Fraction-free Row Reduction of Matrices of Skew Polynomials

Bernhard Beckermann
Laboratoire d'Analyse Numérique et d'Optimisation
Université des Sciences et Technologies de Lille
France
bbecker@ano.univ-lille1.fr

Howard Cheng George Labahn
Department of Computer Science
University of Waterloo
Waterloo, Canada
{hchcheng,glabahn}@scg.math.uwaterloo.ca

ABSTRACT

We present a new algorithm for row reduction of a matrix of skew polynomials. The algorithm can be used for finding full rank decompositions and other rank revealing transformations of matrices of skew polynomials. The algorithm is intended for computation in exact arithmetic domains where the growth of coefficients in intermediate computations is a central concern. This coefficient growth is controlled by using fraction-free methods. This allows us to obtain a polynomial-time algorithm: for an $m \times s$ matrix of input skew polynomials of degree N with coefficients whose lengths are bounded by K the algorithm has a worst case complexity of $O(m^5 s^4 N^4 K^2)$ bit operations.

1. INTRODUCTION

In [2] Abramov and Bronstein give a new fast algorithm for determining what they call a rank revealing transformations for skew polynomial matrices. These are transformations which convert a matrix of skew polynomials into one where the rank is determined entirely by the leading or trailing coefficient matrix. They show that their algorithm can be used for a number of applications including the desingularization of linear recurrence systems and for computing rational solutions of a large class of linear functional systems. In the former application their rank revealing approach improves on the EG-elimination method of Abramov [1].

In the commutative case the algorithm of [2] is the same as that given by Beckermann and Labahn [6]. In both cases the algorithms are fast but their methods require exact arithmetic while not handling coefficient growth except through coefficient GCD computations. Without the GCD computations the coefficient growth can be exponential.

The main contribution in this paper is a new algorithm which performs row reductions on a given matrix of skew polynomials into one having a full rank leading or trailing coefficient matrix. The reductions can be used to find a full rank decomposition of a matrix of skew polynomials along with rank revealing transformations used by Abramov and Bronstein. The main tool used in the algorithm is *order bases* which describes all solutions of a given order problem. The algorithm is noteworthy because it uses only fraction-free arithmetic without coefficient GCD computations, while at the same time controls coefficient growth of intermediate computations. This is similar to the process used by the subresultant algorithm for computing the GCD of two scalar polynomials [9, 10, 11]. The algorithm is based on the FFFG fraction-free method used in Beckermann and Labahn [8] which was developed for fraction-free computation of matrix rational approximants, matrix GCDs and generalized Richardson extrapolation processes. In the scalar case the FFFG algorithm generalizes the subresultant GCD algorithm [7]. We also give a complexity analysis of our algorithm. For an $m \times s$ matrix of input skew polynomials whose coefficients have lengths bounded by K the algorithm has a worst case complexity of $O(m^5 s^4 N^4 K^2)$ bit operations.

The remainder of the paper is as follows. The next section gives the basic definitions for the problem and introduces order bases of skew polynomials, the primary tool that will be used to solve our problem. Section 3 gives a linear algebra formulation to our problem while the following section gives our fraction-free recurrence. Section 5 discusses the stopping criterion and complexity of our algorithm. The paper ends with a conclusion along with a discussion of future work.

2. PRELIMINARIES

Let $\mathbb{D}$ be an integral domain with $\mathbb{Q}$ its quotient field and let $\mathbb{Q}[Z;\sigma]$ be the Ore domain of skew polynomials over $\mathbb{Q}$ with automorphism σ and $\delta = 0$. Thus the elements of $\mathbb{Q}$ interact with the shift Z via $Za = \sigma(a)Z$. An example of such a domain is $\mathbb{D} = \mathbb{K}[n], \mathbb{Q} = \mathbb{K}(n)$ with Z the shift operator and $\sigma(a(n)) = a(qn+d)$ for some integers q and d with $q \neq 0$. The case when $\sigma(a(n)) = a(n+1)$ is particularly important in applications. We remark that, as in [2], we can handle the problem of computing rational solutions of linear functional systems containing differential, difference and q-difference operators by mapping them into the above domains.

Given a matrix of polynomials of skew polynomials we are interested in applying row operations which transform the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ISSAC 2002, July 7-10, 2002, Lille, France
©2000 ACM 1-58113-484-3/ 02/ 0007 $5.00

matrix into a matrix of skew polynomials which has the property that the rank is revealed by either the trailing or leading coefficient. We will focus on the case of trailing coefficients. In this section we provide the preliminary definitions and tools which form the basis for our approach.

We assume that we are given $\mathbf{F}(Z)$, a rectangular $m \times s$ matrix of skew polynomials with entries in $\mathbb{Q}[Z;\sigma]$

$$\mathbf{F}(Z) = \sum_{j=0}^{N} F_j Z^j, \text{ with } F_j \in \mathbb{D}^{m\times s}.$$

We adapt the convention of denoting the elements of $\mathbf{F}(Z)$ by $\mathbf{F}(Z)^{k,\ell}$, and the elements of F_j by $F_j^{k,\ell}$. For any vector of integers $\vec{\omega} = (\vec{\omega}_1, \ldots, \vec{\omega}_m)$, we let $Z^{\vec{\omega}}$ denote the matrix of skew polynomials having $Z^{\vec{\omega}_i}$ on the diagonal and 0 everywhere else. A matrix of skew polynomials is said to have row (column) degree $\vec{\mu}$ if the *i-th* row (column) has maximal degree $\vec{\mu}_i$. The vector $\vec{e}$ is the vector consisting only of 1.

The goal of this paper is to construct the type of rank revealing transformations needed by Abramov and Bronstein [2] for their applications. Let $\mathbb{Q}[Z;\sigma][Z^{-1};\sigma^{-1}]$ be the iterated domain where we have the identities

$$Z\cdot Z^{-1} = Z^{-1}\cdot Z = 1,\ \ Z\cdot a\cdot Z^{-1} = \sigma(a),\ \ Z^{-1}\cdot a\cdot Z = \sigma^{-1}(a)$$

for all $a \in \mathbb{Q}$.

The rank revealing transformations of Abramov and Bronstein can be formalized as follows. Given the matrix of skew polynomials $\mathbf{F}(Z) \in \mathbb{D}[Z;\sigma]^{m\times s}$ (possibly after a shift with $Z^{-\ell}$), we wish to find $\mathbf{T}(Z^{-1}) \in \mathbb{D}[Z^{-1};\sigma^{-1}]^{m\times m}$ such that

$$\mathbf{T}(Z^{-1})\cdot\mathbf{F}(Z) = \mathbf{W}(Z) \in \mathbb{D}[Z;\sigma]^{m\times s},$$

with the number of nonzero rows r of $\mathbf{W}(Z)$ coinciding with the rank of the trailing coefficient W_0, and hence with the rank of $\mathbf{W}(Z)$. In addition we require the existence of $\mathbf{S}(Z) \in \mathbb{Q}[Z;\sigma]^{m\times m}$ such that

$$\mathbf{S}(Z)\cdot\mathbf{T}(Z^{-1}) = \mathbf{I}_m.$$

Notice that the second formula tells us that the process of elimination for getting $\mathbf{W}(Z)$ is invertible. More precisely, we obtain for $\mathbf{F}(Z)$ the *full rank decomposition*

$$\mathbf{F}(Z) = \mathbf{S}(Z)\cdot\mathbf{W}(Z) = \widetilde{\mathbf{S}}(Z)\cdot\widetilde{\mathbf{W}}(Z) \tag{1}$$

with $\widetilde{\mathbf{W}}(Z) \in \mathbb{D}[Z;\sigma]^{r\times n}$ obtained by extracting the nonzero rows of $\mathbf{W}(Z)$, and $\widetilde{\mathbf{S}}(Z) \in \mathbb{Q}[Z;\sigma]^{m\times r}$ by extracting from $\mathbf{S}(Z)$ the corresponding columns. Moreover, the rank of the trailing coefficient of $\widetilde{\mathbf{W}}(Z)$ is of full row rank r, and this quantity coincides with the rank of $\widetilde{\mathbf{W}}(Z)$. Finally, from this last equation we see that the rank of $\mathbf{F}(Z)$ is bounded above by r, whereas the first equation tells us that $\operatorname{rank}\mathbf{F}(Z) \geq \operatorname{rank}\mathbf{W}(Z) = r$. Thus we have found $r = \operatorname{rank}\mathbf{F}(Z)$.

2.1 Order Basis

In this subsection we introduce the notion of order and order bases for a given matrix of skew polynomials. These are the primary tools which will be used for our algorithm.

DEFINITION 2.1. *Let $\mathbf{P}(Z) \in \mathbb{Q}[Z;\sigma]^{1\times m}$ be a vector of skew polynomials and $\vec{\omega}$ a multi-index of integers. Then $\mathbf{P}(Z)$ is said to have* order $\vec{\omega}$ *if*

$$\mathbf{P}(Z)\cdot\mathbf{F}(Z) = \mathbf{R}(Z)\cdot Z^{\vec{\omega}} \tag{2}$$

with $\mathbf{R}(Z) \in \mathbb{Q}[Z;\sigma]^{1\times s}$. $\mathbf{R}(Z)$ in (2) is called a residual. □

In contrast to previous papers dealing with order bases [4, 5, 6, 8], we have chosen an order condition on the right. This has the advantage that while writing

$$\mathbf{F}(Z) = \sum_j F_j Z^j, \quad \mathbf{P}(Z) = \sum_k P_k Z^k,$$

we have

$$\mathbf{P}(Z)\cdot\mathbf{F}(Z) = \sum_j S_j Z^j, \quad S_j = \sum_k P_k \sigma^k(F_{j-k}). \tag{3}$$

Hence the unknowns P_k can be obtained by building a linear system obtained by putting the undesired coefficients of S_j equal to zero. In order to specify these coefficients (see equation (5) below), let us write more explicitly $c_j^{k,\ell}(\mathbf{P}(Z)) := S_j^{k,\ell}$ for the coefficients occurring in (3).

Notice that, though the algebra $\mathbb{Q}[Z;\sigma]$ is non-commutative, the matrix of coefficients will have elements in the field $\mathbb{Q}$. Thus we may build determinants and apply other techniques known from fraction–free algorithms which enable us to control the size of intermediate quantities and to predict common factors.

In what follows we will construct elements from $\mathbb{Q}[Z;\sigma]^{m\times m}$ (and more precisely from $\mathbb{D}[Z;\sigma]^{m\times m}$) which will enable us to describe the entire set of vectors of a given order.

DEFINITION 2.2. *Let $\vec{\omega}$ be some multi-index. A matrix of skew polynomials $\mathbf{M}(Z) \in \mathbb{Q}[Z;\sigma]^{m\times m}$ is said to be an* order basis *of order $\vec{\omega}$ and degree $\vec{\mu}$ if there exists a multi-index $\vec{\mu} = (\vec{\mu}_1, \ldots, \vec{\mu}_m)$ such that*

a) every row of $\mathbf{M}(Z)$ has order $\vec{\omega}$,

b) for every $\mathbf{P}(Z) \in \mathbb{Q}[Z;\sigma]^{1\times m}$ of order $\vec{\omega}$ there exists a $\mathbf{Q}(Z) \in \mathbb{Q}[Z;\sigma]^{1\times m}$ such that

$$\mathbf{P}(Z) = \mathbf{Q}(Z)\cdot\mathbf{M}(Z),$$

where $\deg\mathbf{Q}(Z)^{1,j} \leq \deg\mathbf{P}(Z) - \vec{\mu}_j$ for all j,

c) there exists a nonzero $d \in \mathbb{Q}$ such that

$$\mathbf{M}(Z) = d\cdot Z^{\vec{\mu}} + \mathbf{L}(Z)$$

where $\deg\mathbf{L}(Z)^{k,\ell} \leq \begin{cases} \min\{\vec{\mu}_k - 1, \vec{\mu}_\ell - 1\} & \ell \geq k, \\ \min\{\vec{\mu}_k, \vec{\mu}_\ell - 1\} & \ell < k. \end{cases}$

□

REMARK 2.3. *Note that when $\vec{\omega} = p \cdot \vec{e}$ for a given p, then every row of $Z^{p\vec{e}}$ has order $\vec{\omega}$. Hence part (b) of Definition 2.2 implies that there exists a $\mathbf{M}^*(Z) \in \mathbb{Q}[Z;\sigma]^{m\times m}$ such that*

$$\mathbf{M}^*(Z) \cdot \mathbf{M}(Z) = Z^{p\vec{e}}, \quad \deg \mathbf{M}^*(Z)^{k,\ell} \leq p - \vec{\mu}_\ell,$$

that is, a type of shifted inverse. The existence of a shifted left inverse $\mathbf{M}^*(Z)$ will enable us to generalize the notion of unimodular transformations of order bases to the case of the non-commutative algebra $\mathbb{Q}[Z;\sigma]$. □

An essential implication of Definition 2.2(b) is the following:

THEOREM 2.4. *Suppose that there exists an order basis $\mathbf{M}(Z)$ of order $\vec{\omega}$ and degree $\vec{\mu}$. Then there exists only the trivial row vector $\mathbf{P}(Z) = 0$ with column degree $\leq \vec{\mu} - \vec{e}$ and order $\geq \vec{\omega}$. Thus, for any k, a row vector with column degree $\leq \vec{\mu} - \vec{e} + \vec{e}_k$ and order $\geq \vec{\omega}$ is unique up to multiplication with an element from $\mathbb{Q}$. In particular, an order basis is unique up to multiplication by constants from $\mathbb{Q}$.*

Proof: We only need to show the first part concerning row vectors $\mathbf{P}(Z)$ with column degree $\vec{\mu} - \vec{e}$ and order $\vec{\omega}$, the other parts being an immediate consequence of the first. Suppose that $\mathbf{P}(Z) \neq 0$, $d = deg\, \mathbf{P}(Z)$, and let $\mathbf{Q}(Z)$ be as in Definition 2.2(b). We first claim that there exists at least one index j with

$$\vec{\mu}_j + deg\, \mathbf{Q}(Z)^{1,j} = d. \tag{4}$$

Otherwise, $deg\ \mathbf{Q}(Z)^{1,k} \cdot \mathbf{M}(Z)^{k,\ell} \leq \vec{\mu}_k + deg\, \mathbf{Q}(Z)^{1,k} < d$ for all k and ℓ since $deg\, \mathbf{M}(Z)^{k,\ell} \leq \vec{\mu}_k$ by Definition 2.2(c), in contradiction with the definition of d. Let j be the largest index verifying (4). Then again by Definition 2.2(c)

$$\begin{aligned}
& deg \sum_{k=j+1}^{m} \mathbf{Q}(Z)^{1,k}\mathbf{M}(Z)^{k,j} \\
\leq \quad & \sum_{k=j+1}^{m} d - \vec{\mu}_k - 1 + deg\, \mathbf{M}(Z)^{k,j} \leq d-1, \\
& deg \sum_{k=1}^{j-1} \mathbf{Q}(Z)^{1,k}\mathbf{M}(Z)^{k,j} \\
\leq \quad & \sum_{k=1}^{j-1} deg\, \mathbf{Q}(Z)^{1,k} + \vec{\mu}_k - 1 \leq d-1, \\
& deg\, \mathbf{Q}(Z)^{1,j}\mathbf{M}(Z)^{j,j} = deg\, \mathbf{Q}(Z)^{1,j} + \vec{\mu}_j = d.
\end{aligned}$$

This implies that $deg\, \mathbf{P}(Z)^{1,j} = d \geq \vec{\mu}_j$, which contradicts the assumption of the degree of $\mathbf{P}(Z)$. □

3. DETERMINANTAL REPRESENTATIONS AND MAHLER SYSTEMS

In what follows we will propose an algorithm for computing recursively order bases $\mathbf{M}(Z)$ for increasing order vectors. In order to predict the size of these objects and predict common factors, we derive in this section a determinantal representation together with a particular choice of the constant d.

Suppose that we are looking for a row vector $\mathbf{P}(Z)$ of column degree $\vec{\nu}$ having order $\vec{\omega}$. Comparing with (3), we know that $\mathbf{P}(Z)$ has order $\vec{\omega}$ iff for all $\ell = 1, \ldots, s$, $j = 0, \ldots, \vec{\omega}_\ell - 1$:

$$0 = c_j^{1,\ell}(\mathbf{P}(Z)) = \sum_{k=1}^{m} \sum_{\kappa=0}^{\min\{j,\vec{\nu}_k\}} P_\kappa^{1,k} \sigma^\kappa(F_{j-\kappa}^{k,\ell}).$$

This leads to some system of linear equations of the form

$$(P_0^{1,1}, ..., P_{\vec{\nu}_1}^{1,1}, ..., P_0^{1,m}, ..., P_{\vec{\nu}_m}^{1,m}) \cdot K(\vec{\nu} + \vec{e}, \vec{\omega}) = 0, \tag{5}$$

where the generalized Sylvester matrix is of the form

$$K(\vec{\nu} + \vec{e}, \vec{\omega}) = (K^{k,\ell}(\vec{\nu}_k + 1, \vec{\omega}_\ell))_{k=1,\ldots,m}^{\ell=1,\ldots,s},$$

where the $\nu \times \omega$ submatrix $K^{k,\ell}(\nu, \omega)$ equals

$$\begin{bmatrix}
\sigma^0(F_0^{k,\ell}) & \sigma^0(F_1^{k,\ell}) & \cdots & \cdots & \sigma^0(F_{\omega-1}^{k,\ell}) \\
0 & \sigma^1(F_0^{k,\ell}) & \cdots & \cdots & \sigma^1(F_{\omega-2}^{k,\ell}) \\
\vdots & \ddots & \ddots & & \vdots \\
0 & \cdots & \sigma^{\nu-1}(F_0^{k,\ell}) & \cdots & \sigma^{\nu-1}(F_{\omega-\nu}^{k,\ell})
\end{bmatrix}.$$

Clearly, $K^{k,\ell}(\vec{\nu}_k + 1, \vec{\omega}_\ell)^T$ (and thus $K(\vec{\nu} + \vec{e}, \vec{\omega})^T$) may be written as some striped Krylov matrix [8], that is, a matrix of the form

$$\left[\begin{array}{ccc|c|ccc}
\mathbf{F}_{\omega_\ell}^{(1)} & \cdots & \mathbf{C}_{\omega_\ell}^{\vec{\nu}_1 - 1}\mathbf{F}_{\omega_\ell}^{(1)} & \cdots & \mathbf{F}_{\omega_\ell}^{(m)} & \cdots & \mathbf{C}_{\omega_\ell}^{\vec{\nu}_m - 1}\mathbf{F}_{\omega_\ell}^{(m)}
\end{array}\right].$$

However, by stepping from one column to the next we not only multiply with a lower shift matrix but also apply in addition the application σ. Thus, in contrast to [8], here we obtain a striped Krylov matrix with a matrix C having operator-valued elements.

How can we exploit this representation in order to derive a determinantal representation of order bases? According to (5), it follows from Theorem 2.4 that if there exists an order basis $\mathbf{M}(Z)$ of order $\vec{\omega}$ and degree $\vec{\mu}$ then $K(\vec{\mu}, \vec{\omega})$ has full row rank, and more precisely

$$k = 1, ..., m: \quad \text{rank } K(\vec{\mu}, \vec{\omega}) = \text{rank } K(\vec{\mu} + \vec{e}_k, \vec{\omega}) = |\vec{\mu}|. \tag{6}$$

Suppose more generally that $\vec{\mu}$ and $\vec{\omega}$ are multi-indices verifying (6). We call a *multigradient* $d = d(\vec{\mu}, \vec{\omega})$ any constant ± 1 times the determinant of a regular submatrix $K_*(\vec{\mu}, \vec{\omega})$ of maximal order of $K(\vec{\mu}, \vec{\omega})$, and a *Mahler system* corresponding to $(\vec{\mu}, \vec{\omega})$ a matrix polynomial $\mathbf{M}(Z)$ with rows having order $\vec{\omega}$ and degree structure

$$\mathbf{M}(Z) = d \cdot Z^{\vec{\mu}} + \text{ lower order column degrees.}$$

In order to show that such a system exists, we write down explicitly the linear system of equations needed to compute the unknown coefficients of the kth row of $\mathbf{M}(Z)$: denote by $b^k(\vec{\mu}, \vec{\omega})$ the row added while passing from $K(\vec{\mu}, \vec{\omega})$ to $K(\vec{\mu} + \vec{e}_k, \vec{\omega})$. Then, by (5), the vector of coefficients is a solution of the (overdetermined) system

$$x \cdot K(\vec{\mu}, \vec{\omega}) = d \cdot b^k(\vec{\mu}, \vec{\omega})$$

which by (6) is equivalent to the system

$$x \cdot K_*(\vec{\mu}, \vec{\omega}) = d \cdot b_*^k(\vec{\mu}, \vec{\omega}), \tag{7}$$

where in $b_*^k(\vec{\mu}, \vec{\omega})$ and in $K_*(\vec{\mu} + \vec{e}_k, \vec{\omega})$ we keep the same columns as in $K_*(\vec{\mu}, \vec{\omega})$. Notice that, by Cramer's rule, (7)

leads to a solution with coefficients in $\mathbb{D}$. Moreover, we may formally write down a determinantal representation of the elements of an determinantal order basis, namely

$$\mathbf{M}(Z)^{k,\ell} = \pm det\ \left[\ K_*(\vec{\mu}+\vec{e}_k,\vec{\omega})\ \middle|\ \mathbf{E}_{\ell,\vec{\mu}_\ell-1+\delta_{\ell,k}}(Z)\ \right] \quad (8)$$

with

$$\mathbf{E}_{\ell,\nu}(Z) = [0,\ldots,0|1,Z,\ldots,Z^\nu|0,\ldots,0]^T, \quad (9)$$

the nonzero entries in $\mathbf{E}_{\ell,n}(Z)$ occurring in the ℓ-th stripe. In addition, we have that

$$\sum_j \mathbf{M}(Z)^{k,j}\mathbf{F}(Z)^{j,\ell} = \pm det\ \left[K_*(\vec{\mu}+\vec{e}_k,\vec{\omega})\ \middle|\ \mathbf{E}_{\ell,\vec{\mu}+\vec{e}_k}(Z)\right], \quad (10)$$

where

$$\begin{aligned}\mathbf{E}_{\ell,\vec{\nu}}(Z) \quad = \quad & [\mathbf{F}(Z)^{1,\ell},\ldots,Z^{\vec{\nu}_1-1}\mathbf{F}(Z)^{1,\ell}|\ldots\ldots| \\ & \mathbf{F}(Z)^{m,\ell},\ldots,Z^{\vec{\nu}_m-1}\mathbf{F}(Z)^{m,\ell}]^T.\end{aligned}$$

In both (8) and (10) the matrices have commutative entries in all but the last column. It is understood that the determinant in both cases is expanded along the last column.

We finally mention that, by the uniqueness result of Theorem 2.4, any order basis of degree $\vec{\mu}$ and order $\vec{\omega}$ coincides up to multiplication with some element in $\mathbb{Q}$ with a Mahler system associated to $(\vec{\mu},\vec{\omega})$, which therefore itself is an order basis of the same degree and order. The converse statement is generally not true. However, by a particular pivoting technique we may recover order basis by computing Mahler systems.

4. THE ALGORITHM

In this section we show how to recursively compute order bases in a fraction-free way. For an order basis $\mathbf{M}(Z)$ of a given type $(\vec{\mu},\vec{\omega})$ having a Mahler system normalization, we look at the first terms of the residuals. If they are all equal to zero then we have an order basis of a higher order. Otherwise, we give a recursive formula for building an order basis of higher order and degree. However, a priori this new system has coefficients from $\mathbb{Q}$ since we divide through some factors. In our case, however, the new system will be a Mahler system according to the existence and uniqueness results established before, and hence we will keep objects with coefficients in $\mathbb{D}$.

In the following theorem we give a recurrence relation which closely follows the commutative case of [8, Theorem 6.1(c)] with the resulting order bases having properties similar to [8, Theorem 7.2] and [8, Theorem 7.3].

THEOREM 4.1. *Let $\mathbf{M}(Z)$ be an order basis corresponding to $(\vec{\mu},\vec{\omega})$, $\widetilde{\vec{\omega}} := \vec{\omega}+\vec{e}_\lambda$. Furthermore, denote by $r_j = c^{j,\lambda}_{\vec{\omega}_\lambda}(\mathbf{M}(Z))$, the first term of the residual for the j-th row and λ-th column of $\mathbf{M}(Z)$.*

a) *If $r_1 = \ldots = r_m = 0$ then $\widetilde{\mathbf{M}}(Z) := \mathbf{M}(Z)$ is an order basis of degree $\vec{\nu} := \vec{\mu}$ and order $\widetilde{\vec{\omega}}$.*

b) *Otherwise, let π be the smallest index with $r_\pi \neq 0$ and*

$$\vec{\mu}_\pi = \min_j\{\vec{\mu}_j : r_j \neq 0\}.$$

Then an order basis $\widetilde{\mathbf{M}}(Z)$ of degree $\vec{\nu} := \vec{\mu}+\vec{e}_\pi$ and order $\widetilde{\vec{\omega}}$ with coefficients in $\mathbb{Q}$ is obtained via the formulas

$$p_\pi \cdot \widetilde{\mathbf{M}}(Z)^{\ell,k} = r_\pi \cdot \mathbf{M}(Z)^{\ell,k} - r_\ell \cdot \mathbf{M}(Z)^{\pi,k} \quad (11)$$

for $\ell,k = 1,2,\ldots,m$, $\ell \neq \pi$, and

$$\sigma(p_\pi)\cdot\widetilde{\mathbf{M}}(Z)^{\pi,k} = r_\pi \cdot Z \cdot \mathbf{M}(Z)^{\pi,k} - \sum_{\ell\neq\pi}\sigma(p_\ell)\cdot\widetilde{\mathbf{M}}(Z)^{\ell,k} \quad (12)$$

for $k = 1,2,\ldots,m$, where $p_j = \text{coefficient}(\mathbf{M}(Z)^{\pi,j}, Z^{\vec{\mu}_j+\delta_{\pi,j}-1})$.

c) *If in addition $\mathbf{M}(Z)$ is a Mahler system with respect to $(\vec{\mu},\vec{\omega})$, then $\widetilde{\mathbf{M}}(Z)$ is also a Mahler system with respect to $(\vec{\nu},\widetilde{\vec{\omega}})$. In particular, $\widetilde{\mathbf{M}}(Z)$ has coefficients in $\mathbb{D}$.*

Proof: Part (a) is clear from the fact that the rows of $\mathbf{M}(Z)$ have order $\widetilde{\vec{\omega}}$ when $r_1 = \ldots = r_m = 0$.

For part (b) notice first that $\widetilde{\mathbf{M}}(Z)$ has order $\widetilde{\vec{\omega}}$ by construction, as required in Definition 2.2(a). Also, verifying the new degree constraints of Definition 2.2(c) (with $\vec{\mu}$ being replaced by $\vec{\nu}$) for the matrix $\widetilde{\mathbf{M}}(Z)$ is straightforward and is the same as in the commutative case, see [8, Theorem 7.2]. Also, notice that the leading coefficient of all $\widetilde{\mathbf{M}}(Z)^{\ell,\ell}$ equals r_π by construction (though for the moment we are not sure to obtain a new order basis with coefficients in $\mathbb{D}$).

We now focus on the properties of Definition 2.2(b). If $\mathbf{P}(Z) \in \mathbb{Q}[Z;\sigma]^{1\times m}$ has order $\widetilde{\vec{\omega}}$ then it has order $\vec{\omega}$ and so there exists an $\mathbf{Q}(Z) \in \mathbb{Q}[Z;\sigma]^{1\times m}$ such that

$$\mathbf{P}(Z) = \sum_{j=1}^m \mathbf{Q}(Z)^{1,j}\cdot\mathbf{M}(Z)^{j,\cdot}$$

with $deg\ \mathbf{Q}(Z)^{1,j} \leq deg\ \mathbf{P}(Z) - \vec{\mu}_j$, where $\mathbf{M}(Z)^{j,\cdot}$ denotes the j-th row of $\mathbf{M}(Z)$. Applying the first set of row operations in (11) to rows $\ell \neq \pi$ results in

$$\mathbf{P}(Z) = \sum_{j\neq\pi}^m \hat{\mathbf{Q}}(Z)^{1,j}\cdot\widetilde{\mathbf{M}}(Z)^{j,\cdot} + \hat{\mathbf{Q}}(Z)^{1,\pi}\cdot\mathbf{M}(Z)^{\pi,\cdot} \quad (13)$$

where

$$\begin{aligned}\hat{\mathbf{Q}}(Z)^{1,j} \quad &= \quad \mathbf{Q}(Z)^{1,j}\cdot\frac{p_\pi}{r_\pi} \text{ for all } j\neq\pi \text{ and} \\ \hat{\mathbf{Q}}(Z)^{1,\pi} \quad &= \quad \sum_{i=1}^m \mathbf{Q}(Z)^{1,i}\cdot\frac{r_i}{r_\pi}.\end{aligned}$$

Note that $deg\ \hat{\mathbf{Q}}(Z)^{1,j} \leq deg\ \mathbf{P}(Z) - \vec{\mu}_j = deg\ \mathbf{P}(Z) - \vec{\nu}_j$ for all $j \neq \pi$ while $deg\ \hat{\mathbf{Q}}(Z)^{1,\pi} \leq deg\ \mathbf{P}(Z) - \vec{\mu}_\pi$ because of the minimality of $\vec{\mu}_\pi$. Since $\mathbf{P}(Z)$ and all the $\widetilde{\mathbf{M}}(Z)^{j,\cdot}$ terms have order $\widetilde{\vec{\omega}}$ this must also be the case for $\hat{\mathbf{Q}}(Z)^{1,\pi}\cdot M(Z)^{\pi,\cdot}$. Hence $\hat{Q}_0^{1,\pi}\cdot r_\pi = 0$ and so by assumption on π we have that $\hat{Q}_0^{1,\pi} = 0$. Writing $\hat{\mathbf{Q}}(Z)^{1,\pi} = \bar{\mathbf{Q}}(Z)^{1,\pi}\cdot Z$ gives

$$\mathbf{P}(Z) = \sum_{j\neq\pi}^m \hat{\mathbf{Q}}(Z)^{1,j}\cdot\widetilde{\mathbf{M}}(Z)^{j,\cdot} + \bar{\mathbf{Q}}(Z)^{1,\pi}\cdot Z\cdot\mathbf{M}(Z)^{\pi,\cdot} \quad (14)$$

with $deg\ \bar{\mathbf{Q}}(Z)^{1,\pi} \leq deg\ \mathbf{P}(Z) - (\vec{\mu}_\pi+1) = deg\ \mathbf{P}(Z) - \vec{\nu}_\pi$. Completing the row operations which normalize the

degrees of $\widetilde{\mathbf{M}}(Z)$ in (12) gives a $\widetilde{\mathbf{Q}}(Z)$ with $\mathbf{P}(Z) = \widetilde{\mathbf{Q}}(Z) \cdot \widetilde{\mathbf{M}}(Z)$ having the correct degree bounds. Consequently, the property of Definition 2.2(b) holds.

Finally, for establishing part (c) we know already from Section 3 and the existence of order bases of a specified degree and order that both $(\vec{\mu}, \vec{\omega})$ and $(\vec{\nu}, \widetilde{\vec{\omega}})$ satisfy (6). By the uniqueness result of Theorem 2.4 we only need to show that the "leading coefficient" $\widetilde{d}$ of $\widetilde{\mathbf{M}}(Z)$ in Definition 2.2(c) is a multigradient of $(\vec{\nu}, \widetilde{\vec{\omega}})$, the latter implying that $\widetilde{\mathbf{M}}(Z)$ is a Mahler system and in particular has coefficients from $\mathbb{D}$.

Denote by d the corresponding "leading coefficient" of $\mathbf{M}(Z)$. In the case discussed in part (a), we do not increase the rank by going from $K(\vec{\mu}, \vec{\omega})$ to $K(\vec{\nu}, \widetilde{\vec{\omega}})$ (we just add one column and keep full row rank), hence $d = \widetilde{d}$ being a multigradient with respect to $(\vec{\mu}, \vec{\omega})$ is also a multigradient with respect to $(\vec{\nu}, \widetilde{\vec{\omega}})$. In the final case described in part (b) we have $\widetilde{d} = r_\pi$. Using formula (10) for the residual of the πth row of $\mathbf{M}(Z)$ we learn that r_π coincides (up to a sign) with the determinant of a submatrix of order $|\vec{\nu}|$ of $K(\vec{\nu}, \widetilde{\vec{\omega}})$. Since $r_\pi \neq 0$ by construction, it follows that $\widetilde{d} = r_\pi$ is a new multigradient, as required for the conclusion. □

Theorem 4.1 gives a computational procedure that results in the FFreduce algorithm given in Table 1. The stopping criterion and the complexity of this algorithm is given in the next section.

EXAMPLE 4.2. *For the domain* $\mathbb{D} = Z[n]$, *let*

$$\mathbf{F}(Z) = \begin{bmatrix} n^2+2 & 0 \\ -1 & 0 \end{bmatrix} + \begin{bmatrix} 32 & -1 \\ 0 & 0 \end{bmatrix} Z + \begin{bmatrix} 0 & 0 \\ 1 & 32n \end{bmatrix} Z^2.$$

At the first iteration, we have $\vec{\omega} = \vec{\mu} = (0,0)$, *and the constant coefficients in the first column are* $[n^2+2, -1]^T$. *Choosing* $\pi = 1$ *and performing the reduction, we obtain*

$$\begin{aligned} \mathbf{M}(Z) &= \begin{bmatrix} (n^2+2)Z & 0 \\ 1 & n^2+2 \end{bmatrix} \\ \mathbf{M}(Z)\cdot\mathbf{F}(Z) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ &\quad + \begin{bmatrix} n^4+2n^3+5n^2+4n+6 & 0 \\ 32 & -1 \end{bmatrix} Z \\ &\quad + \begin{bmatrix} 32n^2+64 & -n^2-2 \\ n^2+2 & 32n^3+64n \end{bmatrix} Z^2. \end{aligned}$$

Note that the constant coefficients in the second column of $\mathbf{R}(Z)$ *are zero, so no operations are required to increase* $\vec{\omega}$ *to* $(1,1)$.

Now, $\vec{\omega} = (1,1)$, $\vec{\mu} = (1,0)$, *and* $d = n^2+2$. *The coefficients of* Z *in the first column is* $[n^4+2n^3+5n^2+4n+6, 32]^T$. *Choosing* $\pi = 2$ *and performing the row reductions, we see that* $\mathbf{M}(Z)$ *is*

$$\begin{bmatrix} (-n^2-2n-3)+32Z & -5n^2-4n-n^4-2n^3-6 \\ 1 & (n^2+2)+32Z \end{bmatrix}$$

while $\mathbf{M}(Z)\cdot\mathbf{F}(Z)$ *is given in Figure 1, where we have divided row 1 by* d *and row 2 by* $\sigma(d) = n^2+2n+3$. □

Table 1: ***The FFreduce Algorithm***

ALGORITHM FFreduce

INPUT: Matrix of skew polynomials $\mathbf{F} \in \mathbf{D}[Z;\sigma]^{m\times s}$.

OUTPUT: Mahler system $\mathbf{M} \in \mathbb{D}[Z;\sigma]^{m\times m}$,
Residual $\mathbf{R} \in \mathbb{D}[Z;\sigma]^{m\times s}$
Degree $\vec{\mu}$, order $\vec{\omega}$, rank ρ

INITIALIZATION: $\mathbf{M} \leftarrow \mathbf{I}_m$, $\mathbf{R} \leftarrow \mathbf{F}$, $d \leftarrow 1$,
$\vec{\mu} \leftarrow \vec{0}, \vec{\omega} \leftarrow \vec{0}$, $\rho \leftarrow 0$

While (number of zero rows of $\mathbf{R} + \rho \neq m$):
$\rho \leftarrow 0$
For $\lambda = 1, .., s$ **do**
Calculate for $\ell = 1, .., m$:
first term of residuals $r_\ell \leftarrow R_0^{\ell,\lambda}$
Define set $\Lambda = \{\ell \in \{1, .., m\} : r_\ell \neq 0\}$.

If $\Lambda \neq \{\}$ **then**
Choose $\pi \in \Lambda$ such that:
$\pi = \min\{\ell \in \Lambda : \vec{\mu}_\ell = \min_{\nu\in\Lambda}\{\vec{\mu}_\nu\}\}$.

Calculate for $\ell = 1, .., m$, $\ell \neq \pi$:
$p_\ell \leftarrow$ *coefficient*$(\mathbf{M}^{\pi,\ell}, Z^{\vec{\mu}_\ell + \delta_{\pi,\ell} - 1})$.

Increase order for $\ell = 1, .., m$, $\ell \neq \pi$:
$\mathbf{M}^{\ell,\cdot} \leftarrow \frac{1}{d}[r_\pi \cdot \mathbf{M}^{\ell,\cdot} - r_\ell \cdot \mathbf{M}^{\pi,\cdot}]$
$\mathbf{R}^{\ell,\cdot} \leftarrow \frac{1}{d}[r_\pi \cdot \mathbf{R}^{\ell,\cdot} - r_\ell \cdot \mathbf{R}^{\pi,\cdot}]$

Increase order and adjust degree constraints for row π:
$\mathbf{M}^{\pi,\cdot} \leftarrow \frac{1}{\sigma(d)}[r_\pi \cdot Z \cdot \mathbf{M}^{\pi,\cdot} - \sum_{\ell\neq\pi} \sigma(p_\ell) \cdot \mathbf{M}^{\ell,\cdot}]$
$\mathbf{R}^{\pi,\cdot} \leftarrow \frac{1}{\sigma(d)}[r_\pi \cdot Z \cdot \mathbf{R}^{\pi,\cdot} - \sum_{\ell\neq\pi} \sigma(p_\ell) \cdot \mathbf{R}^{\ell,\cdot}]$

Update multigradient, degree and ρ:
$d = r_\pi$, $\vec{\mu} \leftarrow \vec{\mu} + \vec{e}_\pi$, $\rho \leftarrow \rho + 1$
end if

Adjust residual in column λ: for $\ell = 1, ..., m$
$\mathbf{R}^{\ell,\lambda} \leftarrow \mathbf{R}^{\ell,\lambda}/Z$ (formally)

$\vec{\omega} = \vec{\omega} + \vec{e}_\lambda$
end for

$$\begin{bmatrix} 0 & n^2+2n+3 \\ 0 & -1 \end{bmatrix} Z + \begin{bmatrix} -n^4-2n^3-5n^2-4n+1018 & -32\left(n^5+2n^4+5n^3+4n^2+6n+1\right) \\ n^2+2 & 32(n^2+2)n \end{bmatrix} Z^2$$
$$+ \begin{bmatrix} 0 & n^2+2n+3 \\ 32 & 1024(n+1) \end{bmatrix} Z^3.$$

Figure 1: $\mathbf{M}(Z) \cdot \mathbf{F}(Z)$ after two steps in Example 4.2.

Finally, with respect to the rank revealing transformation mentioned in Section 1, we have the following.

COROLLARY 4.3. *Let $\mathbf{M}(Z)$ be the final order basis of order $\vec{\omega} = k\vec{e}$ and degree $\vec{\mu}$, and let $\mathbf{M}^*(Z)$ be the shifted left inverse of $\mathbf{M}(Z)$ as explained in Remark 2.3. Then the quantities*

$$\begin{aligned} \mathbf{W}(Z) &= Z^{-k\vec{e}} \cdot \mathbf{R}(Z) \cdot Z^{k\vec{e}} \\ \mathbf{T}(Z^{-1}) &= Z^{-k\vec{e}} \cdot \mathbf{M}(Z) \\ \mathbf{S}(Z) &= Z^{-k\vec{e}} \cdot \mathbf{M}^*(Z) \cdot Z^{k\vec{e}} \end{aligned}$$

solve the full rank decomposition problem (1). □

In the case where one is only interested in determining $\widetilde{\mathbf{W}}(Z)$ in a full rank decomposition (1), then one can do a simple modification of our algorithm to obtain an answer with smaller coefficients. Indeed, it will be shown in the next section (Remark 5.4) that one can in fact use the residual one iteration before completion for our rank revealing transformations. One simply uses the rows corresponding to the pivot rows in the last iteration.

EXAMPLE 4.4. *Let $D = Z[n, 2^n]$ and consider*

$$\begin{aligned} \mathbf{F}(Z) &= \begin{bmatrix} 0 & -1 \\ 0 & -12356 \end{bmatrix} + \begin{bmatrix} -80 & 0 \\ -988480 & -8029 \end{bmatrix} Z \\ &+ \begin{bmatrix} -32 & 0 \\ -1037712 & 750 \end{bmatrix} Z^2 + \begin{bmatrix} 0 & 0 \\ -196928 & -300 \end{bmatrix} Z^3 \\ &+ \begin{bmatrix} 0 & 1 \\ 0 & 120 \end{bmatrix} Z^4 + \begin{bmatrix} 2^n(n+1) & 0 \\ 0 & 3077(n+1) \end{bmatrix} Z^5, \end{aligned}$$

which is the same as the example from [2] except that it is multiplied (on the right) by Z^4. Using our algorithm, we terminate at $\vec{\omega} = (6, 6)$ in which the residuals are not all zero in the last two steps. The trailing coefficient of the residual $\mathbf{R}(Z)$ obtained one iteration previously (that is, two steps ago) at $\vec{\omega} = (5, 5)$ has a determinant that is an integer constant times $2^n(n+1) - 80$.

Writing $\mathbf{W}(Z) = Z^{-(5,5)} \cdot \mathbf{R}(Z) \cdot Z^{(5,5)}$, the determinant of the trailing coefficient of $\mathbf{W}(Z)$ is the same as that in [2], up to a constant. We remark that the product of all the factors removed during the complete process is

$$2350159171880334461640000000000\,(2^n(n+1) - 80)\,.$$

□

We remark that the algorithm of [2] also avoids the use of fractions by taking advantage of fraction-free Gaussian elimination of Bareiss [3] for the kernel computations used in their algorithm. The size of the coefficients in the kernel vectors can be reduced by removing the greatest common factor among the components as done in the implementation of [2] in Maple 8. However, extraneous factors introduced in previous iterations are not removed by such a process.

5. STOPPING CRITERIA AND COMPLEXITY

In this section, we show that the stopping criteria of our algorithm ensures that the result is correct and discuss the worst case complexity of the algorithm. For convenience, we call the computation to increase $|\vec{\omega}|$ by 1 as a step, and the computation to increase $\vec{\omega} = k\vec{e}$ to $\vec{\omega}' = (k+1)\vec{e}$ an iteration, so that there are s steps in each iteration. As in the algorithm itself we drop the need to specify the variable Z. Let $\mathbf{M}_k$ be the Mahler system of degree $\vec{\mu}_k$ and $\mathbf{R}_k$ be the residual after the k-th iteration with $\mathbf{R}_k(0)$ denoting the trailing coefficient of $\mathbf{R}_k$.

We first prove a lemma which relates the number of pivots used during the $(k+1)$-st iteration and the rank of $\mathbf{R}_k(0)$.

LEMMA 5.1. *Let $k \geq 0$, and r be the value of ρ at the end of iteration $k+1$. Then $r = \text{rank } \mathbf{R}_k(0)$.*

Proof: Denote by $H_\lambda \in \mathbb{D}^{m \times s}$, $\lambda = 1, ..., s$, the coefficient of Z^k of $\mathbf{M} \cdot \mathbf{F}$ during the k-th iteration at the beginning the single step $\vec{\omega} \leftarrow \vec{\omega} + \vec{e}_\lambda$ (thus H_λ is transformed into $H_{\lambda+1}$ during this step). First, we claim that when row π is chosen as a pivot for column λ, the subspace generated by the rows of H_λ is the same as the subspace generated by row π of H_λ (called a pivot row) and the rows of $H_{\lambda+1}$. This is clearly true after the order has been increased for rows $\ell \neq \pi$ as the recurrence (11) is invertible. Multiplying row π of $\mathbf{M}$ by Z produces zeros in row π in the updated matrix, so that row π of H_λ must be kept. Finally, the adjustment from rows $\ell \neq \pi$ is again invertible. Therefore, the subspaces are the same.

In particular, it follows that, after the k-th iteration, the rows of $H_1 = \mathbf{R}_k(0)$ span the same space as all pivot rows plus the rows of H_{s+1}. Recalling the first $\lambda - 1$ columns of H_λ are zero by the order condition for Mahler systems, we see that $H_{s+1} = 0$. Since in addition the λ-th component of the pivot row at stage λ equals $r_\pi \neq 0$, the pivot rows form a full row rank upper echelon matrix, and $H_{s+1} = 0$. Hence $\text{rank } \mathbf{R}_k(0) = r$. □

We next prove a lemma on the pivots used in each iteration.

LEMMA 5.2. *The pivots used in one iteration of FFreduce are distinct, that is,* $\vec{\mu}^{k+1} \leq \vec{\mu}^k + \vec{e}$. *Moreover, rank* $\mathbf{R}_k(0)$ *is increasing in* k.

Proof: By Definition 2.2(b), there exists a polynomial $\mathbf{Q} \in \mathbb{Q}[Z;\sigma]^{m\times m}$ such that

$$Z \cdot \mathbf{M}_k = \mathbf{Q} \cdot \mathbf{M}_{k+1}, \quad deg\, \mathbf{Q}^{j,\ell} \leq \vec{\mu}_j^k + 1 - \vec{\mu}_\ell^{k+1} \text{ for all } j,\ell.$$

Comparing the coefficients at $Z^{\vec{\mu}_j^k+1}$ in position (j,ℓ), we have on the left a nonsingular lower triangular matrix (with $\sigma(d)$ on diagonal), and on the right the leading row coefficient matrix B of $\mathbf{Q}$ (with coefficients at power $\vec{\mu}_j^k+1-\vec{\mu}_\ell^{k+1}$) multiplied by a lower triangular matrix A. Since we are now in the quotient field, A must be nonsingular, and so B is also nonsingular and hence lower triangular. Hence the degrees on the diagonal cannot be smaller than 0, showing that $\vec{\mu}_j^k + 1 \geq \vec{\mu}_j^{k+1}$, or, in other words, $\vec{\mu}^{k+1} \leq \vec{\mu}^k + \vec{e}$. Thus, the pivots in one iteration are distinct. Also, denoting by C the trailing coefficient of $\mathbf{Q}$, we easily obtain that $C \cdot \mathbf{R}_{k+1}(0)$ coincides with the matrix obtained by applying σ to all elements of $\mathbf{R}_k(0)$ (which has the same rank as $\mathbf{R}_k(0)$). Hence the rank of $\mathbf{R}_k(0)$ is increasing. □

We are now ready to prove the correctness of the algorithm.

THEOREM 5.3. *The matrix* $\mathbf{R}$ *returned by FFreduce satisfies rank* $\mathbf{R}(0) =$ *rank* $\mathbf{F}$.

Proof: Since the rank cannot increase after multiplication with a square matrix, we get from $\mathbf{M}_k \cdot \mathbf{F} = \mathbf{R}_k \cdot Z^k$ the relation $\operatorname{rank}\mathbf{F} \geq \operatorname{rank}(\mathbf{R}_k \cdot Z^k) = \operatorname{rank}\mathbf{R}_k$. On the other hand, using the shifted left inverse $\mathbf{M}_k^*$ of $\mathbf{M}_k$ of Remark 2.3 we have that

$$\begin{aligned} \operatorname{rank}\mathbf{F} = \operatorname{rank}(Z^k \cdot \mathbf{F}) &= \operatorname{rank}(\mathbf{M}_k^* \cdot \mathbf{R}_k \cdot Z^k) \\ &\leq \operatorname{rank}(\mathbf{R}_k \cdot Z^k) = \operatorname{rank}\mathbf{R}_k, \end{aligned}$$

showing that $\operatorname{rank}\mathbf{F} = \operatorname{rank}\mathbf{R}_k$ for all k. If the algorithm stops after the $(k+1)$-st iteration, then

$$r = \operatorname{rank}\mathbf{R}_k(0) \leq \operatorname{rank}\mathbf{R}_{k+1}(0) \leq \operatorname{rank}\mathbf{R}_{k+1} \leq r$$

by Lemma 5.1, Lemma 5.2 and the fact that $\mathbf{R}_{k+1}$ contains r nonzero rows. Consequently, we have equality everywhere, and $r = \operatorname{rank}\mathbf{R}_{k+1} = \operatorname{rank}\mathbf{F}$. □

REMARK 5.4. *We have shown implicitly in the proof that, if we stop after iteration* $(k+1)$, *that the trailing coefficient of* $\mathbf{R}_k$ *already has full rank* r. *Since all the pivots in one iteration are distinct by Lemma 5.2, the set of pivot rows in* $\mathbf{R}_k(0)$ *also has rank* r. *Therefore, the submatrix of* $\mathbf{R}_k$ *consisting of the pivot rows already leads to a full rank decomposition (using the corresponding columns of the shifted left inverse of the previous Mahler system).* □

In order to determine the bit complexity of the FFreduce algorithm we make the assumption that the lengths and costs of coefficient arithmetic satisfies

$$\begin{aligned} length(a \cdot b) &= length(a) + length(b), \\ cost(a \cdot b) &= O(length(a) \cdot length(b)). \end{aligned}$$

Here *length* measures the total storage needed while *cost* measures the number of boolean operations. With this assumption we give our complexity in the following.

THEOREM 5.5. *If* $\mathbf{F}(Z)$ *has total degree* N *then Algorithm FFreduce requires at most* $m(N+1)$ *iterations. Moreover, if* K *is a bound on the lengths of the coefficients appearing in* $\mathbf{F}(Z), Z\cdot\mathbf{F}(Z), \ldots, Z^{m(N+1)+1}\cdot\mathbf{F}(Z)$, *then the bit complexity of the algorithm is* $O(m^5 s^4 N^4 K^2)$.

Proof: From the definition of $\mathbf{R}_k$ we see that $(N-k)\vec{e} + \vec{\mu}^k$ is an upper bound for the sum of the row degrees of $\mathbf{R}_k$. After iteration $k+1$, we know from Lemma 5.2 that a component of this upper bound either is constant (for pivot rows) or otherwise decreases by one. Since, by Lemma 5.1, for all but the last iteration there is at least one nonzero row in $\mathbf{R}_k$ which is not pivot (but which potentially could become a zero row in $\mathbf{R}_{k+1}$), we may conclude that either the sum of the degree bounds of nontrivial rows in $\mathbf{R}_{k+1}$ is lowered by at least 1, or we have created an additional zero row. Taking into account that the initial sum is bounded above by mN, we conclude that there are at most $m(N+1)$ iterations.

For bounding the bit complexity, we follow the complexity analysis in [8] where the upper bound $\mathcal{O}(m|\vec{\omega}|^4 K^2)$ has been established. The key observation is that all coefficients can be written as determinants by (8) and (10). Thus, Hadamard's inequality can be applied to obtain a bound on the lengths of the coefficients. □

REMARK 5.6. *We remark that since the cost of arithmetic in* $\mathbb{K}[n]$ *satisfies our complexity model when we are interested in field operations in* $\mathbb{K}$, *the same complexity bound is applicable for* $\mathbb{D} = \mathbb{K}[n]$ *with* K *being the maximum degree (in* n*) of all the coefficients in appearing in* $\mathbf{F}(Z), Z\cdot\mathbf{F}(Z), \ldots, Z^{m(N+1)+1}\cdot\mathbf{F}(Z)$. *Note that our complexity analysis takes into account the coefficient growth during the algorithm.*

6. CONCLUSION

In this paper we have given a fraction-free algorithm for transforming a given matrix of skew polynomials into one where the rank is determined only by the trailing or leading coefficient matrices. The algorithm is a modification of the FFFG algorithm of [8] in the commutative case. We have shown that our algorithm runs in polynomial time, with near-linear growth in the sizes of coefficients in the intermediate results.

There are a number of topics for future research. Our approach increases the degree of the rows of an order basis from first to last. In fact it is easy to see that one can alter this order, for example based on the minimum degree of the rows of the residual, while still making use the fraction-free

recursion given in this paper. This will be discussed in a coming paper.

We plan to investigate methods for improving the efficiency of our fraction-free approach. At present, our algorithm does not appear to do as well as the algorithm of Abramov and Bronstein [2] (as implemented in Maple 8) unless s is small. This is due to the fact that the coefficient growth in our algorithm is significant even though it is controlled. We would like to find fraction-free methods where linearly independent rows in the leading or trailing coefficient matrix are not modified during an iteration, a property satisfied by the approach in [2, 6].

Furthermore, it is well known that modular algorithms improve on fraction-free methods by an order of magnitude. An advantage of our fraction-free approach is that the result computed by our algorithm is well-defined and can be used as a target for reconstruction in modular algorithms. We expect to take advantage of the approach of Li [12] to reduce the coefficients in $\mathbb{Q}[n]$ to $\mathbb{Z}_p$ for some prime p to obtain an efficient modular algorithm for our rank revealing computations.

We also plan to see how our algorithm can be used to compute GCDs of scalar skew polynomials and compare it to the subresultant algorithms of Li [12]. Finally, we are interested in extending our results to nested skew polynomial domains, allowing for computations in Weyl algebras. This is a difficult extension since then the corresponding associated linear systems do not have commutative elements. As such the standard tools that we use from linear algebra, namely determinants and Cramer's rule, do not exist in the classic sense.

7. REFERENCES

[1] S. Abramov. EG-eliminations. *Journal of Difference Equations and Applications*, 5:393–433, 1999.

[2] S. Abramov and M. Bronstein. On solutions of linear functional systems. In *Proceedings of ISSAC 2001, London*, pages 1–6. ACM Press, 2001.

[3] E. Bareiss. Sylvester's identity and multistep integer-preserving Gaussian elimination. *Math. Comp.*, 22(103):565–578, 1968.

[4] B. Beckermann and G. Labahn. A uniform approach for Hermite Padé and simultaneous Padé approximants and their matrix generalization. *Numerical Algorithms*, 3:45–54, 1992.

[5] B. Beckermann and G. Labahn. A uniform approach for the fast, reliable computation of matrix-type Padé approximants. *SIAM J. Matrix Anal. Appl.*, 15:804–823, 1994.

[6] B. Beckermann and G. Labahn. Recursiveness in matrix rational interpolation problems. *J. Comput. Appl. Math.*, 77:5–34, 1997.

[7] B. Beckermann and G. Labahn. Effective computation of rational approximants and interpolants. *Reliable Computing*, 6:365–390, 2000.

[8] B. Beckermann and G. Labahn. Fraction-free computation of matrix GCD's and rational interpolants. *SIAM J. Matrix Anal. Appl.*, 22(1):114–144, 2000.

[9] W. Brown and J. Traub. On Euclid's algorithm and the theory of subresultants. *J. ACM*, 18:505–514, 1971.

[10] G. Collins. Subresultant and reduced polynomial remainder sequences. *J. ACM*, 14:128–142, 1967.

[11] K. Geddes, S. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer, Boston, MA, 1992.

[12] Z. Li. *A Subresultant Theory for Linear Differential, Linear Difference and Ore Polynomials, with Applications*. PhD thesis, Johannes Kepler Univ. Linz, Austria, 1996.