3)\,(\partial_2 + \partial_3)$, $v''_2 = -(\partial_1 + x_3 - 1 - \partial_3)\,(\partial_1 + x_3)$ and

$$E_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ v''_1 & v''_2 & 1 \end{pmatrix} \in E(3, D),$$

we then get $E_2\,(\partial_1 + x_3 \quad \partial_2 + \partial_3 \quad \partial_3)^T = (\partial_1 + x_3 \quad \partial_2 + \partial_3 \quad \partial_1 + x_3 - 1)^T$. Finally, if we define

$$E_3 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in E(3, D), \qquad E_4 = \begin{pmatrix} 1 & 0 & 0 \\ -(\partial_2 + \partial_3) & 1 & 0 \\ -(\partial_1 + x_3 - 1) & 0 & 1 \end{pmatrix} \in E(3, D),$$

and $E = E_4\, E_3\, E_2\, E_1 \in E(3, D)$, then we have $E\, v = (1 \quad 0 \quad 0)^T$.

We are now in position to state the main result of this paper (we recall that, in this section, D denotes a left noetherian domain).

Theorem 40. *Let k be a field and D a non-commutative k-algebra with an involution θ. Then, any stably free left D-module M defined by a finite free resolution of the form*

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \longrightarrow 0, \tag{26}$$

with $p - q \geq \mathrm{sr}(D)$ is free.

Proof. Using the fact that M is stably free, the exact sequence (26) splits (Rotman, 1979), and thus, R admits a right-inverse $S \in D^{p\times q}$. Let us define $\widetilde{R} = \theta(R) \in D^{p\times q}$ (see Definition 8) and $\widetilde{S} = \theta(S) \in D^{q\times p}$. As we have $\widetilde{S}\,\widetilde{R} = \theta(S)\,\theta(R) = \theta(R\, S) = \theta(I_q) = I_q$, the following exact sequence splits:

$$0 \longleftarrow D^{1\times q} \xleftarrow{.\widetilde{R}} D^{1\times p} \longleftarrow \ker_D(.\widetilde{R}) \longleftarrow 0.$$

Since we have $p > p - q \geq \mathrm{sr}(D)$, the first column $\widetilde{R}_1 \in D^p$ of $\widetilde{R}$ is then stable. Therefore, applying Proposition 38 to $\widetilde{R}_1$, we obtain a matrix $G_1 \in E(p, D)$ which satisfies

$$G_1\, \widetilde{R}_1 = (1\ 0\ \ldots\ 0)^T.$$

If $q = 1$, then we have $R = R_1$ and we set $G = G_1$. Otherwise, we obtain

$$G_1\, \widetilde{R} = \begin{pmatrix} 1 & \star \\ 0 & \\ \vdots & \widetilde{R}_2 \\ 0 & \end{pmatrix}, \quad \widetilde{R}_2 \in D^{(p-1)\times(q-1)},$$

where $\star$ denotes an appropriate number of elements in D.

The matrix $G_1\, \widetilde{R}$ admits a left-inverse (e.g., $\widetilde{S}\, G_1^{-1} \in D^{q\times p}$). We then easily check that every left-inverse L of $G_1\, \widetilde{R}$ has the form

$$L = \begin{pmatrix} 1 & \star \\ 0 & L_2 \end{pmatrix}, \quad L_2 \in D^{(q-1)\times(p-1)},$$

which shows that $L_2\, \widetilde{R}_2 = I_{q-1}$, and thus, the first column of the matrix $\widetilde{R}_2$ is unimodular. Since $q - 1 \geq 1$, we have $p - 1 > p - q \geq \mathrm{sr}(D)$ and we can apply Proposition 38 to the first column of $\widetilde{R}_2$ obtaining $F_2 \in E(p-1, D)$ such that

$$F_2\, \widetilde{R}_2 = \begin{pmatrix} 1 & \star \\ 0 & \\ \vdots & \widetilde{R}_3 \\ 0 & \end{pmatrix}, \quad \widetilde{R}_3 \in D^{(p-2)\times(q-2)}.$$

Hence, if we define $G_2 = \begin{pmatrix} 1 & 0 \\ 0 & F_2 \end{pmatrix}$, then we have $(G_2\, G_1)\, \widetilde{R} = \begin{pmatrix} 1 & \star & \star \\ 0 & 1 & \star \\ \vdots & 0 & \\ \vdots & \vdots & \widetilde{R}_3 \\ 0 & 0 & \end{pmatrix}$.

By induction on the number of columns and using the fact that $p - q \geq \mathrm{sr}(D)$, we finally obtain an elementary matrix $G \in E(p, D)$ which satisfies

$$G\, \widetilde{R} = (I_q \quad 0)^T.$$

We now easily check that we have $\ker_D(.(G\, \widetilde{R})) = D^{1\times(p-q)}\, (0 \quad I_{p-q})$. Hence, if we define the matrix $P = (0 \quad I_{p-q}) \in D^{(p-q)\times p}$ and use the fact that G is invertible over D, then

$$\lambda \in \ker_D(.\widetilde{R}) \Leftrightarrow \lambda \widetilde{R} = 0 \Leftrightarrow (\lambda G^{-1}) G \widetilde{R} = 0 \Leftrightarrow \lambda G^{-1} \in \ker_D(.(G\widetilde{R})) = D^{1\times(p-q)}\, P,$$

i.e., there exists $\mu \in D^{1\times(p-q)}$ such that $\lambda\, G^{-1} = \mu\, P$, i.e., $\lambda = \mu\, P\, G \in D^{1\times(p-q)}\, (P\, G)$. Conversely, any element of the form $\lambda = \mu\, P\, G \in D^{1\times(p-q)}\, (P\, G)$, where $\mu \in D^{1\times(p-q)}$, belongs to $\ker_D(.\widetilde{R})$ and we get $\ker_D(.\widetilde{R}) = D^{1\times(p-q)}\, (P\, G)$. Moreover, $\nu \in \ker_D(.(P\, G))$ satisfies that $\nu\, P\, G = 0$ and, using the fact that G is invertible over D, we then have $\nu\, P = 0$, i.e., $\nu = 0$. Hence, we obtain $\ker_D(.\widetilde{R}) = D^{1\times(p-q)}\, (P\, G) \cong D^{1\times(p-q)}$. If we define $\widetilde{Q} = P\, G$, then we have the following split exact sequence:

$$0 \longleftarrow D^{1\times q} \xleftarrow{.\widetilde{R}} D^{1\times p} \xleftarrow{.\widetilde{Q}} D^{1\times(p-q)} \longleftarrow 0.$$

Using the fact that the adjoint of a split exact sequence is also a split exact sequence (Chyzak et al., 2005; Rotman, 1979), we finally obtain the split exact sequence

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.Q} D^{1\times (p-q)} \longrightarrow 0, \tag{27}$$

with the notation $Q = \theta(\widetilde{Q}) \in D^{p\times(p-q)}$. Therefore, we have

$$M = D^{1\times p}/(D^{1\times q}\, R) \cong D^{1\times p}\, Q = D^{1\times (p-q)},$$

which shows that M is a free left D-module of rank $p-q$ and Q admits a left-inverse. If we denote by $T \in D^{(p-q)\times p}$ a left-inverse of Q, i.e., $T\,Q = I_{p-q}$, then $\{\pi(T_i)\}_{1\leq i\leq p-q}$ is a basis of M, where T_i denotes the ith row of T and $\pi : D^{1\times p} \longrightarrow M$ is the D-morphism which maps any vector in $D^{1\times p}$ to its residue class in M. □

The proof of Theorem 40 was inspired by Corollaire 2.14 in Lombardi (2005) for commutative rings. Hence, Theorem 40 extends this corollary to non-commutative rings.

Remark 41. Theorem 40 has been stated under the hypothesis that D admits an involution θ. However, using a dual version of Proposition 38, namely, for every $v \in U_r(m, D)$, there exists $E \in E(m, D)$ such that $v\,E = (1\ 0\ \ldots\ 0)$, we can follow the proof of Theorem 40 using, however, right multiplication of R by elementary matrices instead of left multiplication of $\widetilde{R}$. Hence, Theorem 40 is true without this restrictive hypothesis. However, as we are mainly interested in an effective implementation of Theorem 40 in OreModules (Chyzak et al., 2007), where only Gröbner bases of left D-modules are computed, we need to impose this condition. Finally, finitely presented right D-modules have no system-theoretic interpretation contrary to left D-modules (see Section 2).

Remark 42. We note that the number $p-q$ only depends on the left D-module M. Indeed, if we have another finite presentation of M of the form

$$0 \longrightarrow D^{1\times q'} \xrightarrow{.R'} D^{1\times r} \xrightarrow{\pi'} M \longrightarrow 0,$$

then, by Schanuel's lemma (Rotman, 1979), we obtain that $D^{1\times q'} \oplus D^{1\times p} \cong D^{1\times q} \oplus D^{1\times p'}$. As D has invariant basis number, we obtain $q' + p = q + p'$, i.e., $p' - q' = p - q$.

Let us sum up the constructive proof of Theorem 40 in the next algorithm.

Algorithm 3. • **Input:** A k-algebra D with an involution θ, a matrix $R \in D^{q\times p}$ which admits a right-inverse $S \in D^{p\times q}$ and satisfies that $p - q \geq \mathrm{sr}(D)$.

• **Output:** Two matrices $Q \in D^{p\times(p-q)}$ and $T \in D^{(p-q)\times p}$ such that $T\,Q = I_{p-q}$ and $\{\pi(T_i)\}_{1\leq i\leq p-q}$ is a basis of the free left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$, where $\pi : D^{1\times p} \longrightarrow M$ denotes the canonical projection and T_i is the ith row of T.

(1) Compute $\widetilde{R} = \theta(R) \in D^{p\times q}$ and set $i = 1$, $V = \widetilde{R}$, $U = I_p$.
(2) Denote by $V_i \in D^{p-i+1}$ the column vector formed by taking the last $p-i+1$ elements of the ith column of V.
(3) Applying Algorithm 2 to V_i, compute the matrix $F_i \in E(p-i+1, D)$ such that $F_i\,V_i = (1\ 0\ \ldots\ 0)^T$.
(4) Define the matrix $G_i = \begin{pmatrix} I_{i-1} & 0 \\ 0 & F_i \end{pmatrix} \in E(p, D)$ with $G_1 = F_1$.
(5) If $i < q$ then return to step (2) with $V \leftarrow G_i\,V$, $U \leftarrow G_i\,U$ and $i \leftarrow i + 1$.

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

(6) Define $G = G_q\, U$ and the matrix $\widetilde{Q}$ formed by selecting the last $p - q$ rows of G.
(7) Define $Q = \theta(\widetilde{Q}) \in D^{p \times (p-q)}$ and compute a left-inverse $T \in D^{(p-q) \times p}$ of Q.

Let us illustrate Algorithm 3 on an example.

Example 43. Let us define $D = A_1(\mathbb{Q})$, the matrices

$$R = \begin{pmatrix} 0 & \frac{\mathrm{d}}{\mathrm{d}t} & 0 & -1 \\ \frac{\mathrm{d}}{\mathrm{d}t} & 0 & -t & 0 \end{pmatrix} \in D^{2\times 4}, \quad S = \begin{pmatrix} 0 & 0 & 0 & -1 \\ t & 0 & \frac{\mathrm{d}}{\mathrm{d}t} & 0 \end{pmatrix}^T \in D^{4\times 2},$$

and the left D-module $M = D^{1\times 4}/(D^{1\times 2}\, R)$. We can easily check that S is a right-inverse of R, i.e., $R\, S = I_2$. Therefore, M is stably free with $\mathrm{rank}_D(M) = 2$. Using Theorem 40 and (3) of Example 35, i.e., $\mathrm{sr}(D) = 2$, we then obtain that M is free.

Let us compute a basis of M following Algorithm 3. The formal adjoint $\widetilde{R}$ of R is

$$\widetilde{R} = \begin{pmatrix} 0 & -\frac{\mathrm{d}}{\mathrm{d}t} & 0 & -1 \\ -\frac{\mathrm{d}}{\mathrm{d}t} & 0 & -t & 0 \end{pmatrix}^T \in D^{4\times 2}.$$

Now, following Algorithm 2 for the first column $v_1 = \begin{pmatrix} 0 & -\frac{\mathrm{d}}{\mathrm{d}t} & 0 & -1 \end{pmatrix}^T$ of $\widetilde{R}$, we obtain that the vector $v_1' = \begin{pmatrix} 1 & -\frac{\mathrm{d}}{\mathrm{d}t} & 0 \end{pmatrix}^T$ is trivially unimodular, which shows that we can choose $a_1 = -1$ and $a_2 = 0$ and define the elementary matrix

$$E_1 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We then have $E_1\, v_1 = \begin{pmatrix} 1 & -\frac{\mathrm{d}}{\mathrm{d}t} & 0 & -1 \end{pmatrix}^T$. Now, using that $w' = (1 \quad 0 \quad 0)$ is a left-inverse of v_1', we can take $b_1 = 1$, $b_2 = 0$ and define the following unimodular matrices:

$$E_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{\mathrm{d}}{\mathrm{d}t} & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We can easily check that we have

$$G_1 = E_4\, E_3\, E_2\, E_1 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -\frac{\mathrm{d}}{\mathrm{d}t} \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in E(4, D), \quad G_1\, \widetilde{R} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & -t \\ 0 & -\frac{\mathrm{d}}{\mathrm{d}t} \end{pmatrix}.$$

Let us now consider the sub-column $v_2 = \begin{pmatrix} 0 & -t & -\frac{\mathrm{d}}{\mathrm{d}t} \end{pmatrix}^T$ of the matrix $G_1\, \widetilde{R}$. We apply Algorithm 2 to v_2 and we can easily check that $v_2' = \begin{pmatrix} -\frac{\mathrm{d}}{\mathrm{d}t} & -t \end{pmatrix}^T$ has a left-inverse defined by $w_2' = \begin{pmatrix} t & -\frac{\mathrm{d}}{\mathrm{d}t} \end{pmatrix}$. Therefore, we can take $a_1 = 1$ and $a_2 = 0$ and define the following unimodular matrices:

$$E_1' = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_2' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -t & \frac{\mathrm{d}}{\mathrm{d}t} & 1 \end{pmatrix}, \quad E_3' = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$E_4' = \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ \frac{\mathrm{d}}{\mathrm{d}t}+1 & 0 & 1 \end{pmatrix}.$$

We then have

$$F_2 = E_4'\,E_3'\,E_2'\,E_1' = \begin{pmatrix} 1+t & -\frac{\mathrm{d}}{\mathrm{d}t} & t \\ t\,(t+1) & -t\,\frac{\mathrm{d}}{\mathrm{d}t}+1 & t^2 \\ t\,\frac{\mathrm{d}}{\mathrm{d}t}+\frac{\mathrm{d}}{\mathrm{d}t}+2 & -\frac{\mathrm{d}^2}{\mathrm{d}t^2} & t\,\frac{\mathrm{d}}{\mathrm{d}t}+2 \end{pmatrix} \in E(4, D),$$

$$F_2\,v_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Let us define the following matrices:

$$G_2 = \begin{pmatrix} 1 & 0 \\ 0 & F_2 \end{pmatrix},$$

$$G = G_2\,G_1 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ t & t+1 & -\frac{\mathrm{d}}{\mathrm{d}t} & -(t+1)\,\frac{\mathrm{d}}{\mathrm{d}t} \\ t^2 & t\,(t+1) & -t\,\frac{\mathrm{d}}{\mathrm{d}t}+1 & -t\,(t+1)\,\frac{\mathrm{d}}{\mathrm{d}t} \\ t\,\frac{\mathrm{d}}{\mathrm{d}t}+2 & t\,\frac{\mathrm{d}}{\mathrm{d}t}+\frac{\mathrm{d}}{\mathrm{d}t}+2 & -\frac{\mathrm{d}^2}{\mathrm{d}t^2} & -\left(t\,\frac{\mathrm{d}}{\mathrm{d}t}+\frac{\mathrm{d}}{\mathrm{d}t}+2\right)\,\frac{\mathrm{d}}{\mathrm{d}t} \end{pmatrix}.$$

Then, we have $G\,\widetilde{R} = (I_2 \quad 0)^T$. Finally, if we consider the following two matrices:

$$\begin{aligned} Q &= \begin{pmatrix} t^2 & -t\,\frac{\mathrm{d}}{\mathrm{d}t}+1 \\ t^2+t & -(t+1)\,\frac{\mathrm{d}}{\mathrm{d}t}+1 \\ t\,\frac{\mathrm{d}}{\mathrm{d}t}+2 & -\frac{\mathrm{d}^2}{\mathrm{d}t^2} \\ t\,(t+1)\,\frac{\mathrm{d}}{\mathrm{d}t}+2\,t+1 & -(t+1)\,\frac{\mathrm{d}^2}{\mathrm{d}t^2} \end{pmatrix}, \\ T &= \begin{pmatrix} 0 & 0 & t+1 & -1 \\ t+1 & -t & 0 & 0 \end{pmatrix}, \end{aligned} \tag{28}$$

where Q is formed by taking the last two columns of the formal adjoint of G and T is a left-inverse of Q, then a basis of M is defined by $\{\pi((0,\ 0,\ t+1,\ -1)),\ \pi((t+1,\ -t,\ 0,\ 0))\}$, where $\pi : D^{1\times 4} \longrightarrow M$ denotes the canonical projection onto M.

Let us consider a left D-module $\mathcal{F}$ (e.g., $\mathcal{F} = C^\infty(\mathbb{R})$) and the behaviour $\ker_{\mathcal{F}}(R.)$. Using the matrix Q defined by (28), we obtain the injective parametrization of $\ker_{\mathcal{F}}(R.)$

$$\begin{cases} \dot{x}_2(t) = u_2(t), \\ \dot{x}_1(t) = t\,u_1(t), \end{cases} \Leftrightarrow \begin{cases} x_1(t) = t^2\,y_1(t) - t\,\dot{y}_2(t) + y_2(t), \\ x_2(t) = (t^2+t)\,y_1(t) - (t+1)\,\dot{y}_2(t) + y_2(t), \\ u_1(t) = t\,\dot{y}_1(t) + 2\,y_1(t) - \ddot{y}_2(t), \\ u_2(t) = t(t+1)\,\dot{y}_1(t) + (2\,t+1)\,y_1(t) - (1+t)\,\ddot{y}_2(t), \end{cases} \tag{29}$$

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

which proves that $\ker_{\mathcal{F}}(R.)$ is flat. A flat output $(y_1 \quad y_2)^T$ of $\ker_{\mathcal{F}}(R.)$ is defined by

$$(y_1 \quad y_2)^T = T\,(x_1 \quad x_2 \quad u_1 \quad u_2)^T \Leftrightarrow \begin{cases} y_1(t) = (t+1)\,u_1(t) - u_2(t), \\ y_2(t) = (t+1)\,x_1(t) - t\,x_2(t). \end{cases}$$

The next corollary is a well-known result in the literature of non-commutative algebra. See for instance McConnell and Robson (2000). However, we give here a simple and constructive proof based on Algorithm 1 and the kind of Gaussian elimination used in the proof of Theorem 40 (see Algorithm 3).

Corollary 44. *Let k be a field and D a non-commutative k-algebra with an involution θ, M a stably free left D-module with $\operatorname{rank}_D(M) \geq \operatorname{sr}(D)$ and (14) a finite free resolution of M. Then, M is a free left D-module.*

Proof. Let us consider a stably free left D-module $M = D^{1\times p_0}/(D^{1\times p_1} R_1)$, where $R_1 \in D^{p_1 \times p_0}$. Using Algorithm 1, we can always suppose that M is defined by the presentation $M \cong D^{1\times p}/(D^{1\times q} R)$, where the matrix $R \in D^{q\times p}$ admits a right-inverse $S \in D^{p\times q}$. See Remark 31 for more details. Hence, we have the following finite free resolution of M:

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \longrightarrow 0.$$

In particular, we have $\operatorname{rank}_D(M) = p - q$, and thus, the hypothesis $\operatorname{rank}_D(M) \geq \operatorname{sr}(D)$ implies $p \geq q + \operatorname{sr}(D)$. Hence, by Theorem 40, M is a free left D-module. □

Algorithm 4. • **Input:** A k-algebra with an involution θ, a matrix $R_1 \in D^{p_1\times p_0}$ such that the left D-module $M = D^{1\times p_0}/(D^{1\times p_1} R_1)$ is stably free with $\operatorname{rank}_D(M) \geq \operatorname{sr}(D)$ and a finite free resolution (14) of M.

- **Output:** $R \in D^{q\times p}$, $Q \in D^{p\times(p-q)}$ and $T \in D^{(p-q)\times p}$ satisfying $M \cong D^{1\times p}/(D^{1\times q} R)$, $T\,Q = I_{p-q}$ and $\{\pi(T_i)\}_{1\leq i\leq p-q}$ is a basis of the free left D-module $D^{1\times p}/(D^{1\times q} R)$, where T_i denotes the ith row of T and $\pi : D^{1\times p} \longrightarrow D^{1\times p}/(D^{1\times q} R)$ the canonical projection.

(1) Applying Algorithm 1, we obtain a finite free resolution of M of the form

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \longrightarrow 0. \tag{30}$$

(2) Applying Algorithm 3 to $R \in D^{q\times p}$, we finally obtain the matrices $Q \in D^{p\times(p-q)}$ and $T \in D^{(p-q)\times p}$ satisfying $T\,Q = I_{p-q}$ and such that $\{\pi(T_i)\}_{1\leq i\leq p-q}$ is a basis of the free left D-module $D^{1\times p}/(D^{1\times q} R) \cong M$ (see Remark 22).

4.2. The Weyl algebra case

We shall now focus on the two particular cases $D = A_n(k)$ and $D = B_n(k)$.

We state another nice result due to J.T. Stafford which will allow us to compute the elements $a_i \in D$ satisfying (20), i.e., to effectively handle step (1) of Algorithm 2.

Theorem 45 (*Stafford, 1978*). *Let k be a field containing $\mathbb{Q}$ and $D = A_n(k)$ or $B_n(k)$. If $v_1, v_2, v_3 \in D$, then there exist $a_1, a_2 \in D$ such that the left ideal $I = D\,v_1 + D\,v_2 + D\,v_3$ of D satisfies*

$$I = D\,(v_1 + a_1\,v_3) + D\,(v_2 + a_2\,v_3).$$

We illustrate Theorem 45 on a simple example.

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

Example 46. Let us consider $D = A_3(\mathbb{Q})$ and the left ideal $I = D\,(\partial_1 + x_3) + D\,\partial_2 + D\,\partial_3$ of D (see Example 39); then we have $I = D\,(\partial_1 + x_3) + D\,(\partial_2 + \partial_3)$ as

$$\begin{cases} \partial_2 = (\partial_2\,(\partial_2 + \partial_3))\,(\partial_1 + x_3) - (\partial_2\,(\partial_1 + x_3))\,(\partial_2 + \partial_3), \\ \partial_3 = (\partial_3\,(\partial_2 + \partial_3))\,(\partial_1 + x_3) - (\partial_3\,(\partial_1 + x_3))\,(\partial_2 + \partial_3). \end{cases}$$

Two constructive algorithms of Theorem 45 have recently been presented by A. Hillebrand and W. Schmale on the one hand and by A. Leykin on the other hand. We refer the reader to Hillebrand and Schmale (2001) and Leykin (2004) for more details. Both strategies have been implemented in the package Stafford (Quadrat and Robertz, 2005–2007). However, we point out that, due to the large number of Gröbner basis computations used in Hillebrand and Schmale (2001) and Leykin (2004), Theorem 45 only works constructively on relatively small examples.

Let us now consider a unimodular column vector $v = (v_1 \ \dots \ v_m)^T$ where $m \geq 3$. Using the fact that $\mathrm{sr}(D) = 2$, v is then stable. Therefore, there exist $a_1, \dots, a_{m-1} \in D$ such that the column vector $v' = (v_1 + a_1\,v_m \ \dots \ v_{m-1} + a_{m-1}\,v_m)^T$ is unimodular. A constructive way to compute the a_i is, for instance, to apply a constructive version of Theorem 45 to the left ideal $I = D\,v_1 + D\,v_2 + D\,v_m$. Then, we find $a_1, a_2 \in D$ such that

$$I = D\,(v_1 + a_1\,v_m) + D\,(v_2 + a_2\,v_m).$$

Using the fact that v is unimodular, i.e., $\sum_{i=1}^{m} D\,v_i = D$, we obtain

$$D\,(v_1 + a_1\,v_m) + D\,(v_2 + a_2\,v_m) + \sum_{i=3}^{m-1} D\,v_i = D,$$

showing that the vector $(v_1 + a_1\,v_m \quad v_2 + a_2\,v_m \quad v_3 \quad \dots \quad v_{m-1})^T$ is unimodular. Hence, using Stafford, we then have a constructive way to perform step (1) of Algorithm 2, and thus, the complete Algorithm 2, as step (3) can be performed using the command LeftInverse of OreModules.

Combining Theorem 40 with (3) and (4) of Example 35, we obtain the following result.

Corollary 47 (*Stafford, 1978*). *If k is a field containing $\mathbb{Q}$ and $D = A_n(k)$ or $B_n(k)$, then any stably free left D-module M satisfying* $\mathrm{rank}_D(M) \geq 2$ *is free.*

With the aid of the functions Involution, Mult and LeftInverse of OreModules, Algorithms 2 and 3 become constructive. Moreover, using the command ShortestFreeResolution (see Remark 31), we have a way to compute a finite free resolution of M of the form (30) and to check whether or not M is a stably free left D-module with $\mathrm{rank}_D(M) \geq 2$ (see 4 of Theorem 10 and Chyzak et al. (2005) for another algorithm checking stably freeness using the computation of certain extension modules $\mathrm{ext}^i_D(\widetilde{N}, D)$, where $\widetilde{N} = D^{1\times q}/(D^{1\times p}\,\theta(R))$ and θ is the involution defined in (2) of Example 9). We conclude that Algorithm 4 can be constructively performed.

Another algorithm for computing bases of free modules over $A_n(k)$ has also been developed in Gago-Vargas (2003) following the proof given by J.T. Stafford (1978). However, despite the interest of Gago-Vargas (2003), Algorithm 4 seems to be easier to understand and to implement. Indeed, it is conceptually nothing but Gaussian elimination as soon as a constructive version of Theorem 45 is available.

Example 48. Let us consider $D = A_3(\mathbb{Q})$, $R = (-\partial_1 + x_3 \quad -\partial_2 \quad -\partial_3)$ and the left D-module $M = D^{1\times 3}/(D\,R)$. We easily check that $S = (-\partial_3 \quad 0 \quad \partial_1 - x_3)^T$ is a right-inverse

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

of R, a fact showing that M is a stably free left D-module of rank 2. Hence, by Corollary 47, we obtain that M is a free left D-module. Let us compute a basis of M following Algorithm 3. We first compute the formal adjoint $\widetilde{R} = (\partial_1 + x_3 \quad \partial_2 \quad \partial_3)^T$ of R. We then need to compute an elementary matrix G such that $G\,\widetilde{R} = (1 \quad 0 \quad 0)^T$. However, such an elementary matrix G has already been computed in Example 39 and was denoted by E. Therefore, if we form the matrix Q by selecting the last two columns of the formal adjoint of $\widetilde{E}$ and $\mathcal{F}$ denotes any left D-module (e.g., $\mathcal{F} = C^\infty(\mathbb{R}^3)$), then we obtain that the following underdetermined linear system of PDEs (a priori similar to the divergence operator in $\mathbb{R}^3$):

$$\mathcal{B} = \{(y_1 \quad y_2 \quad y_3)^T \in \mathcal{F}^3 \mid (\partial_1 - x_3)\, y_1(x) + \partial_2\, y_2(x) + \partial_3\, y_3(x) = 0\}$$

admits the following injective parametrization:

$$\begin{cases} y_1(x) = ((1 - \theta(v_1''))\,(\partial_2 + \partial_3))\,z_1(x) + ((1 - \theta(v_1''))\,(\partial_1 - x_3) + 1)\,z_2(x), \\ y_2(x) = (-\theta(v_2'')\,(\partial_2 + \partial_3) + 1)\,z_1(x) - \theta(v_2'')\,(\partial_1 - x_3)\,z_2(x), \\ y_3(x) = (-(1 + \theta(v_2''))\,(\partial_2 + \partial_3) + 1)\,z_1(x) - (1 + \theta(v_2''))\,(\partial_1 - x_3)\,z_2(x), \end{cases} \tag{31}$$

where z_1 and z_2 are arbitrary functions of $\mathcal{F}$, θ denotes the involution of $A_3(\mathbb{Q})$ and

$$v_1'' = (\partial_1 - \partial_3 + x_3 - 1)\,(\partial_2 + \partial_3), \quad v_2'' = -(\partial_1 - \partial_3 + x_3 - 1)\,(\partial_1 + x_3).$$

If we develop the expressions in (31), we can check that we have

$$\begin{cases} z_1(x) &= (-\partial_1^2 + \partial_1\,\partial_3 - x_3\,\partial_3 + (2\,x_3 - 1)\,\partial_1 + x_3 - x_3^2 + 1)\,y_2(x) \\ & \quad +(\partial_1^2 - \partial_1\,\partial_3 + x_3\,\partial_3 - (2\,x_3 - 1)\,\partial_1 + x_3^2 - x_3)\,y_3(x), \\ z_2(x) &= y_1(x) + (-\partial_3^2 + \partial_1\,\partial_2 - \partial_2\,\partial_3 + \partial_1\,\partial_3 + \partial_2 - (x_3 - 1)\,\partial_3 - x_2\,\partial_2 - 2)\,y_2(x) \\ & \quad +(\partial_3^2 - \partial_1\,\partial_2 + \partial_2\,\partial_3 - \partial_1\,\partial_3 + (x_3 - 1)\,\partial_3 + (x_3 - 1)\,\partial_2 + 2)\,y_3(x), \end{cases}$$

i.e., $\{z_1,\ z_2\}$ is a flat output/basis of the flat system $\ker_{\mathcal{F}}(R.)$/free left D-module M.

Remark 49. If we denote by $\mathbb{C}\{t\}$ the ring of convergent power series, it is known that every left ideal of the ring $D = \mathbb{C}\{t\}[\frac{\mathrm{d}}{\mathrm{d}t};\, \mathrm{id}_{\mathbb{C}\{t\}},\, \frac{\mathrm{d}}{\mathrm{d}t}]$ can be generated by two elements (Galligo (1985); Maisonobe and Sabbah (1993)). Two such generators can be found by means of a computation of a standard basis as is explained in Galligo (1985); Maisonobe and Sabbah (1993). However, we do not know whether D is *strongly simple*, namely, whether, for every v_1, v_2 and $v_3 \in D$, there exist a_1 and $a_2 \in D$, satisfying

$$D\,v_1 + D\,v_2 + D\,v_3 = D\,(v_1 + a_1\,v_3) + D\,(v_2 + a_2\,v_3).$$

If so, Corollary 47 also holds for the particular ring $D = \mathbb{C}\{t\}[\frac{\mathrm{d}}{\mathrm{d}t};\, \mathrm{id}_{\mathbb{C}\{t\}},\, \frac{\mathrm{d}}{\mathrm{d}t}]$. A system-theoretic interpretation of this last result would be that every controllable ordinary differential linear system with convergent power series coefficients and at least two inputs is flat (Corollary 47 already shows that this result is true for polynomial coefficients (see Quadrat and Robertz (2005) for more details)). This question will be studied in the future as well as the case of real analytic coefficients.

Corollary 47 shows that we now need to investigate when a stably free module of rank 1 over the algebras $D = A_n(k)$ or $B_n(k)$ is free. As was shown in Quadrat and Robertz (2005), the question of whether or not a given stably free module of rank 1 over the Weyl algebras $D = A_n(k)$ or $B_n(k)$ is free can be answered by using the concept of *minimal parametrization* (Chyzak et al., 2005; Pommaret and Quadrat, 1999b) and then by deciding whether the corresponding left ideal I of D is principal as D is a domain. M. Barakat and V. Levandovskyy (RWTH-Aachen, Germany) have recently pointed out to us that this last problem can be solved by computing a

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005

reduced Gröbner or minimal Janet basis of I. Indeed, since such a basis is unique (see, e.g., Kandri-Rody and Weispfenning (1990) and Levandovskyy (2005)), this basis consists of one element if and only if I is principal. Finally, if $Q \in D^{p\times 1}$ is a minimal parametrization of the stably free left D-module M of rank 1 and $M \cong D^{1\times p}\, Q$ is a principal left ideal of D generated by the element $P \in D \setminus \{0\}$, then $Q\, P^{-1} \in D^{p\times 1}$ defines an injective parametrization of the free left D-module $M = D^{1\times p}/(D^{1\times q}\, R)$ of rank 1.

We illustrate this remark on a relevant example in control theory (Sontag, 1998).

Example 50. Let us consider the system $\dot{x}(t) = t^k\, u(t)$, where $k \in \mathbb{Z}_{\geq 0}$, and define $D = A_1(\mathbb{Q})$, $R_k = \begin{pmatrix} \frac{\mathrm{d}}{\mathrm{d}t} & -t^k \end{pmatrix}$ and the left D-module $M_k = D^{1\times 2}/(D\, R_k)$. As R_k has full row rank, we know that M_k is stably free iff the left D-module $\widetilde{N} = D^{1\times q}/(D^{1\times p}\, \widetilde{R_k})$, where $\widetilde{R_k} = \begin{pmatrix} -\frac{\mathrm{d}}{\mathrm{d}t} & -t^k \end{pmatrix}^T$ is the formal adjoint of R_k, is the zero module (Chyzak et al., 2005; Pommaret and Quadrat, 1998). Using the definition of $\widetilde{N}$, we then obtain

$$\begin{cases} -\dot{\lambda} = 0, \\ -t^k\, \lambda = 0, \end{cases} \Rightarrow t^k\, \dot{\lambda} + k\, t^{k-1}\, \lambda = 0 \Rightarrow t^{k-1}\, \lambda = 0 \Rightarrow \cdots \Rightarrow \lambda = 0 \Rightarrow \widetilde{N} = 0.$$

Hence, the left D-module M_k is stably free for all $k \in \mathbb{Z}_{\geq 0}$. Now, we can prove that we have the following exact sequence:

$$0 \longrightarrow D \xrightarrow{.R_k} D^{1\times 2} \xrightarrow{.Q_k} D \longrightarrow D/(D^{1\times 2}\, Q_k) \longrightarrow 0, \quad Q_k = \begin{pmatrix} t^{k+1} \\ t\, \frac{\mathrm{d}}{\mathrm{d}t} + k + 1 \end{pmatrix}.$$

Since $P_k = D/(D^{1\times 2}\, Q_k)$ is a non-trivial torsion left D-module, the matrix Q_k is a minimal parametrization of M_k. See Chyzak et al. (2005) and Pommaret and Quadrat (1999b) for more details and algorithms. Hence, we obtain that

$$M_k = D^{1\times 2}/(D\, R_k) \cong D^{1\times 2}\, Q_k = D\, t^{k+1} + D\, \left(t\, \frac{\mathrm{d}}{\mathrm{d}t} + k + 1 \right),$$

showing that M_k is isomorphic to the left ideal I_k of D generated by t^{k+1} and $t\, \frac{\mathrm{d}}{\mathrm{d}t} + k + 1$. Using the fact that D is a domain, we obtain that M_k is a free left D-module iff I_k is a principal left ideal of D. However, we can prove that t^{k+1} and $t\, \frac{\mathrm{d}}{\mathrm{d}t} + k + 1$ form a reduced Gröbner basis (minimal Janet basis) of I_k iff $k \geq 1$, and thus, M_k is a stably free but not free left D-module when $k \geq 1$. When $k = 0$, we check that $I_0 = D\, t + D\, \left(t\, \frac{\mathrm{d}}{\mathrm{d}t} + 1 \right) = D\, t$ as we have $\frac{\mathrm{d}}{\mathrm{d}t}\, t = t\, \frac{\mathrm{d}}{\mathrm{d}t} + 1$. Hence, I_0 is a principal left ideal of D, and thus, M_0 is free.

Finally, we point out that we can also use the concept of *Krull dimension* of a non-commutative ring D to give an upper bound on the rank of stably free left D-modules for which they are free (see, e.g., McConnell and Robson (2000, Theorems 11.1.14 and 11.1.17)). For instance, any stably free left module M over the ring of differential time-delay operators D defined in (2) of Example 5 satisfying $\mathrm{rank}_D(M) \geq 3$ is free.

5. Conclusion

In this paper, we have shown how to use the concept of stable rank of a ring D in order to reduce the computation of bases of free left D-modules to Gaussian elimination. In the case of the Weyl algebras $D = A_n(k)$ or $B_n(k)$ over a field k of characteristic 0, using the recently developed constructive versions of the result of J.T. Stafford on the number of generators of left

D-ideals (Leykin, 2004; Hillebrand and Schmale, 2001; Stafford, 1978), Algorithm 4 gives an effective way of computing bases of stably free left D-modules of rank at least 2. This algorithm has been implemented in the package STAFFORD (Quadrat and Robertz, 2005–2007) developed under OREMODULES (Chyzak et al., 2007). Finally, it seems to us that Algorithm 4 is simpler and more tractable than the algorithm developed in Gago-Vargas (2003).

As noticed in Rouchon (2005), different injective parametrizations of a flat system can be obtained. This result is easily explained by the fact that there are different ways to obtain the elements $a_i \in D$ satisfying (20). In the Weyl algebra case, we have chosen to apply Stafford's result, i.e., Theorem 45, to the vector formed by the first two and the last component of the vector V_i defined in Algorithm 3. See Section 4.2 for more details. This is indeed a particular choice and Algorithm 3 can be optimized by firstly inspecting the components of V_i in order to get simpler $a_1, a_2 \in D$ satisfying (20). In particular, this means that some heuristics must be added in the implementation of Algorithm 3 in order to simplify and speed up the computation of the bases. Some of them have been implemented in STAFFORD (Quadrat and Robertz, 2005–2007), but much work in this direction still needs to be done in the future.

Another aspect which can be used in order to optimize Algorithm 4 is that it allows the use of more general transformations than the elementary ones. Indeed, an inspection of the proof of Theorem 40 shows that we only need that G is an invertible matrix over D, i.e., $G \in \mathrm{GL}(p, D)$. Algorithm 2 gives a general way to compute $E \in E(m, D)$ satisfying $E\,v = (1\ 0\ \ldots\ 0)^T$ for any stable vector $v \in U_c(m, D)$. But, in some particular cases, it is possible to find a simpler $E \in \mathrm{GL}(m, D)$ satisfying $E\,v = (1\ 0\ \ldots\ 0)^T$ which can avoid the multiplication by the factor $v_1' - 1 - v_m$ in (22), and thus, lower the order of the final basis. Much work must be done in order to optimize the time-consuming algorithms of J.T. Stafford's result developed in Leykin (2004) and Hillebrand and Schmale (2001).

All these questions will be studied in the future as well as their extension to different classes of Ore algebras (e.g., differential time-delay systems, multidimensional discrete systems). Applications of the different algorithms developed in this paper to control theory and, in particular, to the effective computation of flat outputs of flat linear systems over Ore algebras will be developed in forthcoming publications. Finally, it was recently shown in Cluzeau and Quadrat (2007) that the computation of bases of free modules (e.g., over the Weyl algebras or a commutative polynomial ring) played a central role in the *decomposition problem* of linear functional systems, i.e., in the computation of unimodular matrices transforming a given matrix of functional operators to a block-triangular or a block-diagonal one. Hence, the computation of bases of free modules should attract more attention in the symbolic computation community.

References

Buchberger, B., 2006. An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal. J. Symbolic Comput. 41 (3–4), 475–511. Ph.D. Thesis, English translation.

Chyzak, F., Quadrat, A., Robertz, D., 2005. Effective algorithms for parametrizing linear control systems over Ore algebras. Appl. Algebra Engrg. Comm. Comput. 16, 319–376.

Chyzak, F., Quadrat, A., Robertz, D., 2007. OREMODULES: A symbolic package for the study of multidimensional linear systems. In: Chiasson, J., Loiseau, J.-J. (Eds.), Applications of Time-Delay Systems. In: Lecture Notes in Control and Information Sciences, vol. 352. Springer, pp. 233–264. http://wwwb.math.rwth-aachen.de/OreModules.

Chyzak, F., Salvy, B., 1998. Non-commutative elimination in Ore algebras proves multivariate identities. J. Symbolic Comput. 26, 187–227.

Cluzeau, T., Quadrat, A., 2007. Factoring and decomposing a class of linear functional systems, Linear Algebra Appl. (in press).

Fabiańska, A., Quadrat, A., 2007. Applications of the Quillen–Suslin theorem to multidimensional systems theory. In: H. Park, G. Regensburger (Eds.), Gröbner Bases in Control Theory and Signal Processing, In: Radon Series on Computation and Applied Mathematics, vol. 3, de Gruyter (in press).

Fliess, M., Lévine, J., Martin, P., Rouchon, P., 1995. Flatness and defect of nonlinear systems: introductory theory and examples. Internat. J. Control 61, 1327–1361.

Gago-Vargas, J., 2003. Bases for projective modules in $A_n(k)$. J. Symbolic Comput. 36, 845–853.

Galligo, A., 1985. Some algorithmic questions on ideals of differential operators. In: EUROCAL'85, Vol. 2 (Linz, 1985). In: Lecture Notes in Comput. Sci., vol. 204. Springer, pp. 413–421.

Goursat, E., 1930. Sur une généralisation du problème de Monge. Ann. Fac. Sci. Math. Sci. Phys. Toulouse 22, 249–295.

Hadamard, J., 1901. Sur l'équilibre des plaques élastiques circulaires libres ou appuyées et celui de la sphère isotrope. Ann. Sci. Ecole Norm. Sup. 18, 313–342.

Hillebrand, A., Schmale, W., 2001. Towards an effective version of a theorem of Stafford. J. Symbolic Comput. 32, 699–716.

Janet, M., 1929. Leçons sur les systèmes d'équations aux dérivées partielles. Cahiers scientifiques IV. Gauthier-Villars.

Janet, M., 1971. P. Zervos et le problème de Monge. Bull. Sci. Math. 95, 15–26.

Kandri-Rody, A., Weispfenning, V., 1990. Non-commutative Gröbner bases in algebras of solvable type. J. Symbolic Comput. 9, 1–26.

Kredel, H., 1993. Solvable Polynomial Rings. Shaker, Aachen.

Lam, T. Y., 1999. Lectures on modules and rings. In: Graduate Texts in Mathematics, vol. 189. Springer.

Levandovskyy, V., 2005. Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. Ph.D. Thesis. University of Kaiserslautern.

Leykin, A., 2004. Algorithmic proofs of two theorems of Stafford. J. Symbolic Comput. 38, 1535–1550.

Lombardi, H., 2005. Dimension de Krull explicite. Applications aux théorèmes de Kronecker, Bass, Serre et Forster. Notes de cours, 14/07/05. http://hlombardi.free.fr/publis/publis.html.

Maisonobe, P., Sabbah, C., 1993. $\mathcal{D}$-modules cohérents et holonomes. In: Travaux en Cours, vol. 45. Hermann.

Malgrange, B., 1962. Systèmes à coefficients constants. In: Séminaire Bourbaki 1962–63. pp. 1–11.

McConnell, J.C., Robson, J.C., 2000. Noncommutative Noetherian Rings. American Mathematical Society.

Mounier, H., 1995. Propriétés des systèmes linéaires à retards: Aspects théoriques et pratiques. Ph.D. Thesis, University of Orsay.

Oberst, U., 1990. Multidimensional constant linear systems. Acta Appl. Math. 20, 1–175.

Polderman, J.W., Willems, J.C., 1998. Introduction to mathematical systems theory. A behavioral approach. In: Texts in Applied Mathematics, vol. 26. Springer.

Pommaret, J.-F., 2001. Partial Differential Control Theory. Kluwer.

Pommaret, J.-F., Quadrat, A., 1998. Generalized Bezout identity. Appl. Algebra Engrg. Comm. Comput. 9, 91–116.

Pommaret, J.-F., Quadrat, A., 1999a. Algebraic analysis of linear multidimensional control systems. IMA J. Math. Control Inform. 16, 275–297.

Pommaret, J.-F., Quadrat, A., 1999b. Localization and parametrization of linear multidimensional control systems. Systems Control Lett. 37, 247–260.

Pommaret, J.-F., Quadrat, A., 2003. A functorial approach to the behaviour of multidimensional control systems. Int. J. Appl. Math. Comput. Sci. 13, 7–13.

Pommaret, J.-F., Quadrat, A., 2004. A differential operator approach to multidimensional optimal control. Internat. J. Control 77, 821–836.

Quadrat, A., Robertz, D., 2005. On the blowing-up of stably free behaviours. In: Proceedings of CDC-ECC'05, Seville, Spain.

Quadrat, A., Robertz, D., 2005–2007. The Stafford project. http://wwwb.math.rwth-aachen.de/OreModules.

Rotman, J.J., 1979. An Introduction to Homological Algebra. Academic Press.

Rouchon, P., 2005. Sur une discussion avec Alban Quadrat à propos d'une lettre de Malgrange, 24/05/05. Note des Mines de Paris.

Sontag, E.D., 1998. Mathematical Control Theory. Deterministic Finite Dimensional Systems, 2nd edition. In: Texts in Applied Mathematics, vol. 6. Springer.

Stafford, J.T., 1978. Module structure of Weyl algebras. J. London Math. Soc. 18, 429–442.

Wood, J., 2000. Modules and behaviours in nD systems theory. Multidimens. Systems Signal Process. 11, 11–48.

Zervos, P., 1932. Le problème de Monge. In: Mémorial des Sciences Mathématiques, fasc. LIII. Gauthier-Villars.

Zerz, E., 2006. An algebraic analysis approach to linear time-varying systems. IMA J. Math. Control Inform. 23, 113–126.

Please cite this article in press as: Quadrat, A., Robertz, D., Computation of bases of free modules over the Weyl algebras. Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005