Journal of Symbolic Computation 46 (2011) 595–608

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases

Viktor Levandovskyy, Kristina Schindelar

Lehrstuhl D für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany

ARTICLE INFO

Article history:
Received 5 March 2009
Accepted 10 April 2010
Available online 13 October 2010

Keywords:
Matrix normal form
Non-commutative Gröbner basis
Matrix diagonalization over ring
Jacobson normal form
Ore localization

ABSTRACT

In this paper we present an algorithm for the computation of a diagonal form of a matrix over non-commutative Euclidean domain over a field with the help of Gröbner bases. We propose a general framework of Ore localizations of non-commutative G-algebras and show its merits and constructiveness. It allows us to handle, among others, common operator algebras with rational coefficients.

We introduce the splitting of the computation of a normal form (like the Jacobson form over simple domain) for matrices over Ore localizations into the diagonalization (the computation of a diagonal form of a matrix) and the normalization (the computation of the normal form of a diagonal matrix). These ideas are also used for the computation of the Smith normal form in the commutative case. We give a special algorithm for the normalization of a diagonal matrix over the rational Weyl algebra and present counterexamples to its idea over rational shift and q-Weyl algebras.

Our implementation of the algorithm in SINGULAR:PLURAL relies on the fraction-free polynomial strategy, details of which will be described in the forthcoming article. It shows quite an impressive performance, compared with methods which directly use fractions. In particular, we experience quite a moderate swell of coefficients and obtain uncomplicated transformation matrices. We leave questions on the algorithmic complexity of this algorithm open, but we stress the practical applicability of the proposed method to a large class of non-commutative algebras.

E-mail addresses: Viktor.Levandovskyy@math.rwth-aachen.de (V. Levandovskyy), Kristina.Schindelar@math.rwth-aachen.de (K. Schindelar).

0747-7171/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2010.10.009

1. Introduction

The existence and computation of normal forms of matrices over a ring is a fundamental mathematical question. The proof for the existence of a normal form is mainly constructive and can be turned into an algorithm. However, such a direct algorithm is not very efficient in general. Computer algebra focuses its attention on these kinds of problems, since they are of elementary interest but of high complexity.

In that sense nearly any computer algebra system is able to compute the Smith normal form for a matrix over a commutative principal ideal domain ($\mathbb{Z}$ or $K[x]$ for a field K). There are many textbooks giving a theoretical background, like for instance (Cohn, 1971; Newman, 1972).

We present a method, which is based on Gröbner bases. In Insua (2005), there is a Gröbner basis based algorithm for the computation of Smith normal form of a matrix with entries in $K[x]$. Despite the fact that this approach seems to be folklore, we were not able to find other references. We generalize this idea and use Gröbner bases in computation of diagonal forms for matrices.

In this paper we consider non-commutative skew polynomial rings. Such rings, among others, offer the possibility to describe time varying systems in Systems and Control theory (Zerz, 2007; Ilchmann and Mehrmann, 2006; Ilchmann et al., 1984). Many known operator algebras can be realized as skew polynomial rings or solvable polynomial rings (Kredel, 1993), some of them can be realized even as much easier Ore algebras (Chyzak and Salvy, 1998; Chyzak et al., 2007). However, general solvable polynomial rings are hard to tackle constructively (say, in a computer algebra system), while the class of Ore algebras of Chyzak and Salvy (1998) and Chyzak et al. (2007) is indeed restrictive.

Based on the PBW algebras (Bueso et al., 2003) also known as G-algebras (Levandovskyy, 2005; Greuel et al., 2006), in Section 2 we propose a new class of univariate skew polynomial rings, which are obtained as Ore localizations of G-algebras. This framework is powerful, convenient and constructive at the same time. Moreover, it is more general than the class of Ore algebras (with defining endomorphism σ being an automorphism) and allows algorithmic treatment of modules. In Proposition 2.2 and Theorem 2.6 several nice properties of such algebras (which are among other Noetherian domains with PBW basis) are established. We stress, that the computations in these algebras, especially Gröbner bases for modules, are algorithmic and, moreover, they can be done without using explicit fractions. It is important, that such algebras and computations in them can be realized in any computer algebra system, which can handle G-algebras or polynomial Ore algebras.

Our implementation uses the polynomial strategy (that is, we keep objects we work with fraction free). It has been released as the library `jacobson.lib` (Schindelar and Levandovskyy, 2009) for the computer algebra system Singular:Plural (Decker et al., 2009; Greuel et al., 2006). The algorithm and its components are described in the central Section 3.

The non-commutative analogue to the Smith form over a *simple* principal ideal domain is the Jacobson form Jacobson (1943) and Cohn (1971). The general normal form problem over a non-simple domain is computationally hard (as well as the Jacobson form) and not very well understood yet. We study these questions in Section 4.

We propose to split the process of obtaining a (strong) normal form into the computation of a diagonal form and the subsequent *normalization* of a given diagonal matrix into the normal form as soon as the latter is defined in the corresponding algebra. And, as will be seen in the article, the diagonalization process can be performed with the same algorithm for Ore localized G-algebras. On the contrary, the normalization algorithm depends on the given algebra, as we show in 4.4 and 4.5.

In Section 5 we compare our implementation with other available packages, which use fractions directly. Notably, in many examples our approach delivers much more compact results with small coefficients.

2. Algebras, localizations and their properties

The framework of this paper is based on skew polynomial rings that are principal ideal domains. An important subclass of skew polynomial rings constitute the so-called polynomial Ore rings. They are non-commutative rings possessing an endomorphism σ and a σ-derivation to define the commutation rule of two elements, that is giving the extension from commutative polynomial ring to

non-commutative. These kinds of rings are used in analyzing the structure of analytic equations, like linear ordinary or partial differential equations or partial shift or difference equations with rational or polynomial coefficients; see Example 2.3. The name is inspired by Øystein Ore, who introduced and studied these kinds of rings. These rings were also studied, for instance, in Chyzak and Salvy (1998) and McConnell and Robson (2001).
Let K be a field and A be a K-algebra. Further let $\sigma : A \to A$ be a ring endomorphism. Then the map $\delta : A \to A$ is called σ-**derivation**, if δ is K-linear and satisfies the skew Leibniz rule

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b \quad \text{for all } a, b \in A.$$

For a σ-derivation δ the ring $A[\partial; \sigma, \delta]$ consisting of all polynomials in ∂ with coefficients in A with the usual addition and a product defined by the commutation rule $\partial a = \sigma(a)\partial + \delta(a)$ for all $a \in A$ is called a **skew polynomial ring** or an **Ore extension** of A with ∂ subject to σ, δ.

It is easy to see that any non-zero element $a \in A[\partial; \sigma, \delta]$ can be written as $a = a_n\partial^n + \cdots + a_1\partial + a_0$, where $n \in \mathbb{N}_0$ and $a_i \in A$. We call n the **degree** of a.

In describing K-algebras via finite sets of generators G and relations R, we write $A = K\langle G \mid R\rangle = K\langle G\rangle/\langle R\rangle$. It means that A is a factor algebra of the free associative algebra, generated by G modulo the two-sided ideal, generated by R.

Example 2.1. (1) Let $A_* = K[x_1, \ldots, x_n], A = K(x_1, \ldots, x_n), \sigma := \mathrm{id}_A$ and $\delta := 0$. Then $A_*[\partial; \sigma, \delta] = K[x_1, \ldots, x_n, \partial]$ and $A[\partial; \sigma, \delta] = K(x_1, \ldots, x_n)[\partial]$.
(2) Let $\mathrm{char}\ K = 0, A = K[x], \sigma := \mathrm{id}_{K[x]}$ and $\delta := \frac{\partial}{\partial x}$. Then

$$W_1(K) := K[x][\partial; \sigma, \delta] = K\langle x, \partial \mid \partial x = x\partial + 1\rangle \text{ resp. } B_1(K) := K(x)\left[\partial; \mathrm{id}_{K(x)}, \frac{\partial}{\partial x}\right]$$

is called the first **polynomial** resp. **rational Weyl algebra**.

Proposition 2.2 (*Bueso et al., 2003*)**.** *Let A be a division ring, $\sigma : A \to A$ be an endomorphism and $R = A[\partial; \sigma, \delta]$ be an Ore extension with a σ-derivation δ.*
If σ is injective (respectively bijective), then

- *(PID) R is a left (resp. right) principal ideal domain.*
- *(Bezout's Theorem) For any non-zero $a, b \in R$ there exists a right (resp. left) greatest common divisor g_r (resp. g_ℓ) of a, b and there exist $s, t \in R$, such that $g_r = sa + tb$ (resp. s', t', such that $g_\ell = as' + bt'$).*
- *(ED) R is a left (resp. right) Euclidean domain.*

Hence, when σ is bijective, there are left and right Euclidean division algorithms. In the next example we enlist some skew polynomial rings (which are Ore algebras indeed; see Chyzak and Salvy (1998)). These rings are of great interest in applications, many of them can be addressed with our implementation; see Section 5.

Example 2.3. Let $\mathrm{char}\ K = 0, 0 \neq q \in K$ and $A = K(x)$.

- The first **rational difference algebra** is defined by

  $$\mathcal{S}_1 := A[\Delta; \sigma, \delta] = K(x)\langle\Delta \mid \Delta x = x\Delta + \Delta + 1\rangle,$$

  where $\sigma(p(x)) = p(x+1)$ and $\delta(p) = \sigma(p) - p$ for all $p \in K(x)$.
- Let $\sigma(p(x)) = p(qx)$ and $\delta := (\frac{\partial}{\partial x})_q, \delta(f(x)) = \frac{f(qx)-f(x)}{(q-1)x}$. Then

  $$W_1^q(K) := A\left[\partial; \sigma, \left(\frac{\partial}{\partial x}\right)_q\right] = K(x)\langle\partial \mid \partial x = q \cdot x\partial + 1\rangle$$

  is called the first **rational** q**-Weyl algebra**.
- The first **rational** q**-difference algebra** is defined by

  $$\mathcal{Q} := A[\partial; \sigma, \delta] = K(x)\langle\partial \mid q \cdot x\partial + (q-1)x\rangle,$$

  where $\sigma(p) = p(qx)$ and $\delta(p) = p(qx) - p(x)$.

Indeed, we can work within the more general algebraic framework as follows. Let S be a multiplicatively closed set (see McConnell and Robson (2001)) in a Noetherian integral domain A, such that $0 \notin S$. S is called an **Ore set** in A, if for all $s_1 \in S$, $a_1 \in A$ there exist $s_2 \in S$, $a_2 \in A$, such that $a_1 s_2 = s_1 a_2$. Then one can see, that formally (that is, allowing fractional expressions) $s_1^{-1} a_1 = a_2 s_2^{-1}$ holds.

Then one defines a **ring of fractions** or an **Ore localization** of A with respect to S to be a ring A_S (often denoted as $S^{-1}A$) together with an injective homomorphism $\phi : A \to A_S$, such that (i) for all $s \in S$, $\phi(s)$ is a unit in A_S and (ii) for all $f \in A_S, f = \phi(s)^{-1}\phi(a)$ for some $a \in A$, $s \in S$.

The Ore property of S in A guarantees, that any left-sided fraction can be written (non-uniquely!) as a right-sided fraction. Moreover, given $a_1, \ldots, a_m \in A$ and $s_1, \ldots, s_m \in S$, there exist $a'_1, \ldots, a'_m \in A$ and $s' \in S$, such that $a_i s' = s_i a'_i$ holds for each i. Thus there exist common right and common left multiples.

Remark 2.4. The question, whether two modules are isomorphic, is one of the fundamental questions in algebra. Any partial algorithmic answer to this question is of great importance, since this question is not algorithmic in general. Assume that there are finitely generated A-modules M, N and an A-module homomorphism $\varphi : M \to N$. If one finds an appropriate Ore set $\tilde{S}$ in A and proves that $\tilde{S}^{-1}\varphi : \tilde{S}^{-1}M \to \tilde{S}^{-1}N$ is not an isomorphism, it implies that $M \ncong N$ as A-modules. In contrast with common localizations of a commutative ring at a complement of prime ideal, we do not know a priori for which S we are looking for and how many different S should we examine.

Definition 2.5. Let A be a quotient of the free associative algebra $K\langle x_1, \ldots, x_n\rangle$ by the two-sided ideal I, generated by the finite set $\{x_j x_i - c_{ij} x_i x_j - d_{ij}\}$ for all $1 \le i < j \le n$, where $c_{ij} \in K^*$ and d_{ij} are polynomials in $x_1, \ldots, x_n$. Without loss of generality we can assume that d_{ij} are given in terms of standard monomials $x_1^{a_1} \ldots x_n^{a_n}$. A is called a *G-algebra* (Levandovskyy and Schönemann, 2003; Levandovskyy, 2005), if

- for all $1 \le i < j < k \le n$ the expression $c_{ik}c_{jk} \cdot d_{ij}x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik}x_j + d_{jk}x_i - c_{ij}c_{ik} \cdot x_i d_{jk}$ reduces to zero modulo I and
- there exists a monomial ordering $\prec$ on $K[x_1, \ldots, x_n]$, such that for each $i < j$, such that $d_{ij} \neq 0$, $\mathrm{lm}(d_{ij}) \prec x_i x_j$. Here, lm stands for the classical notion of leading monomial of a polynomial from $K[x_1, \ldots, x_n]$.

We call an ordering on a G-algebra **admissible**, if it satisfies the second condition of the definition. A G-algebra A is Noetherian integral domain (Levandovskyy and Schönemann, 2003), hence there exists its total two-sided ring of fractions $\mathrm{Quot}(A) = A_{A\setminus\{0\}}$, which is a division ring (a skew field). Assume that A is generated by $x_1, \ldots, x_{n+1}$ and suppose that the set $\Lambda_n(A) = \{\lambda = \{i_1, \ldots, i_n\} \mid i_1 < \cdots < i_n, K\langle x_{i_1}, \ldots, x_{i_n} \mid I_\lambda\rangle$ is a G-algebra$\}$ is not empty, where $I_\lambda = \{x_j x_i - c_{ij} x_i x_j - d_{ij} \mid i, j \in \lambda, i < j\}$. For any $\lambda = \{i_1, \ldots, i_n\} \in \Lambda_n$, let us define B_λ to be a G-algebra, generated by $\{x_{i_1}, \ldots, x_{i_n}\}$.

Theorem 2.6. *Let A be a G-algebra in variables $\{x_1, \ldots, x_n, \partial\}$ and assume that $\lambda = \{x_1, \ldots, x_n\} \in \Lambda_n$. Moreover, let $B := B_\lambda$ and $B^* = B \setminus \{0\}$. Suppose, that there exists an admissible monomial ordering $\prec$ on A, satisfying $x_k \prec \partial$ for all $1 \le k \le n$. Then*

- *B^* is a multiplicatively closed Ore set in A.*
- *$(B^*)^{-1}A$ (Ore localization of A with respect to B^*) can be presented as an Ore extension of* $\mathrm{Quot}(B)$ *by the variable ∂ by an algorithmic procedure.*

Proof. Since B is a G-algebra itself, it is an integral domain, hence B^* is multiplicatively closed and does not contain zero. Since A and B are G-algebras and $\prec$ is an admissible ordering, for a relation $\partial x_j = c_j x_j \partial + d_j$ with $c_j \in K^*$ and a polynomial $d_j \in A$ holds $d_j = 0$ or $\mathrm{lm}(d_j) \prec x_j \partial$. Since $x_j \prec \partial$, then $x_j \partial \prec \partial^2$, hence d_j is at most linear in ∂. Writing $d_j = a_j \cdot \partial + b_j$ for $a_j, b_j \in B$, we define $c'_j = c_j x_j + a_j$ and thus we obtain a relation $\partial x_j = c'_j \partial + b_j$, where $x_j, c'_j, b_j \in B$ and $c'_j \neq 0$.

Then, by defining $\sigma(x_j) = c_j x_j + a_j$ and $\delta(x_j) = b_j$ for all $1 \le j \le n$, we see that σ is an automorphism of $\mathrm{Quot}(B)$. Thus an Ore extension $\mathrm{Quot}(B)[\partial; \sigma, \delta]$ is indeed another presentation of $(B^*)^{-1}A$ as soon as B^* is an Ore set in A.

Since $\mathrm{lm}(d_j) = \mathrm{lm}(a_j\partial + b_j) \prec x_j\partial$, both $\mathrm{lm}(a_j) \prec x_j$ and $\mathrm{lm}(b_j) \prec x_j\partial$ hold. The latter implies, that there exist positive weights ω and $w_1, \ldots, w_n$ for variables $\{\partial, x_1, \ldots, x_n\}$, such that for $\mathrm{lm}(a_j) = x^\alpha$ and $\mathrm{lm}(b_j) = x^\beta$ one has $\sum_i w_i\alpha_i \leq w_j$ and $\sum_i w_i\beta_i \leq w_j + \omega$. In particular, this can be achieved by setting ω large enough. Then we follow the recipe from Bueso et al. (2003) and construct a block ordering from this setting. Consider an ordering $\prec_\partial$ on A, which is a block ordering for blocks of variables $\{\partial\}$, $\{x_1, \ldots, x_n\}$. It means that $\partial \gg x_j$ for all j, that is the variable ∂ is greater than any power of x_j. The second block is an ordering $\prec_B$ on B, for which $\mathrm{lm}(a_j) \prec_B x_j$ holds. For instance, one can take $\prec_B$ to be the restriction of $\prec$ to B. Then $\mathrm{lm}(d_j) = \max_{\prec_\partial}(a_j\partial, b_j) \prec_\partial x_j\partial$ holds, hence $\prec_\partial$ is an admissible ordering on A. From Proposition 28 of García García et al. (2009) (which holds for a much more general situation), the existence of such a block ordering as $\prec_\partial$ implies that the set B^* is an Ore set in A. □

Remark 2.7. Note that by construction $A_{B^*} := (B^*)^{-1}A$ is a Euclidean (principal ideal) domain by Proposition 2.2. In particular, all but one variables are invertible (we call them also *rational* variables). We say that non-invertible variables are of *polynomial* nature. In a more general setting, we like to present localizations of the type A_{B^*}, where B is a sub-G-algebra of A, as a ring of solvable type (Kredel, 1993) or, equivalently, as a PBW ring (Bueso et al., 2003). In the case of several polynomial variables, the analogue to Theorem 2.6 seems to be much more involved.

Example 2.8. To illustrate Theorem 2.6, consider the difference algebra $\mathcal{S}_1 := K\langle x, \Delta \mid \Delta x = x\Delta + \Delta + 1\rangle$. Since $\Delta \prec x\Delta$ is a consequence of $1 \prec x$ (we assume that we are dealing with well-orderings only), $\mathcal{S}_1$ can be localized at both $K[x]^*$ and $K[\Delta]^*$. However, the algebra, associated with the operator of partial integration $\mathcal{I}_1 := K\langle x, I \mid Ix = xI - I^2\rangle$ can be localized only at $K[I]^*$ but not at $K[x]^*$, since $I^2 \prec xI$ is a consequence of $I \prec x$ and any ordering, satisfying $x \prec I$ is not admissible for $\mathcal{I}_1$.

For many problems in module theory and in applications we would like to analyze complicated problems via localizing at large subalgebras. In the situation as above, we obtain a non-commutative Euclidean domain as the result, hence we are interested in computing a sort of normal form of a matrix in this setting. One of the complications, which arise in constructive handling of objects over such algebras, is quite hard arithmetics in the skew field. Several fundamental questions like the transformation of a left fraction into the right one (which is possible, since the Ore condition is satisfied), simplification of a one-sided fraction etc. require quite nontrivial and complex algorithms (like computation of syzygy modules and so on) to be used; see for instance Apel (1988). Even in the commutative case the computations (even with one variable) over a transcendental extension by several generators in practice are still nontrivial and resource consuming for most computer algebra systems. Hence saying "ring R is a (non-commutative) Euclidean domain" does not automatically mean "computations in R are easy".

3. Gröbner bases in the computation of a diagonal form

3.1. Yoga with Gröbner bases

Let us give a short introduction to non-commutative Gröbner basis theory, which has been studied by e.g. Chyzak (1998), Kredel (1993) and Levandovskyy (2005). Suppose, that there is a G-algebra R_* over a field K, which is generated by $x_1, \ldots, x_n, \partial$, such that $R_* = A_*[\partial; \sigma, \delta]$ is an Ore extension of a G-algebra A_*, generated by $\{x_i\}$. By using the lower index $*$, we point out that we deal with structures, objects which always have a polynomial presentation. A nice property of a G-algebra is that it has a K-basis, consisting of **monomials** of R_*

$$\mathrm{Mon}(R_*) = \{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}\partial^k \mid \alpha \in \mathbb{N}^n, k \in \mathbb{N}\} = \{x^\alpha\partial^k \mid x^\alpha \in \mathrm{Mon}(A_*), k \in \mathbb{N}\}.$$

Based on a module ordering we define leading coefficient (lc), leading monomial (lm), leading term (lt) and leading position (lpos) notions as usual. Let $e_i := (0, \ldots, 1, \ldots, 0)$ be the i-th unit vector.

In this paper we will compute Gröbner basis of modules over R_* with respect to position-over-term (POT) monomial module ordering. For $r, s \in \mathrm{Mon}(R_*)$,

$$re_i \prec se_j \Leftrightarrow i < j \text{ or if } i = j \text{ then } r \prec s, \tag{1}$$

and $r < s$ with respect to an admissible well-ordering on R_*, eliminating ∂, that is satisfying $\partial \gg x_n > \cdots > x_1$ on R_*.

In the localized ring $R = (A_* \setminus \{0\})^{-1}R_*$, a Gröbner basis is computed with respect to the induced POT ordering, which takes only degree of ∂ into account since $\mathrm{Mon}(R) = \{\partial^k \mid k \in \mathbb{N}\}$.

We call $a \in R_*$ a **strict left (resp. right) divisor** of $b \in R_*$ if and only if $\exists f \in R_*$ such that $af = b$ (resp. $fa = b$). Extending this notation to R_*^p requires that both elements $a, b \in R_*^p$ have the same leading position. Moreover, a is said to be a **proper** strict divisor of b, if either $b = af$ or $b = fa$ holds, where f is not a unit in R_*. For two monomials $m_1, m_2 \in R_*$ we write $m_1 \leq m_2$ for comparison with the fixed monomial ordering. We say that m_1 **divides** m_2, if each exponent of m_1 is not greater than the corresponding exponent of m_2. The monomials of R_*^p are $\{me_j \mid m \in \mathrm{Mon}(R_*),\ 1 \leq j \leq p\}$. We say that m_1e_i divides m_2e_j if and only if $i = j$ and m_1 divides m_2 in R_*.

Definition 3.1. Let M be a left submodule of R_*^p and $<$ be a monomial module ordering on R_*^p. A finite subset $G \subset M$ is called a **Gröbner basis** of M with respect to $<$, if for every $f \in M \setminus \{0\}$ there exists a $g \in G$, so that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$.

A Gröbner basis G is called **reduced** if and only if for any pair of polynomials $h \neq f \in G$, the leading monomial $\mathrm{lm}(h)$ does not divide any monomial of f. It can be shown, that a normalized (that is with leading coefficients 1) reduced Gröbner basis is unique for a fixed ordering. We recall the common property of a Gröbner basis to be, in particular, a generating set.

Remark 3.2. Let $M \subseteq R_*^p$ with a Gröbner basis G and $f \in M$. Define the submodule S of M to be generated by all $s \in G$ such that $\mathrm{lm}(s) \leq \mathrm{lm}(f)$. Then $f \in S$.

3.2. Working with left and right modules

Opposite algebra. In order to work with left and right modules over an associative K-algebra A, one has to use both A and its opposite algebra A^{op} in general. Recall, that A^{op} is the same vector space as A, endowed with the opposite multiplication: $\forall\, a, b \in A^{op}$, $a \star_{A^{op}} b = b \cdot a$. A natural opposing map makes from a right (resp. left) A-module a left (resp. right) A^{op}-module. There is an algorithmic procedure to set up an opposite algebra to a given G-algebra; see Levandovskyy (2005).

Involutive anti-automorphism. Alternatively, for "swapping sides" one can employ an anti-automorphism θ of A , that is a K-linear map, which obeys $\theta(ab) = \theta(b)\theta(a)$ for all $a, b \in A$, which is involutive, that is $\theta^2 = \mathrm{id}_A$. Often such an anti-automorphism is called **involution**. In classical operator algebras, particularly simple involutions are known (Chyzak et al., 2007). Moreover, it is possible to determine linearly presented involution of a G-algebra via an algorithm (Levandovskyy et al., unpublished, see Singular library `involut.lib` (Becker et al., 2003) for an implementation). A constructive advantage of using involution versus using opposite algebra lies in the fact, that one does not need to create opposite algebra and make an object its opposite. Instead, we apply an involution to an object and remain in the same ring. One application of involution means that the object we deal with changes its side from left to right or vice versa.

An involution can be extended to matrices as follows. Let $\theta : A \to A$ be an involution as above. We define the map $\widetilde{\theta} : A^{p\times q} \to A^{q\times p}$, $M \mapsto (\theta(M))^T$, where $\theta(M) = [\theta(M_{ij})]$ for $1 \leq i \leq p$ and $1 \leq j \leq q$. Then indeed $(\theta(B \cdot C))^T = (\theta(C))^T \cdot (\theta(B))^T$ for $B \in A^{p\times q}$, $C \in A^{q\times k}$. Applied twice, we get $B \cdot C$ back.

3.3. Diagonalization

Let R be a K-algebra and a non-commutative Euclidean PID. Recall, that a matrix $U \in R^{p\times p}$ is called **unimodular** if and only if there exists $U^{-1} \in R^{p\times p}$ such that $UU^{-1} = U^{-1}U = \mathrm{id}_{p\times p}$. Let $M \in R^{p\times q}$ and assume, without loss of generality, that $p > q$. Then there exist unimodular matrices $U \in R^{p\times p}$ and $V \in R^{q\times q}$ such that

$$UMV = \begin{bmatrix} m_1 & & 0 \\ & \ddots & \\ 0 & & m_q \\ & 0_{p-q} & \end{bmatrix}.$$

There are several ways to prove this statement, all based on the Euclidean (and thus PID) property of the underlying ring. From now on, we assume that R is a localization of a G-algebra as in Remark 2.7. We present an algorithm to compute a diagonal form together with unimodular transformation matrices via Gröbner bases. The main idea about the computation is the sequential alternation between the computation of a reduced Gröbner basis of the submodule, generated by, say, the rows of a matrix and acting by the involution $\widetilde{\theta}$ on a submodule. In the Ph.D. thesis (Insua, 2005) this idea was applied to $K[x]$ (of course, without using involution) in order to compute a Smith normal form.

In the following, by ${}_RM$ we denote the left R-module generated by the rows of a matrix M. Further on, by $\mathcal{G}({}_RM)$ we denote the reduced left Gröbner basis of the submodule, generated by ${}_RM$ with respect to the module ordering (1).

For the i-th row of a matrix M we write M_i and M_{ij}, as usual, for the entry in the i-th row and j-th column. With respect to the context we identify $\mathcal{G}({}_RM) = \{g_1, \ldots, g_m\}$ with the matrix $[g_1^t, \ldots, g_m^t]^t$. Define the **degree** of an element $0 \neq m \in R^{1\times q}$ to be the degree of the corresponding leading monomial, that is, $\deg(m) := \deg(\mathrm{lm}(m))$, which is the highest exponent in the variable ∂. Following standard convention, $\deg(0) = -\infty$. Note that the elements of $\mathcal{G}({}_RM)$ have pairwise distinct leading monomials, since they form a reduced Gröbner basis. In a reduced Gröbner basis $\mathrm{lm}(\mathcal{G}({}_RM)_i) \mid \mathrm{lm}(\mathcal{G}({}_RM)_j)$ if and only if $\mathcal{G}({}_RM)_i = \mathcal{G}({}_RM)_j$.

Lemma 3.3. *Order a reduced Gröbner basis in such a way that* $\mathrm{lm}(\mathcal{G}({}_RM)_1) < \cdots < \mathrm{lm}(\mathcal{G}({}_RM)_m)$. *Then* $[\mathcal{G}({}_RM)_1, \ldots, \mathcal{G}({}_RM)_m]^T$ *is a lower triangular matrix.*

Proof. Suppose the claim does not hold. Then there exist $\mathcal{G}({}_RM)_i$ and $\mathcal{G}({}_RM)_j$ with $\mathrm{lpos}(\mathcal{G}({}_RM)_i) = \mathrm{lpos}(\mathcal{G}({}_RM)_j)$ for $i < j$. Thus $\mathrm{lm}(\mathcal{G}({}_RM)_i) = \partial^{\alpha_i} e_k$ and $\mathrm{lm}(\mathcal{G}({}_RM)_j) = \partial^{\alpha_j} e_k$ such that $\alpha_i < \alpha_j$. But then evidently $\mathrm{lm}(\mathcal{G}({}_RM)_i)$ divides $\mathrm{lm}(\mathcal{G}({}_RM)_j)$, which is a contradiction to $\mathcal{G}({}_RM)$ being reduced. □

Due to the previous lemma, we may assume without loss of generality that the matrix $\mathcal{G}({}_RM)$ is lower triangular. Since R is an integral domain, we define the rank of a matrix M to be the rank of M over the field of fractions of R. Now, let us assume that $p = q$ and M is of full rank, that is row and column ranks of M are equal to p. The non-square case will be discussed in Remark 3.7.

Lemma 3.4. *Let* $\mathcal{I}$ *denote the left ideal generated by the elements in the last column of* $\widetilde{\theta}(\mathcal{G}({}_RM))$, *that is, by* $\theta(\mathcal{G}({}_RM)_{p1}), \ldots, \theta(\mathcal{G}({}_RM)_{pp})$. *Then*

$$\mathcal{I} = {}_R\langle\, \mathcal{G}({}_R\widetilde{\theta}(\,\mathcal{G}({}_RM)\,))_{pp}\,\rangle.$$

Proof. Note, that due to Lemma 3.3

$$\underbrace{\begin{bmatrix} * & & \\ \vdots & \ddots & \\ \mathcal{G}({}_RM)_{p1} & \cdots & \mathcal{G}({}_RM)_{pp} \end{bmatrix}}_{\mathcal{G}({}_RM)} \overset{\widetilde{\theta}}{\rightsquigarrow} \begin{bmatrix} & & \theta(\mathcal{G}({}_RM)_{p1}) \\ & \iddots & \vdots \\ * & \cdots & \theta(\mathcal{G}({}_RM)_{pp}) \end{bmatrix} \overset{\mathcal{G}}{\rightsquigarrow} \begin{bmatrix} * & & \\ \vdots & \ddots & \\ * & \cdots & \mathcal{G}({}_R\widetilde{\theta}(\,\mathcal{G}({}_RM)\,))_{pp} \end{bmatrix}.$$

According to the definition of $\mathcal{G}$ the left ideal generated by $\mathcal{G}({}_R\widetilde{\theta}(\,\mathcal{G}({}_RM)\,))_{pp}$ coincides with ${}_R\langle\theta(\mathcal{G}({}_RM)_{p1}), \ldots, \theta(\mathcal{G}({}_RM)_{pp})\rangle$. □

Now we can formulate the algorithm that yields the desired diagonal form.

Algorithm 3.5 (`Diagonalization with Gröbner Bases`)**.**
Input: $M \in R^{g\times g}$ of full rank, $\widetilde{\theta}$ involution as above.
Output: Matrices $U, V, D \in R^{g\times g}$, such that

$$U, V \text{ are unimodular and } U \cdot M \cdot V = \mathrm{Diag}(r_1, \ldots, r_g) = D.$$

$M^{(0)} \leftarrow M, U \leftarrow \mathrm{id}_{g\times g}, V \leftarrow \mathrm{id}_{g\times g}$
$i \leftarrow 0$
while ($M^{(i)}$ is not a diagonal matrix **or** $i \equiv_2 1$) **do**
  $i \leftarrow i + 1$
  Compute $U^{(i)}$ such that $U^{(i)} \cdot M^{(i-1)} = \mathcal{G}({}_RM^{(i-1)})$
  $M^{(i)} \leftarrow \widetilde{\theta}(\mathcal{G}({}_RM^{(i-1)}))$

if $(i \equiv_2 0)$ **then**
  $V \leftarrow V \cdot \widetilde{\theta}(U^{(i)})$
else
  $U \leftarrow U^{(i)} \cdot U$
end if
end while
return $(U, V, M^{(i)})$

Theorem 3.6. *The Algorithm 3.5 terminates and it is correct.*
*That is, for $M \in R^{g\times g}$, let $M^{(i)}$ denote the matrix we get after the i-th execution of the **while** loop. Then there exists an element $k \in \mathbb{N}$ such that $M^{(k)}$ is a diagonal matrix. If k is odd, then the **while** loop is repeated just one more time (define $l := k + (k \mod 2)$ in this case). The matrices U, V obtained in the last loop are unimodular and satisfy $UMV = \mathrm{Diag}(m_1, \ldots, m_g)$.*

Proof. We prove the claim by induction on g, the size of the square matrix M. For $g = 1$ there is nothing to show. Using Lemma 3.4, the equality ${}_R\langle\theta((M^{(i+1)})_{gg})\rangle = {}_R\langle(M^{(i)})_{1g}, \ldots, (M^{(i)})_{gg}\rangle$ holds. Hence we get

$${}_R\langle(M^{(i)})_{gg}\rangle \subseteq {}_R\langle\theta((M^{(i+1)})_{gg})\rangle \quad \text{for all } i.$$

Note that θ preserves the degree. Then the previous inclusion implies by degree arguments that ${}_R\langle(M^{(r)})_{gg}\rangle = {}_R\langle(M^{(r+1)})_{gg}\rangle$ for some r. Using Lemma 3.4 and $(M^{(r)})_{gg} \neq 0$ (since M is of full rank), we obtain that $(M^{(r)})_{gg}$ is a strict left divisor of $(M^{(r)})_{ig}$ for each $1 \leq i \leq g-1$. Then the definition of $\mathcal{G}$ yields that $M^{(r+1)} = M' \oplus (M^{(r+1)})_{gg}$, that is $M^{(r+1)}$ is a block matrix.

The $(g-1)\times(g-1)$ matrix M' can be transformed to a diagonal matrix via unimodular operations by induction. It remains to consider the transformation matrices U and V. For each $i \in \mathbb{N}$, after executing the **while** loop i times, we obtain

$$\begin{cases} M^{(i)} = U^{(i-1)} \cdot U^{(i-3)} \cdots U^{(1)} \cdot\ M\ \cdot \widetilde{\theta}(U^{(2)}) \cdot \widetilde{\theta}(U^{(4)}) \cdots \widetilde{\theta}(U^{(i)}), & \text{if } i \text{ is even} \\ M^{(i)} = U^{(i-1)} \cdot U^{(i-3)} \cdots U^{(1)} \cdot\ \widetilde{\theta}(M)\ \cdot \widetilde{\theta}(U^{(2)}) \cdot \widetilde{\theta}(U^{(4)}) \cdots \widetilde{\theta}(U^{(i)}), & \text{if } i \text{ is odd,} \end{cases}$$

which completes the proof. □

Remark 3.7. In order to extend Theorem 3.6 and Algorithm 3.5 to non-square and non-full rank matrices, we need to add suitable syzygies to U respectively V and zero rows respectively columns to the diagonal matrix, in order to maintain the initial size of M. For a computational solution it is sufficient to extend Algorithm 3.5 in the following way. Let $M^i \in R^{s\times t}$ where either $s = p, t = q$ or $s = q, t = p$ in the i-th while loop. Instead of computing U^i, satisfying $U^i \cdot M^{i-1} = \mathcal{G}({}_RM^{i-1})$, we compute $\mathcal{G}({}_R\tilde{M})$ for the extended matrix $\tilde{M} := [\mathrm{id}_{s\times s}\, M^{i-1}]$, which is obviously a full row rank matrix. Defining $U^i := [\mathcal{G}({}_R\tilde{M})_1^T, \ldots, \mathcal{G}({}_R\tilde{M})_s^T]^T$ and $M^i := [\mathcal{G}({}_R\tilde{M})_{s+1}^T, \ldots, \mathcal{G}({}_R\tilde{M})_t^T]^T$, it is easy to see that $U^iM^{i-1} = M^i$. The matrix M^i consists of the rows of $\mathcal{G}({}_RM^{i-1})$ and additional zero rows, such that $M^i \in R^{s\times t}$.

Example 3.8. Suppose $R = K(x)[\partial; \mathrm{id}, \frac{d}{dx}]$ and $R_* = K[x][\partial; \mathrm{id}, \frac{d}{dx}]$. Let us define an involution on R_* by $\theta(\partial) = -\partial$ and $\theta(x) = x$. Let

$$M = \begin{bmatrix} \partial^2 - 1 & \partial + 1 \\ \partial^2 + 1 & \partial - x \end{bmatrix} \in R^{2\times 2}.$$

Evidently $T = \mathrm{id}_{2\times 2}$ and thus $M^{(0)} := M$, $U = V = \mathrm{id}_{2\times 2}$ and $i = 0$.

1: Since $M^{(0)}$ is not diagonal, go into the while loop

- $i \leftarrow 1$. Since $\begin{bmatrix} -(x+1)\partial + x^2 + x + 1 & (x+1)\partial + x \\ \partial - x & -\partial - 1 \end{bmatrix} M^{(0)} = \mathcal{G}({}_{R_*}M^{(0)})$
  where $\mathcal{G}({}_{R_*}M^{(0)}) = \begin{bmatrix} (x+1)^2\partial^2 + 2(x+1)\partial - x^2 - 1 & 0 \\ -(x+1)\partial^2 - 2\partial + x - 1 & 1 \end{bmatrix}$ and $i \equiv_2 1$

$$M^{(1)} \leftarrow \begin{bmatrix} (x+1)^2\partial^2 + 2(x+1)\partial - x^2 - 1 & -(x+1)\partial^2 + x - 1 \\ 0 & 1 \end{bmatrix}$$
$$U \leftarrow \begin{bmatrix} -(x+1)\partial + x^2 + x + 1 & (x+1)\partial + x \\ \partial - x & -\partial - 1 \end{bmatrix}.$$

2: Since $M^{(1)}$ is not diagonal, go into the while loop

- $i \leftarrow 2$. Since $\begin{bmatrix} 1 & (x+1)\partial^2 - x + 1 \\ 0 & 1 \end{bmatrix} M^{(1)} = \mathcal{G}_{(R_*}M^{(1)})$ and $i \equiv_2 0$

$$M^{(2)} \leftarrow \begin{bmatrix} (x+1)^2\partial^2 + 2(x+1)\partial - x^2 - 1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$V \leftarrow \begin{bmatrix} 1 & 0 \\ (x+1)\partial^2 + 2\partial - x + 1 & 1 \end{bmatrix}.$$

3: Since i is even and $M^{(2)}$ is diagonal, the algorithm returns U and V. Thus

$$UMV = \begin{bmatrix} (x+1)^2\partial^2 + 2(x+1)\partial - x^2 - 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

4. Jacobson form

Let R be a left and right Euclidean domain. Inspired by the Smith form, we will focus on how to sharpen the result of the already discussed diagonal form.

Theorem 4.1 (*Cohn, 1971*; *Jacobson, 1943*)**.** *Every matrix $M \in R^{g\times q}$ is associated to a certain diagonal matrix, namely* $\mathrm{Diag}(m_1, \ldots, m_\ell, 0, \ldots, 0)$ *such that additionally*

$$Rm_{i+1}R \subseteq m_iR \cap Rm_i \tag{2}$$

holds for all $i = 1, \ldots, \min\{g, q\} - 1$.

Due to Jacobson (1943, Theorem 31) the elements m_i are unique up to similarity. Two elements m_i and n_i are called **similar** if and only if there exist $a, b \in R$ such that

$$am_i = n_ib, \qquad R = aR + n_iR, \qquad R = Rb + Rm_i.$$

Using the notation of the previous theorem, we call $\mathrm{Diag}(m_1, \ldots, m_\ell, 0, \ldots, 0)$ a **Jacobson normal form** of M. Note that (2) is hard to tackle constructively in general, since it requires to work with the intersection of a left and a right ideal. This difficulty disappears if R has only trivial two-sided ideals, that is when R is simple. Then each matrix M possesses a Jacobson form $\mathrm{Diag}(1, \ldots, 1, m_M, 0, \ldots, 0)$ with $m_M \in R$.

Lemma 4.2. *Let A_* be a G-algebra, $A = \mathrm{Quot}(A_*)$ and $R = A[\partial; \sigma, \delta]$. Let U, V be unimodular and $a, b, c, d \in R \setminus \{0\}$ such that*

$$U\mathrm{Diag}(a, b)V = \mathrm{Diag}(c, d). \tag{3}$$

Then $\deg(a) + \deg(b) = \deg(c) + \deg(d)$.

Proof. Due to (3) there exists a R-module isomorphism

$$\phi : R/aR \oplus R/bR \to R/cR \oplus R/dR.$$

Since A is a skew field, ϕ induces an A-vector space isomorphism. Thus the A-dimensions of $R/aR \oplus R/bR$ and $R/cR \oplus R/dR$, which are nothing else that the sums of degrees, coincide. □

Of course, inductive argument implies that sums of degrees of diagonal entries of two diagonal presentation matrices of the same module are the same.

Jacobson normal form in the first Weyl algebra. Let R be the rational Weyl algebra $K(x)[\partial; 1, \frac{\partial}{\partial x}]$, which is a simple domain.

Lemma 4.3. *Consider $a, b \in R$ with $\deg(a) > 0$, $b \neq 0$ and $\deg(b) \geq \deg(a)$. Then there exists $i \in \{0, \ldots, \deg(b) - \deg(a) + 1\}$ such that a is not a strict right divisor of bx^i.*

Proof. Suppose that for every $i \in \{0, \ldots, \deg(b) - \deg(a) + 1\}$ there exists a $q_i \in R$ such that $bx^i = q_i a$. Let $b = b_n(x)\partial^n + \cdots + b_1(x)\partial + b_0(x)$. Note, that for any $k \in \mathbb{N}$ the equality $\partial^k x = x\partial^k + k\partial^{k-1}$. Thus we define $r_1 := bx - xb = \sum_{i=1}^{n} b_i(x) i \partial^{i-1}$ with $\deg(r_1) = n - 1 < \deg(b)$ and $r_1 \neq 0$ since $\deg(b) \geq 1$. Since $b = q_0 a$ and $bx = q_1 a$, it follows that $r_1 = bx - xb = (q_1 - q_0 x)a$, that is a is a strict right divisor of r_1. By proceeding with bx^2 and so on, we obtain a sequence of non-zero polynomials r_i, such that $\deg(b) > \deg(r_1) > \cdots$ and a is a strict right divisor of r_i. Since the degree of r_i decreases exactly by 1 at each step, after at most $\deg(b) - \deg(a) + 1$ iterations we obtain a polynomial of degree $\deg(a) - 1$, which is non-zero. Such a polynomial must contain a right factor of degree $\deg(a)$, which is a contradiction. □

Lemma 4.3 suggests an algorithm to compute the Jacobson form from a diagonal matrix over the rational Weyl algebra. Suppose $M \in R^{g \times q}$, where $g = q = 2$. The extension to $g, q \in \mathbb{N}$ is evident. Algorithm 3.5 returns unimodular matrices U, V such that $UMV = \mathrm{Diag}(m_1, m_2)$. Without loss of generality, assume that $\deg(m_2) \leq \deg(m_1)$.

(1) If m_2 is a unit, we get the Jacobson form just by replacing U by $\mathrm{Diag}(1, m_2^{-1})U$. Otherwise, choose an exponent $i \in \mathbb{N}$ (it exists by Lemma 4.3) such that $m_1 x^i = a m_2 + b$ with $\deg(b) < \deg(m_2)$ and $b \neq 0$. Then

$$\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m_1 & 0 \\ 0 & m_2 \end{bmatrix} \cdot \begin{bmatrix} 1 & x^i \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 & b \\ 0 & m_2 \end{bmatrix}.$$

Replace U by $\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} U$ and V by $V \begin{bmatrix} 1 & x^i \\ 0 & 1 \end{bmatrix}$.

(2) Apply Algorithm 3.5 to the matrix $\begin{bmatrix} m_1 & r \\ 0 & m_2 \end{bmatrix}$. Its result is $\mathrm{Diag}(m_1', m_2')$, where $\deg(m_2') < \deg(m_2)$.

Thus, by iterating (1) and (2) we compute U and V, such that $UMV = \mathrm{Diag}(1, m_M)$.
It seems to us, that the process of obtaining Jacobson normal form from an appropriate diagonal matrix can be generalized to any constructive simple Euclidean PID. Moreover, applied to a matrix over non-simple domain, one can expect some simplification, depending on the input matrix.

Example 4.4. Over the first rational shift algebra $A = K(t)\langle s \mid st = ts + s\rangle$ (which is a not a simple domain), we provide a counterexample for a statement, similar to 4.3. Consider the 2×2 diagonal matrix $D_1 = \mathrm{Diag}(s, s)$. Then the left module $M_1 = A^2/A^2 D_1$ (it is of dimension 2 over $K(t)$) is annihilated by the two-sided ideal $\langle s\rangle$ and hence D_1 is not equivalent to a matrix of the form $D_2 = \mathrm{Diag}(1, p)$. If it were so, by defining $M_2 = A^2/A^2 D_2$, we see that $\mathrm{lm}(p) = s^2$ due to the $K(t)$-dimension of M_1. Since $M_2 = A^2/A^2\mathrm{Diag}(1, p) \cong A/Ap$, we have $\mathrm{Ann}_A M_2 = \langle p\rangle$. Since it is not equal to $\mathrm{Ann}_A M_1 = \langle s\rangle$, $M_1 \ncong M_2$. Hence, unlike over the Weyl algebra (or a simple domain as in Cohn (1971)), there are many different types of diagonal normal forms.

Example 4.5. Consider the rational q-Weyl algebra, cf. 2.3 and define $f = (q-1)\partial + x^{-1}$. The algebra is not simple since e.g. the ideal $\langle f\rangle$ is a proper two-sided ideal. By the same argumentation as in the previous example we can show that $\mathrm{Diag}(f, f)$ is not equivalent to any matrix of the type $\mathrm{Diag}(1, g)$.

Since little is known about normal forms of non-simple domains, this approach is very interesting to investigate in the future.

5. Examples, applications and comparison

Implementations of Jacobson normal form. To the best of our knowledge, Jacobson normal form algorithm has been implemented in Maple by Culianez and Quadrat (2005), by Blinkov et al. (2003);

Chyzak et al. (2007), by Middeke (2008) and by Beckermann et al. (2002), Cheng and Labahn (2007) and Davies et al. (2008).

We could not locate the download version of the implementation of Culianez and Quadrat (2005). The packages FFReduce (Beckermann et al., 2002) and MODReduce (Cheng and Labahn, 2007) are available via personal request to their authors. The implementation of Middeke (2008) was, according to its author, merely a check of ideas and was not supposed to become a freely distributed package for MAPLE. This package is able to compute in the first Weyl algebra with coefficients in a differential field.

D. Robertz informed us, that his publicly available implementation (Blinkov et al., 2003) directly follows the classical algorithm and it has not been specially optimized. Nevertheless, in what follows, we compare our implementation with the one in the MAPLE package JANET (Blinkov et al., 2003) on some nontrivial examples.

In packages by H. Cheng et al. modular (MODReduce) and fraction-free (FFReduce) versions of an order basis of a polynomial matrix M from an Ore algebra A are implemented. In particular, such a basis is used to compute the left nullspace of M, and indirectly the Popov form of M.

Our implementation. A drawback of applying Gröbner bases directly in $R = A[\partial; \sigma, \delta]$ (that is, having *rational coefficients*) lies in the complicated arithmetics with respect to the invertible elements. It will cause more trouble as soon as the number of variables of A grows. There is, however, a recipe to partially overcome these difficulties, widely used in commutative algebra. This is called "polynomial strategy" and originates from the work of Gianni et al. (1988). By extracting content instead of division by invertible elements, one can keep the whole Gröbner basis computation on the fraction-free level. We follow this idea and compute a special reduction of Gröbner basis with respect to a monomial ordering from Theorem 2.6 in a polynomial ring $R_* = A_*[\partial; \sigma, \delta]$. The details of this method will appear in the forthcoming article.

Example 5.1. Consider a double pendulum with lengths ℓ_1 and ℓ_2. Thus ℓ_1, ℓ_2 and g are constants, that is non-zero elements of K (for details see Culianez and Quadrat (2005), Example 3.2.2). The linearization of this problem leads to the system of linear partial differential equations in $\partial = \frac{\partial}{\partial t}$, which can be written in the matrix form with the matrix

$$M = \begin{bmatrix} \ell_1\partial^2 + g & 0 & -g \\ 0 & \ell_2\partial^2 + g & -g \end{bmatrix}.$$

Since the variable t does not appear in M, the ground ring for the diagonalization process can be thought of as $A = \mathbb{Q}(g)(\ell_1, \ell_2)[\partial]$. Thus, indeed one can compute the Smith normal form. Our implementation of the diagonal form of M on this example returns

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & g(\ell_1 - \ell_2) & 0 \end{bmatrix} = UMV, \qquad U = \begin{bmatrix} -1/g & 0 \\ -1/g & 1/g \end{bmatrix},$$

$$V = \begin{bmatrix} 0 & g\ell_2 & -g\ell_2\partial^2 - g^2 \\ 0 & g\ell_1 & -g\ell_1\partial^2 - g^2 \\ 1 & \ell_2(\ell_1\partial^2 + g) & -\ell_1\ell_2\partial^4 - g\ell_1 - g\ell_2\partial^2 - g^2 \end{bmatrix}.$$

This result agrees with results, obtained in Culianez and Quadrat (2005). Note, that a purely fractional method (as well as coefficient normalization procedure) will return 1 instead of $g(\ell_1 - \ell_2)$. With our polynomial approach we obtain a polynomial matrix, which is useful for further investigations. In particular, in the current example we see that setting $\ell_1 = \ell_2$ implies the drop of the rank of the Smith form from 2 to 1, thus the properties of the corresponding system will change. In control theory one establishes quite different properties of the module in the non-generic case $\ell_1 = \ell_2$.

Remark 5.2. In Levandovskyy and Zerz (2007) the algorithm for finding the so-called "obstructions to genericity" was derived and discussed. A lesson learned from that paper can be applied for an implementation of Jacobson (and hence Smith) form as follows. We propose to split the algorithm (resp. the implementation) into two parts. In the first part one computes a diagonal matrix, where the invertibles of the ground ring are not canceled artificially. The second part applies the normalization

on the invertibles; this part is rather trivial to achieve. Note, that our polynomial algorithm allows one to keep a close track on suspicious invertibles due to this scheme.

Example 5.3. Over the first rational Weyl algebra $\mathbb{Q}(t)[\partial; \mathrm{id}, \frac{d}{dt}]$, consider the matrix

$$R = \begin{bmatrix} \partial^2 & \partial + 1 & 0 \\ \partial + 1 & 0 & \partial^3 - t^2\partial \\ 2\partial + 1 & \partial^3 + \partial^2 & \partial^2 \end{bmatrix}.$$

An implementation of the Jacobson normal form returns the matrix $D = \mathrm{Diag}(g, 1, 1)$ together with transformation matrices $U, V \in \mathbb{Q}(t)[\partial; \mathrm{id}, \frac{d}{dt}]^{3\times 3}$ such that $URV = D$. Below, we write down just the leading term of each matrix entry and the number of lower order terms ("l.o.t."). Moreover, since the matrices U and V look similar, we show U only. The implementation of the fraction-free version of Algorithm 3.5 in Singular returns $D = \mathrm{Diag}(2t^2d^8 + 33 \text{ l.o.t.}, 1, 1)$. The left transformation matrix is

$$U = \begin{bmatrix} \frac{1}{2}t\partial^{13} + 24 \text{ l.o.t.} & \frac{1}{2}t\partial^{10} + 19 \text{ l.o.t.} & \frac{1}{2}t\partial^{11} + 44 \text{ l.o.t.} \\ \frac{1}{2} & 0 & 0 \\ -\frac{1}{4}\partial^5 + 2 \text{ l.o.t.} & -\frac{1}{4}\partial^2 & \frac{1}{4} + 2 \text{ l.o.t.} \end{bmatrix}.$$

Janet returns a matrix $\mathrm{Diag}(1, 1, (279936t^{14} + 14 \text{ l.o.t.})^{-1}(279936t^{14}\partial^8 + 145 \text{ l.o.t.}))$,

$$U = \begin{bmatrix} 1 & 0 & 0 \\ (6t^2 + 2 \text{ l.o.t.})^{-1}(\partial^2 + 1 \text{ l.o.t.}) & (6t^2 + 2 \text{ l.o.t.})^{-1}(\partial^3 + 3 \text{ l.o.t.}) & (6t^2 + 2 \text{ l.o.t.})^{-1} \\ u_{31} & u_{32} & u_{33} \end{bmatrix},$$

where $g = (559872t^{14} + 14 \text{ l.o.t.})$, $u_{31} = g^{-1}(-279936t^{14}\partial^9 + 158 \text{ l.o.t.})$, $u_{32} = g^{-1}(279936t^{14}\partial^{10} + 182 \text{ l.o.t.})$, $u_{33} = g^{-1}(279936t^{14}\partial^7 + 127 \text{ l.o.t.})$.

Application. Over R, the decomposition as above can be applied as follows. We start with a system of equations $M\omega = 0$ in unknown functions $\omega = (\omega_1, \ldots, \omega_p)$. Since U and V are unimodular over R and $UMV = \mathrm{Diag}(d_{11}, \ldots, d_{pp})$, we obtain a decoupled system $\{d_{ii}z_i = 0\}$, where $z = V^{-1}\omega$, which is equivalent to $M\omega = 0$ over R. Note, that $d_{ii} = 0$ is possible, then one calls z_i a free variable of the system in the literature. Clearly the decoupling, provided by a diagonal form, is of great importance for solving systems of operator equations with rational coefficients and for the structural analysis, performed in the algebraic system and control theory (see e.g. Theorem 8 of Zerz (2006)).

6. Conclusion and future work

Indeed, this paper is a part of a general program on providing effective computations within Ore localized G-algebras. Notably, polynomial strategy, which will be described in details in the forthcoming paper, is one of the key elements of the program. There is ongoing work on the implementation of Gröbner bases for Ore localized G-algebras under the codename Singular::Locapal.

We have proposed to apply the diagonalization not only over natural Euclidean Ore domains as in Examples 2.1 and 2.3, but also over large localizations of polynomial non-commutative algebras. Notably, as soon as there is an implementation of Gröbner bases for modules (and hence syzygies) over a G-algebra A, under some mild assumptions one is able to work effectively with and over Ore localization A_{B^*} of A with respect to a multiplicatively closed Ore set $B^* = B \setminus \{0\}$, where B is a suitable G-subalgebra of A (cf. Theorem 2.6). This allows us to tackle practical problems for many important algebras effectively with the machinery, previously used as Jacobson form over simple domains.

Our implementation of the Jacobson normal form will be developed further to provide a user with the possibility to compute in more general algebras. At the moment, the stable version of the library (Schindelar and Levandovskyy, 2009) supports first rational Weyl, shift and difference algebras. Investigation of normal forms over non-simple domains (as in 4.4, 4.5) is an important future task.

Middeke (2008) has reported, that the classical algorithm, computing Jacobson form of a matrix over the Weyl algebra over a differential field is polynomial time. However, it seems to us (due to the polynomial strategy approach) that the subalgebra of invertible elements must be involved in

the complexity analysis. Perhaps one should consider different models for studying complexity, since experience with practical applications suggests, that the important role, played by the coefficient arithmetics (which is not the arithmetics over a numerical field anymore!) must be appropriately reflected in the overall complexity. Otherwise the complexity of operations over the skew field of invertible elements remains hidden.

Recently, Mark Giesbrecht and George Labahn suggested the use of another technique from Kaltofen et al. (1989), namely the randomization. Starting with a matrix M, one multiplies M with random square (hence unimodular) matrices from both sides, in order to reduce the number of iterations in Algorithm 1. Some experiments confirm that this might be generalized to the setting of localized G-algebras. However, in practice the computations become much harder to deal with due to increased size of polynomials. This is another reason for our proposal to investigate the different notions of complexity of operations over skew fields.

We work on the next paper, where we will give all the details on the polynomial strategy, more details of implementation, examples over non-simple domains, cyclic vector method and investigations of R_*-unimodularity of transformation matrices.

Acknowledgements

We are very grateful to Eva Zerz and Hans Schönemann for their advice on numerous aspects of the problems treated in this article. We thank Daniel Robertz, Johannes Middeke and Howard Cheng for explanations about respective implementations. The anonymous referees helped us a lot with their insightful remarks and suggestions.

References

Apel, J., 1988. Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung. Dissertation, Universität Leipzig.

Becker, M., Levandovskyy, V., Yena, O., 2003. A Singular 3.0 library for computations and operations with involutions `involut.lib`. URL: www.singular.uni-kl.de.

Beckermann, B., Cheng, H., Labahn, G., 2002. Fraction-free row reduction of matrices of skew polynomials. In: Mora, T. (Ed.), Proc. of the International Symposium on Symbolic and Algebraic Computation, ISSAC'02. ACM Press, pp. 8–15.

Blinkov, Y.A., Cid, C.F., Gerdt, V.P., Plesken, W., Robertz, D., 2003. The MAPLE package "janet": II. Linear partial differential equations. In: Proceedings of the 6th International Workshop on Computer Algebra in Scientific Computing. pp. 41–54. URL: http://wwwb.math.rwth-aachen.de/Janet.

Bueso, J., Gómez-Torrecillas, J., Verschoren, A., 2003. Algorithmic methods in non-commutative algebra. In: Applications to Quantum Groups. Kluwer Academic Publishers.

Cheng, H., Labahn, G., 2007. Modular computation for matrices of Ore polynomials. In: Computer Algebra 2006: Latest Advances in Symbolic Algorithms. pp. 43–66.

Chyzak, F., 1998. Gröbner bases, symbolic summation and symbolic integration. In: Buchberger, B., Winkler, F. (Eds.), 33 Years of Gröbner Bases. In: LMS LNS, vol. 251. Cambridge University Press, pp. 32–60.

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: LNCIS, vol. 352. Springer, pp. 233–264. URL: 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 (2), 187–227.

Cohn, C., 1971. Free Rings and their Relations. Academic Press.

Culianez, G., Quadrat, A., 2005. Formes de Hermite et de Jacobson: implementations et applications. Tech. rep., INRIA Sophia Antipolis.

Davies, P., Cheng, H., Labahn, G., 2008. Computing Popov form of general Ore polynomial matrices. In: Proceedings of the Milestones in Computer Algebra (MICA) Conference. pp. 149–156.

Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2010. Singular 3-1-2 — a computer algebra system for polynomial computations. URL: http://www.singular.uni-kl.de.

García García, J.I., García Miranda, J., Lobillo, F.J., 2009. Elimination orderings and localization in PBW algebras. Linear Algebra Appl. 430 (8–9), 2133–2148.

Gianni, P., Trager, B., Zacharias, G., 1988. Gröbner bases and primary decomposition of polynomial ideals. J. Symbolic Comput. 6 (2–3), 149–167.

Greuel, G.-M., Levandovskyy, V., Schönemann, H., 2006. Plural. A Singular 3.0 subsystem for computations with non-commutative polynomial algebras. Centre for Computer Algebra, University of Kaiserslautern. URL: http://www.singular.uni-kl.de.

Ilchmann, A., Mehrmann, V., 2006. A behavioral approach to time-varying linear systems. I: general theory. SIAM J. Control Optim. 44 (5), 1725–1747.

Ilchmann, A., Nürnberger, I., Schmale, W., 1984. Time-varying polynomial matrix systems. Int. J. Control 40, 329–362.

Insua, M.A., 2005. Varias perspectives sobre las bases de Gröbner: Forma normal de Smith, Algoritme de Berlekamp y álgebras de Leibniz. Ph.D. thesis, Universidade de Santiago de Compostela, Spain.

Jacobson, N., 1943. The Theory of Rings. American Mathematical Society.
Kaltofen, E., Krishnamoorthy, M.S., Saunders, B.D., 1989. Mr. Smith goes to Las Vegas: randomized parallel computation of the Smith normal form of polynomial matrices. In: Davenport, J.H. (Ed.), Proc. EUROCAL'87. In: LNCS, vol. 378. Springer, pp. 317–322.
Kredel, H., 1993. Solvable Polynomial Rings. Shaker.
Levandovskyy, V., 2005. Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. Ph.D. thesis, Universität Kaiserslautern. URL: http://kluedo.ub.uni-kl.de/volltexte/2005/1883/.
Levandovskyy, V., Schönemann, H., 2003. Plural — a computer algebra system for noncommutative polynomial algebras. In: Proc. of the International Symposium on Symbolic and Algebraic Computation, ISSAC'03. ACM Press, pp. 176–183. URL: http://doi.acm.org/10.1145/860854.860895.
Levandovskyy, V., Zerz, E., 2007. Obstructions to genericity in study of parametric problems in control theory. In: Park, H., Regensburger, G. (Eds.), Gröbner Bases in Control Theory and Signal Processing. In: Radon Series Comp. Appl. Math., vol. 3. Walter de Gruyter & Co., pp. 191–214. See also URL: http://arxiv.org/abs/0708.2078.
McConnell, J., Robson, J., 2001. Noncommutative Noetherian Rings. AMS.
Middeke, J., 2008. A polynomial-time algorithm for the Jacobson form for matrices of differential operators. Tech. Rep. 2008-13, RISC, J. Kepler University Linz.
Newman, M., 1972. Integral Matrices. Academic Press.
Schindelar, K., Levandovskyy, V., 2009. A SINGULAR 3.1 library with algorithms for Smith and Jacobson normal forms `jacobson.lib`. URL: http://www.singular.uni-kl.de.
Zerz, E., 2006. An algebraic analysis approach to linear time-varying systems. IMA J. Math. Control Inform. 23 (1), 113–126.
Zerz, E., 2007. State representations of time-varying linear systems. In: Park, H., Regensburger, G. (Eds.), Gröbner Bases in Control Theory and Signal Processing. In: Radon Series Comp. Appl. Math., vol. 3. Walter de Gruyter & Co., pp. 235–251.

Further reading

Lübeck, F., 2002. On the computation of elementary divisors of integer matrices. J. Symbolic Comput. 33 (1), 57–65.