Computing the Hermite Form of a Matrix of Ore Polynomials

Mark Giesbrecht

Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada

Myung Sub Kim

Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada

Abstract

Let $\mathsf{F}[\partial;\sigma,\delta]$ be the ring of Ore polynomials over a field (or a skew field) F, where σ is an automorphism of F and δ is a σ-derivation. Given a matrix $A \in \mathsf{F}[\partial;\sigma,\delta]^{m\times n}$, we show how to compute the Hermite form H of A and a unimodular matrix U such that $UA = H$. The algorithm requires a polynomial number of operations in F in terms of the dimensions m and n, and the degrees (in ∂) of the entries in A. When $\mathsf{F} = \mathsf{k}(z)$ for some field k, it also requires time polynomial in the degrees in z of the coefficients of the entries, and if $\mathsf{k} = \mathbb{Q}$ it requires time polynomial in the bit length of the rational coefficients as well. Explicit analyses are provided for the complexity, in particular for the important cases of differential and shift polynomials over $\mathbb{Q}(z)$. To accomplish our algorithm, we apply the Dieudonné determinant and quasideterminant theory for Ore polynomial rings to get explicit bounds on the degrees and sizes of entries in H and U.

1. Introduction

The Ore polynomials are a natural algebraic structure which captures difference, q-difference, differential, and other non-commutative polynomial rings. The basic concepts of pseudo-linear algebra are presented nicely by Bronstein and Petkovšek (1996); see (Ore, 1931) for the seminal introduction.

On the other hand, canonical forms of matrices over commutative principal ideal domains (such as $\mathbb{Z}$ or $\mathsf{F}[x]$, for a field F) have proven invaluable for both mathematical and computational purposes. One of the successes of computer algebra over the past three decades has been the development of fast algorithms for computing these canonical forms. These include triangular forms such as the Hermite form (Hermite, 1851), low

Email addresses: mwg@uwaterloo.ca (Mark Giesbrecht), ms2kim@uwaterloo.ca (Myung Sub Kim).

degree forms like the Popov form (Popov, 1972), as well as the diagonal Smith form (Smith, 1861).

Canonical forms of matrices over non-commutative domains, especially rings of differential and difference operators, are also extremely useful. These have been examined at least since the work of Dickson (1923), Wedderburn (1932), and Jacobson (1943). Recently they have found uses in control theory (Chyzak, Quadrat, and Robertz, 2005; Zerz, 2006; Halás, 2008). Computations with multidimensional linear systems over Ore algebras are nicely developed by Chyzak, Quadrat, and Robertz (2007), and an excellent implementation of many fundamental algorithms is provided in the OreModules package of Maple.

In this paper we consider canonical forms of matrices of Ore polynomials over a skew field F. Let $\sigma : \mathsf{F} \to \mathsf{F}$ be an automorphism of F and $\delta : \mathsf{F} \to \mathsf{F}$ be a σ-derivation. That is, for any $a, b \in \mathsf{F}$, $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$. We then define $\mathsf{F}[\partial; \sigma, \delta]$ as the set of usual polynomials in $\mathsf{F}[\partial]$ under the usual addition, but with multiplication defined by

$$\partial a = \sigma(a)\partial + \delta(a)$$

for any $a \in \mathsf{F}$. This is well-known to be a left (and right) principal ideal domain, with a straightforward Euclidean algorithm (see (Ore, 1933)).

Some important cases over the field of rational functions $\mathsf{F} = \mathsf{k}(z)$ over a field k are as follows:

(1) $\sigma(z) = \mathcal{S}(z) = z + 1$ is a so-called *shift* automorphism of $\mathsf{k}(z)$, and δ identically zero on k. Then $\mathsf{k}(z)[\partial; \mathcal{S}, 0]$ is generally referred to as the ring of *shift polynomials*. With a slight abuse of notation we write $\mathsf{k}(z)[\partial; \mathcal{S}]$ for this ring.

(2) $\delta(z) = 1$ and $\sigma(z) = z$, so $\delta(h(z)) = h'(z)$ for any $h \in \mathsf{k}(z)$ with h' its usual derivative. Then $\mathsf{k}(z)[\partial; \sigma, \delta]$ is called the ring of *differential polynomials*. With a slight abuse of notation we write $\mathsf{k}(z)[\partial; \prime]$ for this ring.

A primary motivation in the definition of $\mathsf{k}(z)[\partial; \prime]$ is that there is a natural action on the space of infinitely differentiable functions in z, namely the differential polynomial

$$a_m\partial^m + a_{m-1}\partial^{m-1} + \cdots + a_1\partial + a_0 \in \mathsf{k}(z)[\partial; \prime]$$

acts as the linear differential operator

$$a_m(z)\frac{d^m f(z)}{dz^m} + a_{m-1}(z)\frac{d^{m-1} f(z)}{dz^{m-1}} + \cdots + a_1(z)\frac{df(z)}{dz} + a_0(z)f(z)$$

on an infinitely differentiable function $f(z)$. See (Bronstein and Petkovšek, 1996).

The (row) Hermite form we will compute here is achieved purely by row operations, and we treat a matrix $A \in \mathsf{F}[\partial; \sigma, \delta]^{m \times n}$ as generating the left $\mathsf{F}[\partial; \sigma, \delta]$-module of its rows. Thus, by *left row rank*, we mean the rank of the free left $\mathsf{F}[\partial; \sigma, \delta]$-module of rows of A, and will denote this simply as the *rank* of A for the remainder of the paper. A matrix $H \in \mathsf{F}[\partial; \sigma, \delta]^{m \times n}$ of rank r is in *Hermite form* if an only if

(i) Only the first r rows are non-zero;

(ii) In each row the leading (first non-zero) element is monic;

(iii) All entries in the column below the leading element in any row are zero;

(iv) All entries in the column above the leading element in any row are of lower degree than the leading element.

For square matrices of full rank the Hermite form will thus be upper triangular with monic entries on the diagonal, whose degrees dominate all other entries in their column.

For example, in the differential polynomial ring $\mathbb{Q}(z)[\partial;\prime]$ as above:

$$A = \begin{pmatrix} 1+(z+2)\partial+\partial^2 & 2+(2z+1)\partial & 1+(1+z)\partial \\ (2z+z^2)+z\partial & (2+2z+2z^2)+\partial & 4z+z^2 \\ (3+z)+(3+z)\partial+\partial^2 & (8+4z)+(5+3z)\partial+\partial^2 & (7+8z)+(2+4z)\partial \end{pmatrix} \in \mathbb{Q}(z)[\partial;\prime]^{3\times 3} \quad (1.1)$$

has Hermite form

$$H = \begin{pmatrix} (2+z)+\partial & 1+2z & \frac{-2+z+2z^2}{2z} - \frac{1}{2z}\partial \\ 0 & (2+z)+\partial & 1+\frac{7z}{2}+\frac{1}{2}\partial \\ 0 & 0 & -\frac{2}{z}+\frac{-1+2z+z^2}{z}\partial+\partial^2 \end{pmatrix} \in \mathbb{Q}(z)[\partial;\prime]^{3\times 3}.$$

Note that the Hermite form may have denominators in z. Also, while this example does not demonstrate it, the degrees in the Hermite form, in both numerators and denominators in z and ∂, are generally substantially larger than in the input (in Theorem 5.6 we will provide polynomial, though quite large, bounds on these degrees, and suspect these bounds may well be met generically).

For any matrix $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ of full rank, there exists a unique unimodular matrix $U \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ (i.e., a matrix whose inverse exists and is also in $\mathsf{F}[\partial;\sigma,\delta]^{n\times n}$) such that $UA = H$ is in Hermite form. This form is canonical in the sense that if two matrices $A, B \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ are such that $A = PB$ for unimodular $P \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ then the Hermite form of A equals the Hermite form of B. Existence and uniqueness of the Hermite form are established much as they are over $\mathbb{Z}^{n\times n}$ in Section 2. For rank deficient matrices and rectangular matrices, the Hermite form also exists but the transformation matrix may not be unique. See Section 6 for further details.

In commutative domains such as $\mathbb{Z}$ and $\mathsf{F}[x]$ there have been enormous advances in the past two decades in computing Hermite, Smith and Popov forms. Polynomial-time algorithms for the Smith and Hermite forms over $\mathsf{F}[x]$ were developed by Kannan (1985), with important advances by Kaltofen, Krishnamoorthy, and Saunders (1987), Villard (1995), Mulders and Storjohann (2003), Pernet and Stein (2010), and many others. One of the key features of this recent work in computing canonical forms has been a careful analysis of the complexity in terms of matrix size, entry degree, and coefficient swell. Clearly identifying and analyzing the cost in terms of all these parameters has led to a dramatic drop in both theoretical and practical complexity.

Computing the classical Smith and Hermite forms of matrices over Ore domains has received less attention though canonical forms of differential polynomial matrices have applications in solving differential systems and control theory (see (Halás, 2008; Kotta, Leiback, and Halás, 2008)). Abramov and Bronstein (2001) analyze the number of reduction steps necessary to compute a *row-reduced form*, while Beckermann, Cheng, and Labahn (2006) analyze the complexity of row reduction in terms of matrix size, degree and the sizes of the coefficients of some shifts of the input matrix. Beckermann et al. (2006) demonstrate tight bounds on the degree and coefficient sizes of the output, which we will employ here. For the Popov form, Cheng (2003) gives an algorithm for matrices of shift polynomials. Cheng's approach involves order

bases computation in order to eliminate lower order terms of Ore polynomial matrices. A main contribution of Cheng (2003) is to give an algorithm computing the rank and a row-reduced basis of the left nullspace of a matrix of Ore polynomials in a fraction-free way. This idea is extended in Davies, Cheng, and Labahn (2008) to compute the Popov form of general Ore polynomial matrices. They reduce the problem of computing Popov form to a nullspace computation. However, though Popov form is useful for rewriting high order terms with respect to low order terms, we want a different canonical form more suited to solving system of linear diophantine equations. Since the Hermite form is upper triangular, it meets this goal nicely, not to mention the fact that it is a "classical" canonical form. An implementation of the basic (exponential-time) Hermite algorithm is provided by Culianez (2005). In (Giesbrecht and Kim, 2009), we present a polynomial-time algorithm for the Hermite form over $\mathbb{Q}(z)[\partial;']$, for full rank square matrices. While it relies on similar techniques as this current paper, the cost of the algorithm is higher, the coefficient bounds weaker, and it does not work for matrices of general Ore polynomials.

The related "two-sided" problem of computing the Jacobson (non-commutative Smith) canonical form has also been recently considered. Blinkov, Cid, Gerdt, Plesken, and Robertz (2003) implement the standard algorithm in the package *Janet*. Levandovskyy and Schindelar (2011) provide a very complete implementation, for the full Ore case over skew fields, of a Jacobson form algorithm using Gröbner bases in Singular. Middeke (2008) has recently demonstrated that the Jacobson form of a matrix of differential polynomials can be computed in time polynomial in the matrix size and degree (but the coefficient size is not analyzed). Giesbrecht and Heinle (2012) give a probabilistic polynomial-time algorithm for this problem in the differential case.

One of the primary difficulties in both developing efficient algorithms for matrices of Ore polynomials, and in their analysis, is the lack of a standard notion of determinant, and the important bounds this provides on degrees in eliminations. In Section 3 we establish bounds on the degrees of entries in the inverse of a matrix over any non-commutative field with a reasonable degree function. We do this by introducing the *quasideterminant* of Gel'fand and Retakh (1991, 1992) and analyzing its interaction with the degree function. We also prove similar bounds on the degree of the Dieudonné determinant. In both cases, the bounds are essentially the same as for matrices over a commutative function field.

In Section 4 we consider matrices over the Ore polynomials and bound the degrees of entries in the Hermite form and corresponding unimodular transformation matrices. We also bound the degrees of the Dieudonné determinants of these matrices.

In Section 5 we present our algorithm for the Hermite form. The degree bounds and costs of our algorithms are summarized as follows, from Theorems 4.7, 4.9 and 5.6.

Summary Theorem. Let $A \in \mathsf{k}[z][\partial;\sigma,\delta]^{n\times n}$ have full rank with entries of degree at most d in ∂, and coefficients of degree at most e in z. Let $H \in \mathsf{k}(z)[\partial;\sigma,\delta]^{n\times n}$ be the Hermite form of A and $U \in \mathsf{k}(z)[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$.

(a) The sum of degrees in ∂ in any row of H is at most nd, and each entry in U has degree in ∂ at most $(n-1)d$.

(b) All coefficients from $\mathsf{k}(z)$ of entries of H and U have degrees in z, of both numerators and denominators, bounded by $O(n^2de)$.

(c) We can compute H and U deterministically with $O^{\sim}(n^9d^4e)$ [†], operations in k.

[†] We employ soft-Oh notation: for functions σ and φ we say $\sigma \in O^{\sim}(\varphi)$ if $\sigma \in O(\varphi \log^c \varphi)$ for some constant $c \geq 0$.

(d) Assume k has at least $4n^2de$ elements. We can compute the Hermite form H and U with an expected number of $O^{\sim}(n^7d^3e)$ of operations in k using standard polynomial arithmetic. This algorithm is probabilistic of the Las Vegas type; it never returns an incorrect answer.

The cost of our algorithm for Ore polynomials over an arbitrary skew field, as well as over more specific fields like $\mathbb{Q}(z)$, is also shown to be polynomially bounded, and is discussed in Section 5.

It should be noted from the above theorem that the output is of quite substantial size. The transformation matrix U as above is an $n \times n$ matrix of polynomials in ∂ of degree bounded by nd in ∂ and each coefficient has degree bounded by n^2de, for a total size of $O(n^5d^2e)$ elements of k. While we have not proven our size bounds are tight, we have some confidence they are quite strong.

The algorithm presented in Section 5 is derived from the "linear systems" approach of Kaltofen et al. (1987) and Storjohann (1994). In particular, it reduces the problem to that of linear system solving over the generally commutative ground field (e.g., $\mathsf{k}(z)$). There are efficient algorithms and implementations for solving this problem. While we expect that further algorithmic refinements and reductions in cost can be achieved before an industrial-strength implementation is made, the general approach of reducing to well-studied computational problem in a commutative domain would seem to have considerable merit in theory and practice.

In Section 6 we show that for the case of rank-deficient and rectangular matrices, the computation of the Hermite form is reduced to the full rank, square case.

2. Existence and Uniqueness of the Hermite form over Ore domains

In this section we establish the basic existence and uniqueness of Hermite forms over Ore domains. These follow similarly to the traditional proofs over $\mathbb{Z}$; see for example (Newman, 1972, Theorems II.2 and II.3), which we outline below.

Fact 2.1 (Jacobson (1943), Section 3.7)**.** *Let $a, b \in \mathsf{F}[\partial; \sigma, \delta]$, not both zero with $g = \operatorname{gcrd}(a, b)$, $u, v \in \mathsf{F}[\partial; \sigma, \delta]$ such that $ua + vb = g$, and $s, t \in \mathsf{F}[\partial; \sigma, \delta]$ such that $sa = -tb = \operatorname{lclm}(a, b)$. Then*

$$W = \begin{pmatrix} u & v \\ s & t \end{pmatrix} \in \mathsf{F}[\partial; \sigma, \delta]^{2\times 2} \quad \text{is such that} \quad W \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix},$$

and W is unimodular.

This is easily generalized to $n \times n$ matrices as follows.

Lemma 2.2. *Let $w = (w_1, \ldots, w_n)^T \in \mathsf{F}[\partial; \sigma, \delta]^{n\times 1}$, and $i, j \in \{1, \ldots, n\}$. There exists a matrix*

$$E = E(i, j; w) \in \mathsf{F}[\partial; \sigma, \delta]^{n\times n}$$

such that $Ew = (u_1, \ldots, u_n)^T \in \mathsf{F}[\partial; \sigma, \delta]^{n\times 1}$, with $u_i = \operatorname{gcrd}(w_i, w_j)$ and $u_j = 0$.

Proof. If both $w_i = w_j = 0$ are zero, then E is the identity matrix. If $w_i = 0$ and $w_j \neq 0$, then let E be the permutation matrix which swaps rows j and i.

Otherwise, let $W = \begin{pmatrix} u & v \\ s & t \end{pmatrix}$ be as in Fact 2.1 with $(a,b)^T = (w_i, w_j)^T$, and $W(w_i, w_j)^T = (g, 0)^T$ for $g = \mathrm{gcrd}(w_i, w_j)$. Define $E(i, j; w)$ as the identity matrix except

$$E_{ii} = u, \quad E_{ij} = v, \quad E_{ji} = s, \quad E_{jj} = t.$$

Clearly E satisfies the desired properties. □

We note that off diagonal entries in a triangular matrix can be unimodularly reduced by the diagonal entry below it.

Lemma 2.3. *Let $J \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$ be upper triangular with non-zero diagonal. There exists a unimodular matrix $R \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$, which is upper triangular and has ones on the diagonal, such that in every column of RJ, the degree of each diagonal entry is strictly larger than the degrees of the entries above it.*

Proof. For any $a, b \in \mathsf{F}[\partial; \sigma, \delta]$ with $b \neq 0$, we have $a = qb + r$ for quotient $q \in \mathsf{F}[\partial; \sigma, \delta]$ and remainder $r \in \mathsf{F}[\partial; \sigma, \delta]$ with $\deg_\partial r < \deg_\partial b$, and

$$\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r \\ b \end{pmatrix}.$$

Embedding such unimodular matrices Q into $n \times n$ identity matrices, we can "reduce" the off diagonal entries of J by the diagonal entries below them. □

Theorem 2.4. *Let $A \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$ have full rank. Then there exists a matrix $H \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$ in Hermite form, and a unimodular matrix $U \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$, such that $UA = H$.*

Proof. The proof follows by observing the traditional (but inefficient) algorithm to compute the Hermite form. We first use a (unimodular row) permutation to move any non-zero element in column 1 into the top left position; failure to find a non-zero element in column 1 means our matrix is rank deficient. We then repeatedly apply Lemma 2.2 to find Q_1 such that $Q_1 A$ only has the top left position non-zero. This same procedure is then repeated on subdiagonal of columns $2, 3, \ldots, n$ in sequence, so there exists a unimodular matrix $Q = Q_1 \cdots Q_n$ such that QA is upper triangular. The matrix is then unimodularly reduced using Lemma 2.3. □

Theorem 2.5. *Let $A \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$ have full row rank. Suppose $UA = H$ for unimodular $U \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$ and Hermite form $H \in \mathsf{F}[\partial; \sigma, \delta]^{n \times n}$. Then both U and H are unique.*

$A = U^{-1}H$, $G = VA = VU^{-1}H$ also unimodular

Proof. Suppose H and G are both Hermite forms of A. Thus, there exist unimodular matrices U and V such that $UA = H$ and $VA = G$, and $G = WH$ where $W = VU^{-1}$ is unimodular. Since G and H are upper triangular matrices, we know W is as well. Moreover, since G and H have monic diagonal entries, the diagonal entries of W equal 1. We now prove W is the identity matrix. By way of contradiction, first assume that W is not the identity, so there exists an entry W_{ij} which is the first nonzero off-diagonal entry on the ith row of W. Since $i < j$ and since $W_{ii} = 1$, $G_{ij} = H_{ij} + W_{ij}H_{jj}$. Because $W_{ij} \neq 0$, we see $\deg_\partial G_{ij} \geq \deg_\partial G_{jj}$, which contradicts the definition of the Hermite form.

Uniqueness of U is easily established since $UA = VA$, so $U^{-1}V = I$ and $U = V$. □

3. Non-commutative determinants and degree bounds for linear equations

One of the main difficulties in matrix computations in skew (non-commutative) fields, and a primary difference with the commutative case, is the lack of the usual determinant. In particular, the determinant allows us to bound the degrees of solutions to systems of equations, the size of the inverse or other decompositions, not to mention the degrees at intermediate steps of computations, through Hadamard-like formulas and Cramer's rules.

The most common non-commutative determinant was defined by Dieudonné (1943), and is commonly called the *Dieudonné determinant*. It preserves some of the multiplicative properties of the usual commutative determinant, but is insufficient to establish the degree bounds we require (amongst other inadequacies). Gel'fand and Retakh (1991, 1992) introduced *quasideterminants* and a rich associated theory as a central tool in linear algebra over non-commutative rings. Quasideterminants are more akin to the (inverse of the) entries of the classical adjoint of a matrix than a true determinant. We employ quasideterminants here to establish bounds on the degree of the entries in the inverse of a matrix, and on the Dieudonné determinant in this section, and on the Hermite form and its multiplier matrices in Section 4.

We will establish bounds on degrees of quasideterminants and Dieudonné determinants for a general skew field K with a *degree* $\deg : \mathsf{K} \to \mathbb{Z} \cup \{-\infty\}$ satisfying the following properties. For $a, b \in \mathsf{K}$:

(i) If $a \neq 0$ then $\deg a \in \mathbb{Z}$, and $\deg 0 = -\infty$;
(ii) $\deg(a + b) \leq \max\{\deg a, \deg b\}$;
(iii) $\deg(ab) = \deg a + \deg b$;
(iv) If $a \neq 0$ then $\deg(a^{-1}) = -\deg a$.

As a simple commutative example, if $\mathsf{K} = \mathsf{F}(y)$ for some field F and commuting indeterminate y, for any $a = a_N/a_D$ with polynomials $a_N, a_D \in \mathsf{F}[y]$ ($a_D \neq 0$), we can define $\deg a = \deg a_N - \deg a_D$.

More properly, our degree function is a *non-archimedean valuation* on K. Since our main application will be to non-commutative Ore polynomial rings, where degrees are a natural and traditional notion, we will adhere to the nomenclature of degrees. *We note, however, that the degrees as defined here may become negative.* See Lemma 4.3 for the effective application to the Ore polynomial case.

3.1. Quasideterminants and degree bounds

Following Gel'fand and Retakh (1991, 1992), we define the *quasideterminant* as a collection of n^2 functions from $\mathsf{K}^{n\times n} \to \mathsf{K} \cup \{\perp\}$, where $\perp$ represents the function being *undefined*. Let $A \in \mathsf{K}^{n\times n}$ and $p, q \in \{1, \ldots, n\}$. Assume $A_{pq} \in \mathsf{K}$ is the (p, q) entry of A, and let $A^{(pq)} \in \mathsf{K}^{(n-1)\times(n-1)}$ be the matrix A with the pth row and qth column removed. Define the (p, q)-quasideterminant of A as

$$|A|_{pq} = A_{pq} - \sum_{i\neq p, j\neq q} A_{pi}(|A^{(pq)}|_{ji})^{-1}A_{jq},$$

where the sum is taken over all summands where $|A^{(pq)}|_{ji}$ is defined. If all summands have $|A^{(pq)}|_{ji}$ undefined then $|A|_{pq}$ is undefined (and has value $\perp$). See (Gel'fand and Retakh, 1992).

Fact 3.1 (Gel'fand and Retakh (1991), Theorem 1.6)**.** *Let $A \in \mathsf{K}^{n\times n}$ over a (possibly skew) field K.*

(1) The inverse matrix $B = A^{-1} \in \mathsf{K}^{n\times n}$ exists if and only if the following are true:
- *(a) If the quasideterminant $|A|_{ij}$ is defined then $|A|_{ij} \neq 0$, for all $i, j \in \{1, \ldots, n\}$;*
- *(b) For all $p \in \{1, \ldots, n\}$ there exists a $q \in \{1, \ldots, n\}$, such that the quasideterminant $|A|_{pq}$ is defined;*
- *(c) For all $q \in \{1, \ldots, n\}$ there exists a $p \in \{1, \ldots, n\}$ such that the quasideterminant $|A|_{pq}$ is defined;*

(2) If the inverse B exists, then for $i, j \in \{1, \ldots, n\}$ we have

$$B_{ji} = \begin{cases} (|A|_{ij})^{-1} & \text{if } |A|_{ij} \text{ is defined,} \\ 0 & \text{if } |A|_{ij} \text{ is not defined.} \end{cases}$$

Over a commutative field K, where $A \in \mathsf{K}^{n\times n}$ has inverse B, the quasideterminants behave like a classical adjoint: $|A|_{ij} = (-1)^{i+j} \det A / \det A^{(ij)} = 1/B_{ji}$. If B_{ji} is zero then $|A|_{ij}$ is undefined.

We now bound the size of the quasideterminants in terms of the size of the entries of A. Assume that K has a degree function as above.

Theorem 3.2. *Let $A \in \mathsf{K}^{n\times n}$, such that either $A_{ij} = 0$ or $0 \leq \deg A_{ij} \leq d$ for all $i, j \in \{1, \ldots, n\}$. For all $p, q \in \{1, \ldots, n\}$ such that $|A|_{pq}$ is defined we have $-(n-1)d \leq \deg |A|_{pq} \leq nd$.*

Proof. We proceed by induction on n.

For $n = 1$, $p = q = 1$ and $|A|_{11} = A_{11}$, so clearly the property holds. Assume the statement is true for dimension $n - 1$. Then

$$\deg |A|_{pq} = \deg \left(A_{pq} - \sum_{i\neq p, j\neq q} A_{pi}(|A^{(pq)}|_{ji})^{-1}A_{jq} \right),$$

where the sum is over all defined summands. Then using the inductive hypothesis we have

$$\begin{aligned} \deg |A|_{pq} &\leq \max \left\{ \deg A_{pq}, \max_{i\neq p, j\neq q} \left\{ \deg A_{pi} - \deg |A^{(pq)}|_{ji} + \deg A_{jq} \right\} \right\} \\ &\leq 2d + (n-2)d \leq nd, \end{aligned}$$

and

$$\deg |A|_{pq} \geq -\deg |A^{(pq)}|_{ji} \geq -(n-1)d. \qquad \square$$

Corollary 3.3. *Let $A \in \mathsf{K}^{n\times n}$ be unimodular, and $B \in \mathsf{K}^{n\times n}$ such that $AB = I$. Assume $A_{ij} = 0$ or $0 \leq \deg A_{ij} \leq d$ for all $i, j \in \{1, \ldots, n\}$. Then $\deg B \leq (n-1)d$.*

Proof. From Fact 3.1 we know that $B_{ji} = (|A|_{ij})^{-1}$ when $|A|_{ij}$ is defined (and $B_{ji} = 0$ otherwise). Thus $\deg B_{ji} = -\deg |A|_{ij} \leq (n-1)d$, and $B_{ij} = 0$ or $\deg B_{ij} \geq 0$ since A is unimodular. $\square$

3.2. Dieudonné Determinants

Let $[\mathsf{K}^*, \mathsf{K}^*]$ be the *commutator subgroup* of the multiplicative group K^* of K, the (normal) subgroup of K^* generated by all pairs of elements of the form $a^{-1}b^{-1}ab$ for $a, b \in \mathsf{K}^*$. Thus $\mathsf{K}^*/[\mathsf{K}^*, \mathsf{K}^*]$ is a commutative group.

Let $A \in \mathsf{K}^{n\times n}$ be a matrix with a right inverse. The *Bruhat Normal Form* of A is a decomposition $A = TDPV$, where $P \in \mathsf{K}^{n\times n}$ is a permutation matrix inducing the permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, and $T, D, V \in \mathsf{K}^{n\times n}$ are

$$T = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}, \qquad D = \operatorname{diag}(u_1, \ldots, u_n), \qquad V = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ * & \cdots & * & 1 \end{pmatrix}.$$

See (Draxl, 1983, Chapter 19) for more details. The Bruhat decomposition arises from Gaussian elimination, much as the LUP decomposition does in the commutative case. We then define $\delta\varepsilon\tau(A) = \operatorname{sign}(\sigma) \cdot u_1 \cdots u_n \in \mathsf{K}$ (sometimes called the *pre-determinant* of A). Let π be the canonical projection from $\mathsf{K}^* \to \mathsf{K}/[\mathsf{K}^*, \mathsf{K}^*]$. Then the Dieudonné determinant is defined as $\mathcal{D}\mathrm{et}(A) = \pi(\delta\varepsilon\tau(A)) \in \mathsf{K}/[\mathsf{K}^*, \mathsf{K}^*]$, or $\mathcal{D}\mathrm{et}(A) = 0$ if A is not invertible.

The Dieudonné determinant has a number of the desirable properties of the usual determinant, as proven in (Dieudonné, 1943):

(1) $\mathcal{D}\mathrm{et}(AB) = \mathcal{D}\mathrm{et}(A)\,\mathcal{D}\mathrm{et}(B)$ for any $A, B \in \mathsf{K}^{n\times n}$;
(2) $\mathcal{D}\mathrm{et}(P) = 1$ for any permutation matrix;
(3) $\mathcal{D}\mathrm{et}\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \mathcal{D}\mathrm{et}(A)\,\mathcal{D}\mathrm{et}(B)$.

Also note that if K has a degree function as above, then $\deg(\mathcal{D}\mathrm{et}(A))$ is well defined, since all elements of the equivalence class of $\pi(\mathcal{D}\mathrm{et}(A))$ have the same degree (since the degree of all members of the commutator subgroup is zero). Gel'fand and Retakh (1991) show that

$$\begin{aligned} \delta\varepsilon\tau(A) &= |A|_{11}|A^{(11)}|_{22}|A^{(12,12)}|_{33}|A^{(123,123)}|_{44}\cdots|A^{(1\ldots n-1,1\ldots,n-1)}|_{nn} \\ &= |A|_{11} \cdot \delta\varepsilon\tau(A^{(11)}), \end{aligned}$$

when all these quasideterminants are defined (or equivalently P is the identity in the Bruhat decomposition above), where $A^{(1\dots k,1\dots k)}$ is the matrix A with rows $1\dots k$ and columns $1\dots k$ removed (keeping the original labelings of the remaining rows and columns).

More generally, let $R = (r_1, \dots, r_n)$, $C = (c_1, \dots, c_n)$ be permutations of $\{1, \dots, n\}$, let $R_k = (r_1, \dots, r_k)$, $C_k = (c_1, \dots, c_k)$, and define $A^{(R_k, C_k)}$ as the matrix A with rows $r_1, \dots, r_k$ and columns $c_1, \dots, c_k$ removed (where $A^{(R_0, C_0)} = A$). Define

$$\begin{aligned}\delta\varepsilon\tau_{R,C}(A) &= |A|_{r_1,c_1}|A^{(R_1,C_1)}|_{r_2,c_2}|A^{(R_2,C_2)}|_{r_3,c_3}\cdots|A^{(R_{n-1},C_{n-1})}|_{r_n,c_n} \\ &= |A|_{r_1,c_1}\cdot\delta\varepsilon\tau_{R,C}(A^{(r_1,c_1)}) \\ &= |A|_{r_1,c_1}\cdot|A^{(R_1,C_1)}|_{r_2,c_2}\cdot\delta\varepsilon\tau(A^{(R_2,C_2)}).\end{aligned} \tag{3.1}$$

Fact 3.4 (Gelfand, Gelfand, Retakh, and Wilson (2005), Section 3.1)**.** *Let R, C be permutations of $\{1, \dots, n\}$ and R_k, C_k defined as above. If $|A^{(R_k,C_k)}|_{r_{k+1},c_{k+1}}$ is defined for $k = 0 \dots n-1$, then*

$$\mathcal{D}\mathrm{et}(A) = \mathrm{sign}(R)\cdot\mathrm{sign}(C)\cdot\pi(\delta\varepsilon\tau_{R,C}(A)).$$

In other words, the Dieudonné determinant is essentially invariant of the order of the sequence of submatrices specified in (3.1).

Theorem 3.5. *Let $A \in \mathsf{K}^{n\times n}$ be invertible, with $\deg A_{ij} \le d$. Then $\deg \mathcal{D}\mathrm{et}(A) \le nd$.*

Proof. We proceed by induction on n. For $n = 1$ this is clear. For $n = 2$, the possible predeterminants are

$$\begin{aligned}\delta\varepsilon\tau_{12,12}(A) &= |A|_{11}A_{22} = (A_{11} - A_{12}A_{22}^{-1}A_{21})A_{22}, \\ \delta\varepsilon\tau_{12,21}(A) &= |A|_{12}A_{21} = (A_{12} - A_{11}A_{21}^{-1}A_{22})A_{21}, \\ \delta\varepsilon\tau_{21,12}(A) &= |A|_{21}A_{22} = (A_{21} - A_{22}A_{12}^{-1}A_{11})A_{12}, \\ \delta\varepsilon\tau_{21,21}(A) &= |A|_{22}A_{11} = (A_{22} - A_{21}A_{11}^{-1}A_{12})A_{11},\end{aligned}$$

at least one of which must be defined and non-zero, and all of which clearly have degree at most $2d$.

Now assume the theorem is true for matrices of dimension less than n. Choose $r_1, c_1 \in \{1, \dots, n\}$ such that $|A|_{r_1,c_1}$ is non-zero and of minimal degree; that is $\deg|A|_{r_1,c_1} \le \deg|A|_{k,\ell}$ for all k, ℓ such that $|A|_{k,\ell}$ is defined and non-zero. The fact that $|A|_{r_1,c_1} \neq 0$ implies that $A^{(r_1,c_1)}$ is invertible, and we can continue this process recursively. Thus, let $R = (r_1, \dots, r_n)$ and $C = (c_1, \dots, c_n)$ be permutations of $\{1, \dots, n\}$ such that $|A^{(R_i,C_i)}|_{r_{i+1},c_{i+1}} \neq 0$ and $\deg|A^{(R_i,C_i)}|_{r_{i+1},c_{i+1}}$ is minimal over the degrees of non-zero,

defined quasideterminants $|A^{(R_i,C_i)}|_{k,\ell}$, for $0 \le i < n$. Now

$$\begin{aligned}
\delta\varepsilon\tau_{R,C}(A) &= |A|_{r_1,c_1} \cdot |A^{(r_1,c_1)}|_{r_2,c_2} \cdot \delta\varepsilon\tau_{R,C}(A^{(R_2,C_2)}) \\
&= \left(A_{r_1,c_1} - \sum_{k,\ell} A_{r_1 k} |A^{(r_1,c_1)}|^{-1}_{\ell k} A_{\ell c_1} \right) \cdot |A^{(r_1,c_1)}|_{r_2,c_2} \cdot \delta\varepsilon\tau_{R,C}(A^{(R_2,C_2)}) \\
&= A_{r_1,c_1} \cdot |A^{(r_1,c_1)}|_{r_2,c_2} \cdot \delta\varepsilon\tau_{R,C}(A^{(R_2,C_2)}) \\
&\quad - \sum_{k,\ell} A_{r_1 k} |A^{(r_1,c_1)}|^{-1}_{\ell k} A_{\ell c_1} \cdot |A^{(r_1,c_1)}|_{r_2,c_2} \cdot \delta\varepsilon\tau_{R,C}(A^{(R_2,C_2)}) \\
&= A_{r_1,c_1} \cdot \delta\varepsilon\tau_{R,C}(A^{(R_1,C_1)}) \\
&\quad - \sum_{k,\ell} A_{r_1 k} |A^{(r_1,c_1)}|^{-1}_{\ell k} A_{\ell c_1} \cdot |A^{(r_1,c_1)}|_{r_2,c_2} \cdot \delta\varepsilon\tau_{R,C}(A^{(R_2,C_2)}),
\end{aligned}$$

where all sums are taken only over defined quasideterminants as above. Thus

$$\deg \mathcal{D}\mathrm{et}(A) = \deg \delta\varepsilon\tau_{R,C}(A) \le \max\{d + (n-1)d, 2d + (n-2)d\} \le nd,$$

using the induction hypothesis and the assumption that $\deg |A^{(r_1,c_1)}|_{r_2,c_2}$ is chosen to be minimal. □

4. Degree bounds on matrices over $\mathsf{F}[\partial; \sigma, \delta]$

Some well-known properties of $\mathsf{F}[\partial; \sigma, \delta]$ are worth recalling; see (Ore, 1933) for the original theory or (Bronstein and Petkovšek, 1994) for an algorithmic presentation. Given $f, g \in \mathsf{F}[\partial; \sigma, \delta]$, there is a degree function (in ∂) which satisfies the usual properties: $\deg_\partial(fg) = \deg_\partial f + \deg_\partial g$ and $\deg_\partial(f+g) \le \max\{\deg_\partial f, \deg_\partial g\}$. We set $\deg_\partial 0 = -\infty$. $\mathsf{F}[\partial; \sigma, \delta]$ is a left (and right) principal ideal ring, which implies the existence of a right (and left) division with remainder algorithm such that there exists unique $q, r \in \mathsf{F}[\partial; \sigma, \delta]$ such that $f = qg + r$ where $\deg_\partial(r) < \deg_\partial(g)$. This allows for a right (and left) Euclidean-like algorithm which shows the existence of a greatest common right divisor, $h = \mathrm{gcrd}(f, g)$, a polynomial of minimal degree (in ∂) such that $f = uh$ and $g = vh$ for $u, v \in \mathsf{F}[\partial; \sigma, \delta]$. The GCRD is unique up to a left multiple in $\mathsf{F}\backslash\{0\}$, and there exist co-factors $a, b \in \mathsf{F}[\partial; \sigma, \delta]$ such that $af + bg = \mathrm{gcrd}(f, g)$. There also exists a least common left multiple $\mathrm{lclm}(f, g)$. Analogously there exists a greatest common left divisor, $\mathrm{gcld}(f, g)$, and least common right multiple, $\mathrm{lcrm}(f, g)$, both of which are unique up to a right multiple in F. From (Ore, 1933) we also have that

$$\begin{cases} \deg_\partial \mathrm{lclm}(f, g) = \deg_\partial f + \deg_\partial g - \deg_\partial \mathrm{gcrd}(f, g), \\ \deg_\partial \mathrm{lcrm}(f, g) = \deg_\partial f + \deg_\partial g - \deg_\partial \mathrm{gcld}(f, g). \end{cases} \tag{4.1}$$

It will be useful to work in the quotient skew field $\mathsf{F}(\partial; \sigma, \delta)$ of $\mathsf{F}[\partial; \sigma, \delta]$, and to extend the degree function $\deg_\partial$ appropriately. We first show that any element of $\mathsf{F}(\partial; \sigma, \delta)$ can be written as a *standard fraction* fg^{-1}, for $f, g \in \mathsf{F}[\partial; \sigma, \delta]$ (and in particular, since $\mathsf{F}[\partial; \sigma, \delta]$ is non-commutative, we insist that g^{-1} is on the right).

Fact 4.1 (Ore (1933), Section 3)**.** *Every element of* $\mathsf{F}(\partial; \sigma, \delta)$ *can be written as a standard fraction.*

$\sigma f = M f \qquad M f = b$

$f = M^{-1} b$

The notion of degree extends naturally to $\mathsf{F}(\partial;\sigma,\delta)$ as follows.

Definition 4.2. For $f,g\in\mathsf{F}[\partial;\sigma,\delta]$, $g\neq 0$, the *degree* $\deg_\partial(fg^{-1})=\deg_\partial f-\deg_\partial g$.

The proof of the next lemma is left to the reader.

Lemma 4.3. *For $f,g,u,v\in\mathsf{F}[\partial;\sigma,\delta]$, with $g,v\neq 0$, we have the following:*
(a) if $fg^{-1}=uv^{-1}$ then $\deg_\partial(fg^{-1})=\deg_\partial(uv^{-1})$;
(b) $\deg_\partial((fg^{-1})\cdot(uv^{-1}))=\deg_\partial(fg^{-1})+\deg_\partial(uv^{-1})$;
(c) $\deg_\partial(fg^{-1}+uv^{-1})\leq\max\{\deg_\partial(fg^{-1}),\deg_\partial(uv^{-1})\}$;
(d) $\deg_\partial((fg^{-1})^{-1})=-\deg_\partial(fg^{-1})$.

In summary, the degree function on $\mathsf{F}(\partial;\sigma,\delta)$ meets the requirement of a degree function on a skew field as in Section 3, and is once again, actually a valuation on $\mathsf{F}(\partial;\sigma,\delta)$.

4.1. Determinantal degree and unimodularity

We show unimodular matrices are precisely those with a Dieudonné determinant of degree zero.

Lemma 4.4. *Let $W\in\mathsf{F}[\partial;\sigma,\delta]^{2\times 2}$ be as in Fact 2.1. Then $\deg_\partial\mathcal{D}\mathrm{et}\,W=0$.*

Proof. We may assume that $\mathrm{gcrd}(a,b)=g=1$, since the same matrix satisfies $W(ag^{-1},bg^{-1})^T=(1,0)^T$. Also assume both $a,b\neq 0$ (otherwise the lemma is trivial). Then

$$\begin{pmatrix}u & v\\ s & t\end{pmatrix}\begin{pmatrix}a & 0\\ b & 1\end{pmatrix}=\begin{pmatrix}1 & v\\ 0 & t\end{pmatrix},\qquad\text{and}\quad\mathcal{D}\mathrm{et}(W)\cdot a\equiv t\bmod[\mathsf{F}[\partial;\sigma,\delta]^*,\mathsf{F}[\partial;\sigma,\delta]^*],$$

so $\deg_\partial\mathcal{D}\mathrm{et}\,W+\deg_\partial a=\deg_\partial t$. Since $\mathrm{gcrd}(a,b)=1$, from (4.1) we know $\deg_\partial a=\deg_\partial t$, so $\deg_\partial\mathcal{D}\mathrm{et}\,W=0$. □

Embedding the 2×2 matrices into $n\times n$ identity matrices, as in Lemma 2.2, we obtain the following (the proof of which is left to the reader).

Corollary 4.5. *Let $E\in\mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be as in Lemma 2.2. The $\deg_\partial\mathcal{D}\mathrm{et}\,E=0$.*

The characterization of unimodular matrices as those with Dieudonné determinant of degree zero follows by looking at the Hermite form of a unimodular matrix.

Theorem 4.6. *$U\in\mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ is unimodular if and only if $\deg_\partial\mathcal{D}\mathrm{et}\,U=0$.*

Proof. Suppose U is unimodular. The Hermite form of U must be the identity: all the diagonal entries must be invertible in $\mathsf{F}[\partial;\sigma,\delta]$ and the entries above the diagonal are reduced to 0. Thus, the unimodular multiplier to the Hermite form of U will be the inverse U.

Following the simple algorithm to compute the Hermite form in Theorem 2.4, we see it worked via a sequence of unimodular transforms, all of which were either permutations, off-diagonal reductions from Lemma 2.2, or are of the form E in Lemmas 2.2 and 4.5. The

Dieudonné determinants of permutations and reduction transformations are both equal to 1, by the basic properties of Dieudonné determinants discussed at the beginning of Section 3.2, and hence have degree 0. The Dieudonné determinants of the transformations E are of degree 0 by Corollary 4.5. The proof is now complete by the multiplicative property of Dieudonné determinants, and the additive properties of their degrees.

Assume conversely that $\deg_\partial \mathcal{D}\mathrm{et}\, U = 0$, and that $V \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ is a unimodular matrix such that $VU = H$ is in Hermite form. Then $\deg_\partial \mathcal{D}\mathrm{et}\, V + \deg_\partial \mathcal{D}\mathrm{et}\, U = \deg_\partial \mathcal{D}\mathrm{et}\, H = 0$. But the only matrix in Hermite form with degree 0 is the identity matrix. Thus V is the inverse of U, and U must be unimodular. □

4.2. Degree bounds on the Hermite form

In this section we establish degree bounds on Hermite forms of matrices over $\mathsf{F}[\partial;\sigma,\delta]$ and their unimodular transformation matrices.

Theorem 4.7. *Let $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ have full rank and entries of degree at most d and Hermite form $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$. Then*

(a) The sum of the degrees of the diagonal entries of H has degree at most nd;

(b) The sum of the degrees of the entries in any row of H has degree at most nd.

Proof. Let $V \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be unimodular such that $A = VH$, whence $\mathcal{D}\mathrm{et}(A) = \mathcal{D}\mathrm{et}(V)\,\mathcal{D}\mathrm{et}(H)$. Therefore (a) follows from

$$\deg_\partial \mathcal{D}\mathrm{et}(A) = \deg_\partial \mathcal{D}\mathrm{et}(H) = \sum_{1\le i\le n} \deg_\partial H_{ii} \le nd.$$

Point (b) follows from the fact that each entry above the diagonal in the Hermite form has, by definition, degree smaller than the degree of the diagonal entry below it. □

We now show that all entries in H^{-1} have non-positive degrees.

Lemma 4.8. *Let $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be of full rank and in Hermite form, and let $J = H^{-1}$. Then $\deg_\partial J_{ij} \le 0$ for $1 \le i,j \le n$.*

Proof. We consider the equation $JH = I$, and note that J, like H is upper triangular. For each $r \in \{1,\dots,n\}$ we show by induction on c (for $r \le c \le n$) that $\deg_\partial J_{rc} \le 0$.

For the base case $c = r$, $J_{rr}H_{rr} = 1$, so $\deg_\partial J_{rr} = -\deg_\partial H_{rr} \le 0$.

Assume now that $r < c$ and $\deg_\partial J_{r\ell} \le 0$ for $r \le \ell < c$. We need to show that $\deg_\partial J_{rc} \le 0$. We know that

$$\sum_{1\le i\le n} J_{r\ell}H_{\ell c} = \sum_{r\le \ell\le c} J_{r\ell}H_{\ell c} = 0.$$

Since $\deg_\partial J_{r\ell} \le 0$ for $r \le \ell < c$ and $\deg_\partial H_{cc} > \deg_\partial H_{\ell c}$ for $r \le \ell < c$, it must be the case that $\deg_\partial J_{rc} \le 0$ as well. □

Theorem 4.9. *Let $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be invertible (over $\mathsf{F}(\partial;\sigma,\delta)$), whose entries all have degree at most d in ∂. Suppose A has Hermite form $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$, with $UA = H$ and $UV = I$ for $U,V \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$. Then $\deg_\partial V \le d$ and $\deg_\partial U \le (n-1)d$.*

$U = HA^{-1}$

$V = U^{-1} = A \cdot H$

Proof. Note that $V = AH^{-1}$, and by Lemma 4.8 all entries in H^{-1} have non-positive degree. Thus $\deg_\partial V \leq \deg_\partial A$. By Corollary 3.3, $\deg_\partial U \leq (n-1)d$. □

5. Computing Hermite forms by linear systems over $\mathsf{F}[\partial;\sigma,\delta]$

In this section we present our polynomial-time algorithm to compute the Hermite form of a matrix over $\mathsf{F}[\partial;\sigma,\delta]$. This generally follows the "linear systems" approach of Kaltofen et al. (1987), and more specifically the refinements in Storjohann (1994) (for matrices over $\mathsf{k}[x]$ for a field k). We will need the tools for $\mathsf{F}[\partial;\sigma,\delta]$ we have developed in the previous sections. The method only directly constructs the matrix U such that $H = UA$. The Hermite form H can be found by performing the multiplication UA.

The general approach is similar to that described in Giesbrecht and Kim (2009), with a primary difference that in that paper the technique of Kaltofen et al. (1987) was adapted. This new technique is considerably more efficient (see below). As well, our earlier paper was constrained to differential rings as the necessary degree bounds were not available for all Ore polynomials.

Assume that $A_{ij} = \sum_{0\leq k\leq d} A_{ijk}\partial^k$ for $A_{ijk} \in \mathsf{F}$. Let $\operatorname{row}(A,i) \in \mathsf{F}[\partial;\sigma,\delta]^{1\times n}$ be the ith row of A and define

$$\mathcal{L}(A) = \left\{ \sum_{1\leq i\leq n} b_i \cdot \operatorname{row}(A,i) : b_1,\ldots,b_n \in \mathsf{F}[\partial;\sigma,\delta] \right\},$$

the left module of the row space of A. The following lemma is shown analogously to (Storjohann, 1994, §4.3.1, Lemma 4).

Lemma 5.1. *Let $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be nonsingular, with Hermite form H. Let $h_i = \deg_\partial H_{ii}$ for $1 \leq i \leq n$. For $v = (0,\ldots,0,v_\ell,\ldots,v_n) \in \mathsf{F}[\partial;\sigma,\delta]^{1\times n}$, with $\deg_\partial v_\ell < h_\ell$, then if $v \in \mathcal{L}(A)$ we have $v_\ell = 0$, and if $v_\ell \neq 0$ then $v \notin \mathcal{L}(A)$.*

The following theorem is analogous to (Storjohann, 1994, §4.3.1, Lemma 5), with a different, slightly weaker degree bound.

Theorem 5.2. *Let $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ have full rank, with $\deg_\partial A_{ij} \leq d$ for $1 \leq i,j \leq n$. Let $(d_1,\ldots,d_n)$ be a given vector of non-negative integers. Let T be an $n\times n$ matrix with $T_{ij} = \sum_{0\leq k\leq \varrho} t_{ijk}\partial^k$ for unknowns t_{ijk}, where $\varrho \geq (n-1)d + \max_i\{d_i - h_i\}$. Consider the system of equations in t_{ijk} with constraints:*

$$\begin{aligned}
(TA)_{i,i,d_i} &= 1, \text{ for } 1\leq i\leq n, && \text{— diagonal entries are monic;}\\
(TA)_{i,i,k} &= 0, \text{ for } k > d_i, && \text{— diagonal entry in row } i \text{ has degree } d_i;\\
(TA)_{i,j,k} &= 0, \text{ for } i\neq j \text{ and } k \geq d_j && \text{— off diagonal entries have lower degree than the diagonal entry in that column.}
\end{aligned} \tag{5.1}$$

By a solution for T *we mean an assignment of variables $t_{ijk} \leftarrow \alpha_{ijk} \in \mathsf{F}$ for some $1 \leq i,j \leq n$ and $0 \leq k \leq \varrho$ such* (5.1) *holds.*

Let $h_1,\ldots,h_n \in \mathbb{N}$ be the degrees of the diagonal entries of the Hermite form of A. The following statements about the above system hold:

(i) If $d_i \geq h_i$ for $1 \leq i \leq n$ then there exists a solution for T;

(ii) If there exists a positive integer $\ell \leq n$ such that $d_i = h_i$ for $1 \leq i < \ell$ and $d_\ell < h_\ell$ then there is no solution for T;

(iii) If $d_i = h_i$ for $1 \leq i \leq n$ then there is a unique solution for T such that $G = TA$ is equal to the Hermite form of A under that solution.

Proof. Let $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be the Hermite form of A and let $U \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be the unique unimodular matrix such that $UA = H$.

To show (i), let $D = \operatorname{diag}(\partial^{d_1-h_1}, \ldots, \partial^{d_n-h_n}) \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$, and consider the equality $DUA = DH$. Let $H^* \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ be the Hermite form of DH and $U^* \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ the unimodular matrix such that $U^*DUA = H^*$. We construct H^* from DH simply by reducing the entries above the diagonal (since it is already upper triangular). Thus U^* is upper triangular, with ones on the diagonal, and $\deg_\partial U^*_{ij} < (d_i - h_i) - (d_j - h_j)$ for $i < j$. We claim $T = U^*DU$ is a solution to (5.1) . First note that the particular choice of D, together with the definition of H^* ensure that the constraints of (5.1) are met. Furthermore, entries in the ith row of U^*D have degree at most $d_i - h_i$. By Theorem 4.9, $\deg_\partial U \leq (n-1)d$, hence $\deg_\partial T \leq (n-1)d + \max_i\{d_i - h_i\} \leq \varrho$.

To prove (ii), suppose by contradiction that there exists a nonnegative integer $\ell \leq n$ and a solution T such that $\deg_\partial((TA)_{ii}) = d_i$ for $1 \leq i < \ell$ and $\deg_\partial((TA)_{\ell\ell}) < h_\ell$. Note that $\operatorname{row}(TA,\ell) = ((TA)_{\ell,1}, \ldots, (TA)_{\ell,n})$ is in $\mathcal{L}(A)$. First, if $\ell = 1$, then $\deg_\partial(TA)_{\ell,1} < h_1$, so by Lemma 5.1, $(TA)_{1,1} = 0$, which is impossible since (5.1) ensures this entry is monic. Now assume $\ell > 1$. Then $\deg_\partial(TA)_{\ell,1} < h_1$ (to satisfy (5.1)), and hence by Lemma 5.1, so $(TA)_{\ell,1} = 0$. A simple induction shows that $(TA)_{\ell,j} = 0$ for $1 \leq j < \ell$. Now consider $(TA)_{\ell,\ell}$, which has degree $d_\ell < h_\ell$ by our assumption. Again by Lemma 5.1 $(TA)_{\ell,\ell} = 0$, which (5.1) ensures is monic, a contradiction.

If the conditions of (iii) hold, then by (i) there exists at least one solution for T. We can use an inductive proof similar to that used in our proof of (ii) to show that elements below the diagonal in TA are zero (i.e., that $(TA)_{ij} = 0$ for $i > j$). By the uniqueness of the Hermite form we must have $TA = H$. □

This theorem allows us to work with a partial order on the degree sequences. For any $(h_1,\ldots,h_n),(d_1,\ldots,d_n) \in \mathbb{Z}^n$, we say that $(h_1,\ldots,h_n) \preceq (d_1,\ldots,d_n)$ if and only if $h_i \leq d_i$ for all $1 \leq i \leq n$ (and similarly define $\precneqq$ for strict precedence). Thus, (5.1) has a solution if and only if $(h_1,\ldots,h_n) \preceq (d_1,\ldots,d_n)$ and this is unique if and only if $(h_1,\ldots,h_n) = (d_1,\ldots,d_n)$.

We now embed the system (5.1) into a system of linear equations over F, with no Ore component. We embed $\mathsf{F}[\partial;\sigma,\delta]$ into vectors over F via τ_ℓ: $\mathsf{F}[\partial;\sigma,\delta] \to \mathsf{F}^{\ell+1}$, with

$$\tau_\ell(u_0 + u_1\partial + u_2\partial^2 + \cdots + u_\ell\partial^{\ell-1}) = (u_0,\ldots,u_\ell) \in \mathsf{F}^{\ell+1}.$$

For $g \in \mathsf{F}[\partial;\sigma,\delta]$ of degree d, $u \in \mathsf{F}[\partial;\sigma,\delta]$ of degree at most m, and assuming $\ell \geq m+d$, the equation $ug = f$ can be realized by a matrix equation over F:

$$(u_0,\ldots,u_m)\underbrace{\begin{pmatrix} \tau_\ell(g) \\ \hline \tau_\ell(\partial g) \\ \hline \vdots \\ \hline \tau_\ell(\partial^m g) \end{pmatrix}}_{\mu^\ell_m(g) \in \mathsf{F}^{(m+1)\times(\ell+1)}} = (f_0,\ldots,f_\ell) \quad\Longleftrightarrow\quad \tau_m(u)\,\mu^\ell_m(g) = \tau_\ell(f).$$

≃ Sylvester matrix

Fixing $d_1, \ldots, d_n \in \mathbb{N}$ as in Theorem 5.2, and setting $\varrho \geq (n-1)d + \max_i\{d_i - h_i\}$, we can then study (5.1), as realized as (a subset of) the linear equations in the matrix equation over F:

$$\underbrace{\begin{pmatrix} \tau_\varrho(T_{11}) & \cdots & \tau_\varrho(T_{1n}) \\ \vdots & & \vdots \\ \tau_\varrho(T_{n1}) & \cdots & \tau_\varrho(T_{nn}) \end{pmatrix}}_{\widehat{T} \in \mathsf{F}^{n \times (\varrho+1)n}} \underbrace{\begin{pmatrix} \mu_\varrho^{\varrho+d}(A_{11}) & \cdots & \mu_\varrho^{\varrho+d}(A_{1n}) \\ \vdots & & \vdots \\ \mu_\varrho^{\varrho+d}(A_{n1}) & \cdots & \mu_\varrho^{\varrho+d}(A_{nn}) \end{pmatrix}}_{\widehat{A} \in \mathsf{F}^{n(\varrho+1) \times (\varrho+d+1)n}} = \underbrace{\begin{pmatrix} \tau_{\varrho+d}(G_{11}) & \cdots & \tau_{\varrho+d}(G_{1n}) \\ \vdots & & \vdots \\ \tau_{\varrho+d}(G_{n1}) & \cdots & \tau_{\varrho+d}(G_{nn}) \end{pmatrix}}_{\widehat{G} \in \mathsf{F}^{n \times (\varrho+d+1)n}}. \tag{5.2}$$

This set of equations is a superset of the equation (5.1). Some entries in $\widehat{G}$ are unknown, in particular those corresponding to coefficients of degrees (in ∂) strictly less than the degree of the diagonal below it. However, these entries in $\widehat{G}$ are not mentioned or involved in Theorem 5.2, and we can remove these columns from $\widehat{G}$. Similarly, since they impose no constraint on (5.1), we can remove the corresponding columns of $\widehat{A}$. By Theorem 5.2, if we know $d_1, \ldots, d_n$, the remaining equations will have a unique solution, from which we completely determine $\widehat{T}$.

Example 5.3. Consider the following matrix in $\mathbb{Q}(z)[\partial; \prime]$ (the differential polynomials over $\mathbb{Q}(z)$):

$$A = \begin{pmatrix} (z+1) + \partial & z + z\partial & \partial \\ (z^2+z) + z\partial & z+1 & 2\partial \\ (-z-z^2) - z\partial & z\partial & z\partial \end{pmatrix} \in \mathbb{Q}(z)[\partial; \prime]^{3\times 3}.$$

Assume for this example that we know the degrees of the entries in the Hermite form are $(d_1, d_2, d_3) = (1, 0, 2)$. Then $n = 3$, and we can set $\varrho = 2$, and have

$$\widehat{T} = \left(\begin{array}{ccc|ccc|ccc} t_{110} & t_{111} & t_{112} & t_{120} & t_{121} & t_{122} & t_{130} & t_{131} & t_{132} \\ \hline t_{210} & t_{211} & t_{212} & t_{220} & t_{221} & t_{222} & t_{230} & t_{231} & t_{232} \\ \hline t_{210} & t_{211} & t_{212} & t_{220} & t_{221} & t_{222} & t_{230} & t_{231} & t_{232} \end{array}\right)$$

$$\widehat{A} = \left(\begin{array}{cccc|cccc|cccc} z+1 & 1 & 0 & 0 & z & z & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & z+1 & 1 & 0 & 1 & z+1 & z & 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & z+1 & 1 & 0 & 2 & z+2 & z & 0 & 0 & 0 & 1 \\ \hline z^2+z & z & 0 & 0 & z+1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 2z+1 & z^2+z+1 & z & 0 & 1 & z+1 & 0 & 0 & 0 & 0 & 2 & 0 \\ 2 & 4z+2 & z^2+z+2 & z & 0 & 2 & z+1 & 0 & 0 & 0 & 0 & 2 \\ \hline -z^2-z & -z & 0 & 0 & 0 & z & 0 & 0 & 0 & z & 0 & 0 \\ -2z-1 & -z^2-z-1 & -z & 0 & 0 & 1 & z & 0 & 0 & 1 & z & 0 \\ -2 & -4z-2 & -z^2-z-2 & -z & 0 & 0 & 2 & z & 0 & 0 & 2 & z \end{array}\right)$$

$$= \widehat{G} = \left(\begin{array}{cccc|cccc|cc} G_{110} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & G_{130} & G_{131} & 0 & 0 \\ G_{210} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & G_{230} & G_{231} & 0 & 0 \\ G_{310} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & G_{330} & G_{331} & 1 & 0 \end{array}\right).$$

As noted above, $\widehat{G}$ still has some indeterminates, from columns which specify coefficients of the entries of G which are of degree strictly less than the maximum in the corresponding column of G. These entries are not mentioned in (5.1), and we remove them to form $\widetilde{G}$. The corresponding columns of A are similarly not involved in (5.1), and are removed to form $\widetilde{A}$. We obtain now obtain a reduced system of equations which corresponds precisely to (5.1):

$$\overbrace{\left(\begin{array}{ccc|ccc|ccc} t_{110} & t_{111} & t_{112} & t_{120} & t_{121} & t_{122} & t_{130} & t_{131} & t_{132} \\ \hline t_{210} & t_{211} & t_{212} & t_{220} & t_{221} & t_{222} & t_{230} & t_{231} & t_{232} \\ \hline t_{210} & t_{211} & t_{212} & t_{220} & t_{221} & t_{222} & t_{230} & t_{231} & t_{232} \end{array}\right)}^{\widehat{T}}$$

$$\overbrace{\left(\begin{array}{ccc|cccc|cc} 1 & 0 & 0 & z & z & 0 & 0 & 0 & 0 \\ z+1 & 1 & 0 & 1 & z+1 & z & 0 & 1 & 0 \\ 2 & z+1 & 1 & 0 & 2 & z+2 & z & 0 & 1 \\ \hline z & 0 & 0 & z+1 & 0 & 0 & 0 & 0 & 0 \\ z^2+z+1 & z & 0 & 1 & z+1 & 0 & 0 & 2 & 0 \\ 4z+2 & z^2+z+2 & z & 0 & 2 & z+1 & 0 & 0 & 2 \\ \hline -z & 0 & 0 & 0 & z & 0 & 0 & 0 & 0 \\ -z^2-z-1 & -z & 0 & 0 & 1 & z & 0 & z & 0 \\ -4z-2 & -z^2-z-2 & -z & 0 & 0 & 2 & z & 2 & z \end{array}\right)}^{\widetilde{A}\ :\ 9\times 9}$$

$$= \overbrace{\left(\begin{array}{ccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right)}^{\widetilde{G}} \in \mathsf{F}^{n(\varrho+1)\times n(\varrho+1)}.$$

By Theorem 5.2, since we have "guessed" the degree sequence of the diagonal entries $(d_1, d_2, d_3) = (1, 0, 2)$ correctly, the system has a unique solution:

$$\widehat{T} = \left(\begin{array}{ccc|ccc|ccc} \frac{z+1}{2\,z+1} & 0 & 0 & -\frac{z}{2\,z+1} & 0 & 0 & -\frac{z+1}{2\,z+1} & 0 & 0 \\ -\frac{z}{2\,z+1} & 0 & 0 & \frac{z+1}{2\,z+1} & 0 & 0 & \frac{z}{2\,z+1} & 0 & 0 \\ -\frac{2\,z^2+3\,z+2}{(z^2+z+2)(2\,z+1)} & -\frac{z}{z^2+z+2} & 0 & \frac{2\,z^2+z-1}{(z^2+z+2)(2\,z+1)} & \frac{z+1}{z^2+z+2} & 0 & \frac{2\,z^3-z^2-2\,z-1}{z(z^2+z+2)(2\,z+1)} & \frac{z}{z^2+z+2} & 0 \end{array}\right)$$

which corresponds to

$$T = \left(\begin{array}{ccc} \frac{z+1}{2\,z+1} & -\frac{z}{2\,z+1} & -\frac{z+1}{2\,z+1} \\ -\frac{z}{2\,z+1} & \frac{z+1}{2\,z+1} & \frac{z}{2\,z+1} \\ -\frac{2\,z^2+3\,z+2}{(z^2+z+2)(2\,z+1)} - \frac{z}{z^2+z+2}\partial & \frac{2\,z^2+z-1}{(z^2+z+2)(2\,z+1)} + \frac{z+1}{z^2+z+2}\partial & \frac{2\,z^3-z^2-2\,z-1}{z(z^2+z+2)(2\,z+1)}) + \frac{z}{z^2+z+2}\partial \end{array}\right) \in \mathbb{Q}(z)[\partial;\prime]^{3\times 3}$$

giving

$$H = TA = \left(\begin{array}{ccc} (z+1)+\partial & 0 & -\frac{z^2+2z-1}{2z+1}\partial \\ 0 & 1 & \frac{z^2+z+2}{2z+1}\partial \\ 0 & 0 & \frac{2z^3+3z^2-2z-5}{(z^2+z+2)(2z+1)}\partial + \partial^2 \end{array}\right) \in \mathbb{Q}(z)[\partial;\prime]^{3\times 3}$$

in Hermite form.

We can now state our algorithm for computing the Hermite form given the degrees of the diagonal elements.

Algorithm `HermiteFormGivenDegrees`

Input: $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ of full rank, with (unknown) Hermite form H with diagonal degrees $(h_1,\ldots,h_n) \in \mathbb{N}^n$;
Input: $(d_1,\ldots,d_n) \in \mathbb{N}^n$, the proposed degrees of the diagonal entries of H
Output: $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ if $(d_1,\ldots,d_n) = (h_1,\ldots,h_n)$, or a message that $(d_1,\ldots,d_n)$ is lexicographically smaller or larger than $(h_1,\ldots,h_n)$;

1: Let $\varrho = (n-1)d + \max_i d_i$
2: Form the matrix equation $\widehat{T}\widehat{A} = \widehat{G}$ as in (5.2)
3: Remove all columns from $\widehat{G}$ containing an indeterminate, and corresponding columns from $\widehat{A}$, to form the "reduced" linear system $\widetilde{T}\widetilde{A} = \widetilde{G}$, where $\widetilde{A}$ and $\widetilde{G}$ are now matrices over F
4: **if** $\operatorname{rank}\widetilde{A} < (n+1)\varrho$ **then**
5: **return** "$(h_1,\ldots,h_n) \trianglerighteq (d_1,\ldots,d_n)$" // System is underconstrained
6: **if** $\widehat{T}\widetilde{A} = \widetilde{G}$ has no solution **then**
7: **return** "$(h_1,\ldots,h_n) \not\trianglerighteq (d_1,\ldots,d_n)$" // System is inconsistent
8: Solve the system $\widehat{T}\widetilde{A} = \widetilde{G}$ for $\widehat{T}$
9: Construct $T \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ from $\widehat{T}$
10: **return** $H = TA$ and $U = T$

From Theorem 4.7 we know that each entry in the Hermite form of $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$, with $\deg_\partial A_{ij} \le d$ for $1 \le i,j \le n$, has degree at most nd. If the diagonal entries of A have degrees $(h_1,\ldots,h_n)$, then we know that

$$(0,\ldots,0) \trianglelefteq (h_1,\ldots,h_n) \trianglelefteq (nd,nd,\ldots,nd).$$

Algorithm `HermiteFormGivenDegrees` detects whether our choice of degree sequence is equal to, larger than, or not larger than or equal to the actual one. Thus, a simple component-wise binary search allows us to find the actual degree sequence $(h_1,\ldots,h_n)$. That is, start by finding for the h_1 by executing `HermiteFormGivenDegrees` with degree sequence $(d_1,nd,\ldots,nd)$ for different values of d_1. This will require $O(\log(nd))$ attempts. Then search for h_2 using degree sequence $O(h_1,d_2,nd,\ldots,nd)$ for different values of d_2, etc. It will require at most $O(n\log(nd))$ attempts to find the entire correct degree sequence $(h_1,\ldots,h_n)$.

Lemma 5.4. *Given $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ of full rank, where each entry has degree (in ∂) less than d, we can compute the Hermite form $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ of A, and $U \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$. The algorithm requires us to call Algorithm* `HermiteFormGivenDegrees` *$O(n\log(nd))$ times, with input A and varying degree sequences.*

For a first, general analysis of the complexity we will assume that operations in F have unit cost (and hence no coefficient growth is accounted for). To perform the rank test in Step 4, the inconsistency test in Step 6, and the equation solution in Step 8, we can simply do an LU decomposition of $\widetilde{A}$ using Gaussian elimination. $\widetilde{A}$ has size $n(\varrho+1)\times m$,

where $n(\varrho+1) \le m \le n(\varrho+d+1)$, i.e., $O(n^2d) \times O(n^2d)$. Gaussian elimination, which computes an LU-decomposition or more generally a Bruhat normal form (see Section 3.2 or (Draxl, 1983, Chapter 19)) is effective over any skew field, and on a $p \times q$ matrix requires $O(p^2q)$ operations, and hence in our case can be accomplished with $O(n^6d^3)$ operations in F. Combining this with Lemma 5.4 we obtain the following.

Theorem 5.5. *Let $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ have full rank with entries of degree (in ∂) less than d. We can compute the Hermite form $H \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ of A, and $U \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$. The algorithm requires $O(n^7d^3\log(nd))$ operations in F.*

We next analyze our algorithm for computing the Hermite form of a matrix $A \in \mathsf{k}(z)[\partial;\sigma,\delta]^{n\times n}$ over the field $\mathsf{F} = \mathsf{k}(z)$, where k is a field and z an indeterminate. Without loss of generality $A \in \mathsf{k}[z][\partial;\sigma,\delta]^{n\times n}$ by clearing denominators (which is a left-unimodular operation), but note that the Hermite form may still be in $\mathsf{k}(z)[\partial;\sigma,\delta]$ (see Example 5.3). We will also assume for convenience that $\sigma(z) \in \mathsf{k}[z]$ and $\deg_z \delta(z) \le 1$. Thus $\partial z = \sigma(z)\partial + \delta(z) \in \mathsf{k}[z][\partial]$ and the degree in z and ∂ remains unchanged. A more general analysis could follow similarly.

We assume that multiplying two polynomials in $\mathsf{k}[z]$ of degree at most m can be accomplished with $O(\mathsf{M}(m))$ operations in k: $\mathsf{M}(m) = m^2$ using standard arithmetic or $\mathsf{M}(m) = m\log m\log\log m$ using fast arithmetic (Cantor and Kaltofen, 1991). We similarly assume that two integers with ℓ bits can be multiplied with $O(\mathsf{M}(l))$ bit operations. Finally, when we talk of the *degree* of a rational function in $\mathsf{k}(z)$ we mean the maximum degree of the numerator and denominator, assuming they are co-prime. This gives a reasonable indication of representation size.

Theorem 5.6. *Let $A \in \mathsf{k}[z][\partial;\sigma,\delta]^{n\times n}$ have full rank with entries of degree at most d in ∂, and of degree at most e in z. Let $H \in \mathsf{k}(z)[\partial;\sigma,\delta]^{n\times n}$ be the Hermite form of A and $U \in \mathsf{k}(z)[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$.*

(a) $\deg_z H_{ij} \in O(n^2de)$ and $\deg_z U_{ij} \in O(n^2de)$ for $1 \le i,j \le n$.

(b) We can compute H and U deterministically with $O(n^7d^3\log(nd)\cdot\mathsf{M}(n^2de))$ or $O^{\sim}(n^9d^4e)$ operations in k.

(c) Assume k has at least $4n^2de$ elements. We can compute the Hermite form H and U with an expected number of $O(n^7d^3\log(nd) + n^7d^3e)$ of operations in k using standard polynomial arithmetic. This algorithm is probabilistic of the Las Vegas type; it never returns an incorrect answer.

Proof. To show (a), recall that the matrix $\widetilde{A}$ is of size $O(n^2d) \times O(n^2d)$ and degree $O(e)$. Using Hadamard's bound and Cramer's rule, the numerators and denominators in $\widehat{T}$ thus have degree at most $O(n^2de)$ in z. $H = UA$ has the same degree bound in z.

To prove (b) we solve the system of equations (5.1) as in Theorem 5.5 but now taking into account coefficient growth. Since we have an explicit bound on the degree in z of numerators and denominators of the solution, we can compute modulo an irreducible polynomial $\Gamma \in \mathsf{k}[z]$ more than twice this degree and recover the solution over $\mathsf{k}(z)$ by rational recovery. Each operation in $\mathsf{k}(z) \in \mathsf{k}[z]/(\Gamma)$ will thus take $O^{\sim}(\mathsf{M}(n^2de))$ operations in k. The stated total cost follows from the cost in Theorem 5.5 multiplied by this operation cost.

To show (c), we note that the tests for rank deficiency in Step 4, and inconsistency in Step 6, can be done by considering the equation $\widehat{T}\widetilde{A} = \widetilde{G} \bmod (z-\alpha)$ for a randomly

chosen α from a subset of k of size at least $4n^2de$. This follows because the largest invariant factor $w \in \mathsf{k}[z]$ of $\widetilde{A}$ has degree at most n^2de by Hadamard's bound (see part (a)), and the rank modulo $(z-\alpha)$ changes only if α is a root of w. By the Schwartz-Zippel Lemma (Schwartz, 1980) this happens with probability at most $1/4$ for each choice of α (and this probability of error can be made exponentially smaller by repeating with different random choices). Thus, these tests require only $O(n^6d^3)$ operations in k to perform, correctly with high probability. During the binary search for the degree sequence we only perform these cheaper tests, requiring a total of $O(n^7d^3\log(nd))$ operations in k before finding the correct degree sequence.

Once we have found the correct degree sequence, we employ Dixon's (1982) algorithm to solve the linear system over $\mathsf{k}(z)$ (this is the fastest known algorithm using standard matrix arithmetic, and is very effective in practice; one could also employ the asymptotically faster method of Storjohann (2003) with sub-cubic matrix arithmetic). This lifts the solution to the system modulo $(z-\alpha)^i$ for $i = 1, \ldots, 2n^2de$, where α is a non-root of the (unknown) largest invariant factor of A (i.e., is such that $\operatorname{rank} A = \operatorname{rank} A \bmod (z-\alpha)$). Computing the solution modulo $(z-\alpha)^{2n^2de}$ is sufficient to recover the solution in $\mathsf{k}(z)$ using rational function reconstruction, since both the numerator and denominator have degree less than n^2de by part (a); see (von zur Gathen and Gerhard, 2003), Section 5.7. A random choice of α from a subset of k of size $4n^2de$ is sufficient to obtain a non-zero of the largest invariant factor (and hence not change the dimension of the solution space) with probability at least $1/4$ by the Schwartz-Zippel Lemma. In the first step of Dixon's algorithm, we compute the LU-decomposition of A mod $(z-\alpha)$ using $O(n^6d^3)$ operations in k. We then lift the solution to $\widehat{T}\widetilde{A} \equiv \widetilde{G} \bmod (z-\alpha)^i$ for $i = 0, \ldots, 2n^2de$. Each lifting step requires $O(n^5d^2)$ operations in k, yielding a total cost of $O(n^7d^3e)$. $\square$

For comparison, the cost of the algorithm in (Giesbrecht and Kim, 2009), for the case of matrices over $\mathsf{k}(z)[\partial;']$, required $O^{\sim}(n^{10}d^4e)$ operations in k.

Finally, we consider coefficient growth in $\mathbb{Q}$ of Ore polynomial rings over $\mathbb{Q}(z)$. For the computation, once we have constructed the matrix $\widetilde{A}$, we can bound the coefficient-sizes in $\widehat{T}$ directly using Hadamard-type bounds. We can then employ a Chinese remainder scheme to find the Hermite form using the above algorithm (or any other method, for that matter). For example, we could simply choose a single prime p with twice as many bits as the largest numerator or denominator in the solution to (5.2) and then compute modulo that prime, in $\mathbb{Z}_p[z]$; the rational coefficients of H can be recovered by integer rational reconstruction from their images in $\mathbb{Z}_p$ (von zur Gathen and Gerhard, 2003, §5.7).

However, for the purposes of analysis, it is interesting to see how big these coefficients can grow. We consider matrices in $A \in \mathbb{Z}[z][\partial;\sigma,\delta]^{n\times n}$ without loss of generality. For convenience in this analysis (though not in complete generality), we assume that $\deg_z \delta(z) \leq 1$ and $\sigma(z) \in \mathbb{Z}[z]$, so $\partial z = \sigma(z)\partial + \delta(z) \in \mathbb{Z}[z]$.

For a polynomial $a = a_0 + a_1 z + \cdots + a_m z^m \in \mathbb{Z}[z]$, let $\|a\|_\infty = \max_i |a_i|$. For $f = f_0(z) + f_1(z)\partial + \cdots + f_r(z)\partial^r \in \mathbb{Z}[z][\partial;\sigma,\delta]$, let $\|f\|_\infty = \max_i \|f_i\|_\infty$. Define $\|A\|_\infty = \max_{ij} \|A_{ij}\|_\infty$. In equation (5.2), the entries in $\widetilde{A}$ have size at most

$$\|A\|_\infty^{(\varrho)} = \max_{ij} \max_{\ell} \{\|A_{ij}\|_\infty, \|\partial A_{ij}\|_\infty, \ldots, \|\partial^\varrho A_{ij}\|_\infty\} \in \mathbb{Z}. \tag{5.3}$$

Theorem 5.7. *Let $A \in \mathbb{Z}[z][\partial;\sigma,\delta]^{n\times n}$ be of full rank and such that $\deg_\partial(A) = d$, $\deg_z(A) \le e$ and $\|A\|_\infty^{(\partial)} \le \beta$. Then the Hermite form $H \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ and $U \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$ satisfy*

$$\log \|H\|_\infty,\ \log \|U\|_\infty \in O(n^2 d\,(\log e + \log\beta + \log n + \log d)).$$

Proof. Entries in $\widetilde{A}$ are polynomials in $\mathbb{Z}[z]$ of degree at most e and coefficient size at most β. Every minor of $\widetilde{A}$, and hence each entry in the solution $\widehat{T}$, is bounded by Hadamard's bound, which in this case is

$$\big((1+e)\beta(n^2 d)\big)^{O(n^2 d)}$$

(see Giesbrecht (1993) Theorem 1.5 for height bounds on polynomial products). □

By performing all computations modulo an appropriately large prime (as discussed above), we immediately get the following.

Corollary 5.8. *Let $A \in \mathbb{Z}[z][\partial;\sigma,\delta]^{n\times n}$ have full rank with entries of degree at most d in ∂, of degree at most e in z, and $\|A\|_\infty^{(\varrho)} \le \beta$ (where $\varrho = O(n^2 d)$). Let $H \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ be the Hermite form of A and $U \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$.*

We can compute the Hermite form $H \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ of A, and $U \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$, using an algorithm that requires an expected number $O((n^7 d^3 \log(nd) + n^7 d^3 e)\cdot \mathsf{M}(n^2 d(\log e + \log\beta + \log n + \log d)))$, or $O^{\sim}(n^9 d^4 e \log\beta)$ bit operations. This algorithm is probabilistic of the Las Vegas type (never returning an incorrect answer).

The following corollary summarizes this growth explicitly over two common rings, the differential polynomials $\mathbb{Q}(z)[\partial;']$, and the shift polynomials $\mathbb{Q}(z)[\partial;\mathcal{S}]$.

Corollary 5.9. *Let $A \in \mathbb{Z}[z][\partial;\sigma,\delta]^{n\times n}$ be of full rank and such that $\deg_\partial(A) = d$, $\deg_z(A) \le e$, $H \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ the Hermite form of A, and $U \in \mathbb{Q}(z)[\partial;\sigma,\delta]^{n\times n}$ such that $UA = H$. For both the differential polynomials $\mathbb{Q}(z)[\partial;']$ (where $\sigma(z) = z$, $\delta(z) = 1$) and the shift polynomials $\mathbb{Q}(t)[\partial;\mathcal{S}]$ (where $\sigma(z) = z+1$, $\delta(z) = 0$), we have*

$$\log \|U\|_\infty,\ \log \|H\|_\infty \in \widetilde{O}(n^2 d\,(e + \log \|A\|_\infty)).$$

bound on the coefficients of the Hermite form

Proof. To show this for differential polynomials, we note that for $a = \sum_{0\le i\le d} a_i(z)\partial^i \in \mathbb{Z}[z][\partial;']$,

$$\partial^\ell a = \sum_{0\le j\le \ell} \binom{\ell}{j} \sum_{0\le i\le d} a_i(z)^{(j)} \partial^{\ell-j},$$

where $a_i(z)^{(j)}$ is the jth derivative of $a_i(z)$. Since only the first e derivatives of any a_i are non-zero

$$\|\partial^\ell a\|_\infty \le \ell^e \cdot \|a\|_\infty \cdot e!$$

and hence $\log \|A\|_\infty^{(\varrho)} \in O(\log\|A\|_\infty + e\log(n^2 d))$ for $\varrho = O(n^2 d)$. The result follows by Theorem 5.7.

To show this for shift polynomials we note that for $a = \sum_{0\le i\le d} a_i(z)\partial^i \in \mathbb{Z}[\partial,\mathcal{S}]$,

$$\partial^\ell a = \sum_{0\le i\le d} a_i(z+\ell)\partial^i,$$

so

$$\|\partial^\ell a\|_\infty \leq \|a\|_\infty 2^{e/2}\ell^e,$$

and hence $\log \|A\|_\infty^{(\varrho)} \in O(\log \|A\|_\infty + e\log(n^2 d))$ for $\varrho = n^2 d$. Again, the result follows from Theorem 5.7. □

6. Rectangular and rank deficient matrices

To this point we have assume that our matrices $A \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ were both square and of full rank. In this section we relax both these conditions to show a polynomial-time algorithm for the Hermite form in all cases.

6.1. Matrices with non-full rank

Suppose now that $A \in \mathsf{F}[\partial;\sigma,\delta]^{m\times n}$ has rank $r \leq m$. We first show how to compute a unimodular matrix $P \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$ such that PA has precisely r non-zero rows. Since P is unimodular, the left $\mathsf{F}[\partial;\sigma,\delta]$-modules generated by the rows of A and the rows of PA are equal.

We employ the row reduction algorithm developed by Beckermann et al. (2006), and discussed in (Davies et al., 2008). Let $b = m \cdot \deg_\partial A$ and $Q = \operatorname{diag}(\partial^b, \ldots, \partial^b) \in \mathsf{F}[\partial;\sigma,\delta]^{n\times n}$, and form the matrix

$$B = \begin{pmatrix} AQ \\ -I_n \end{pmatrix} \in \mathsf{F}[\partial;\sigma,\delta]^{(m+n)\times n}.$$

We compute a basis for the left nullspace basis of B in Popov form using the algorithm in Beckermann et al. (2006), and suppose it has form

$$\begin{pmatrix} P \mid R \end{pmatrix} \in \mathsf{F}[\partial;\sigma,\delta]^{m\times(m+n)} \quad \text{for} \quad P \in \mathsf{F}[\partial;\sigma,\delta]^{m\times m}.$$

Then by (Davies et al., 2008, Theorem 4.5, 5.5), $P \in \mathsf{F}[\partial;\sigma,\delta]^{m\times m}$ is unimodular and PA is in Popov form. In particular, only r rows are non-zero.

Theorem 6.1. *Let $A \in \mathsf{k}[z][\partial;\sigma,\delta]^{n\times n}$ have rank $r \leq m$, with $\deg_\partial A \leq d$ and $\deg_z A \leq e$. We can find a unimodular matrix $P \in \mathsf{k}[z][\partial;\sigma,\delta]^{m\times m}$ such that PA has r non-zero rows using $O(m^9 n^9 (\deg_\partial A)^4 (\deg_z A)^4)$ operations in k. It also requires a polynomial number of bit operations when $\mathsf{k} = \mathbb{Q}$.*

Proof. The matrix B has $\deg_\partial(B) \leq (m+1)\cdot\deg_\partial A$ and $\deg_z(B) \leq \deg_z(A)$. The algorithm of Beckermann et al. (2006) to compute the Popov form, as summarized in their Corollary 7.7, requires $O(m^9 n^9 (\deg_\partial A)^4 (\deg_z A)^4)$ operations in k. It also requires a polynomial number of bit operations when $\mathsf{k} = \mathbb{Q}$. □

After eliminating the zero rows, we are left to compute the Hermite form of a (possibly rectangular) matrix with full rank.

6.2. Rectangular matrices of full rank

Let $A \in \mathsf{F}[\partial;\sigma,\delta]^{m\times n}$ have full rank with $n > m$. Then there exists a lexicographically first set of columns $\tau_1,\ldots,\tau_m$ such that the submatrix

$$A_\tau = \begin{pmatrix} A_{1,\tau_1} & A_{1,\tau_2} & \cdots & A_{1,\tau_m} \\ \vdots & & & \vdots \\ A_{m,\tau_1} & A_{m,\tau_2} & \cdots & A_{m,\tau_m} \end{pmatrix} \in \mathsf{F}[\partial;\sigma,\delta]^{m\times m}$$

has full rank. We can compute the unique U such that UA_τ is in Hermite form using the algorithm of the previous section. Then it must be the case that UA has form

$$UA = \begin{pmatrix} H_{1,\tau_1} & * & \cdots & \cdots & \cdots & * \\ & H_{2,\tau_2} & * & \cdots & & * \\ & & & \ddots & & \\ & & & & & H_{m,\tau_m} \end{pmatrix} \in \mathsf{F}[\partial;\sigma,\delta]^{m\times n},$$

the Hermite form of A. This suggests an easy strategy of simply conducting a binary search for the lexicographically smallest subset $\{\tau_1,\ldots,\tau_m\}$ of $\{1,\ldots,n\}$ such that the U computed to put A_τ in Hermite form also puts UA in Hermite form. Since there are $\binom{n}{m} \le 2^n$ subsets of size m, our binary search will require at most $\log_2 \binom{n}{m} \le n$ iterations.

We can now offer the following theorem for rectangular matrices of full row rank.

Theorem 6.2. *Let $A \in \mathsf{k}[z][\partial;\sigma,\delta]^{m\times n}$ have full rank with entries of degree at most d in ∂, and of degree at most e in z. Let $H \in \mathsf{k}(z)[\partial;\sigma,\delta]^{m\times n}$ be the Hermite form of A and $U \in \mathsf{k}(z)[\partial;\sigma,\delta]^{m\times m}$ such that $UA = H$.*

(a) $\deg_z H_{ij} \in O(m^2de)$ for $1 \le i,j \le n$, and $\deg_z U_{ij} \in O(m^2de)$ for $1 \le i,j \le m$.

(b) We can compute H and U with a deterministic algorithm that requires $O(nm^7d^4 \log(md)\cdot \mathsf{M}(m^2de) + n^2m^3d^2\cdot \mathsf{M}(m^2de))$ or $O^{\sim}(nm^9d^3e + n^2m^5d^3e)$ operations in k.

(c) Assume k has at least $4m^2de$ elements. We can compute H and U with an expected number $O(nm^7d^3\log(md) + nm^7d^3e + n^2m^5d^3e)$ of operations in k (using standard polynomial arithmetic). This algorithm is probabilistic of the Las Vegas type; it never returns an incorrect answer.

Proof. Part (a) from Theorem 5.6 (a), follows since the transformation is computed from an $m \times m$ submatrix of A.

Part (b) follows because each iteration of the binary search requires computing the Hermite form and transformation matrix U of an $m \times m$ submatrix of A. The cost of this is shown in Theorem 5.6. We then check if UA is in Hermite form, which is a matrix multiplication of the $m \times m$ matrix U times the $m \times n$ matrix A. Each entry in U has degree $O(md)$ in ∂ and degree $O(m^2de)$ in z, so the check requires $O(nm^3d^2\cdot \mathsf{M}(m^2de))$. Both the Hermite form computation and the check are done n times, giving the total shown cost. Note that in the event we choose an $m \times m$ submatrix which is row rank deficient, the algorithm will fail, either in the computation of the Hermite form, or in the

final multiplication test, and we do not need to resort to the more expensive row-reduction algorithm outlined in Subsection 6.1.

Part (c) follows similarly to part (b), except that the probabilistic algorithm described in Theorem 5.6 (c) is used. □

Acknowledgement

The authors would like to thank Howard Cheng for his assistance with Section 6.1, and the anonymous referees for their exceptionally detailed and helpful reviews.

They also acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and MITACS Canada.

References

S. Abramov and M. Bronstein. On solutions of linear functional systems. In *Proc. ACM International Symposium on Symbolic and Algebraic Computation*, pages 1–7, 2001.

B. Beckermann, H. Cheng, and G. Labahn. Fraction-free row reduction of matrices of Ore polynomials. *Journal of Symbolic Computation*, 41(1):513–543, 2006.

Y. A. Blinkov, C. F. Cid, V. P. Gerdt, W. Plesken, and D. Robertz. The Maple package Janet: II. linear partial differential equations. In *Proc. Workshop on Computer Algebra and Scientific Computation (CASC)*, pages 41–54, 2003.

M. Bronstein and M. Petkovšek. On Ore rings, linear operators and factorisation. *Programmirovanie*, 20:27–45, 1994.

M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157(1):3–33, 1996.

D. Cantor and E. Kaltofen. Fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28:693–701, 1991.

H. Cheng. *Algorithms for Normal Forms for Matrices of Polynomials and Ore Polynomials.* PhD thesis, University of Waterloo, 2003. URL http://www.cs.uleth.ca/~cheng/publications.html.

F. Chyzak, A. Quadrat, and D. Robertz. Effective algorithms for parametrizing linear control systems over Ore algebras. *Appl. Algebra Eng., Commun. Comput.*, 16:319–376, 2005.

F. Chyzak, A. Quadrat, and D. Robertz. OreModules: A symbolic package for the study of multidimensional linear systems. *Applications of Time Delay Systems*, January 2007.

G. Culianez. Formes de Hermite et de Jacobson: implémentations et applications. Technical report, INRIA, Sophia Antipolis, 2005.

P. Davies, H. Cheng, and G. Labahn. Computing Popov form of general Ore polynomial matrices. In *Milestones in Computer Algebra*, pages 149–156, 2008.

L.E. Dickson. *Algebras and their arithmetics.* G.E. Stechert, New York, 1923.

J. Dieudonné. Les déterminants sur un corps non commutatif. *Bull. Soc. Math. France*, 71:27–45, 1943.

J.D. Dixon. Exact solution of linear equations using p-adic expansions. *Numer. Math.*, 40:137–141, 1982.

P. K. Draxl. *Skew Fields.* Number 81 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1983.

J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, New York, Melbourne, 2003. ISBN 0521826462.

I. Gelfand, S. Gelfand, V. Retakh, and R. Wilson. Quasideterminants. *Advances in Mathematics*, 193(1):56–141, 2005.

I. M. Gel'fand and V. S. Retakh. Determinants of matrices over non-commutative rings. *Functional Analysis and Its Applications*, pages 91–102, 1991.

I. M. Gel'fand and V. S. Retakh. A theory of noncommutative determinants and characteristic functions of graphs. *Functional Analysis and Its Applications*, pages 231–246, 1992.

M. Giesbrecht. *Nearly Optimal Algorithms for Canonical Matrix Forms*. PhD thesis, University of Toronto, 1993. 196 pp.

M. Giesbrecht and A. Heinle. A polynomial-time algorithm for the Jacobson form of a matrix of Ore polynomials. In *Proc. Computer Algebra in Scientific Computation (CASC 2012)*, 2012. To appear.

M. Giesbrecht and M. Kim. On computing the Hermite form of a matrix of differential polynomials. In *Proc. Workshop on Computer Algebra and Scientific Computation (CASC 2009)*, volume 5743 of *Lecture Notes in Computer Science*, pages 118–129, 2009. doi: 10.1007/978-3-642-04103-7_12.

M. Halás. An algebraic framework generalizing the concept of transfer functions to nonlinear systems. *Automatica J. IFAC*, 44(5):1181–1190, 2008.

C. Hermite. Sur l'introduction des variables continues dans la théorie des nombres. *Journal für die reine und angewandte Mathematik*, 41:191–216, 1851.

N. Jacobson. *The Theory of Rings*. American Math. Soc., New York, 1943.

E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Fast parallel computation of Hermite and Smith forms of polynomial matrices. *SIAM Journal of Algebraic and Discrete Methods*, 8:683–690, 1987.

R. Kannan. Polynomial-time algorithms for solving systems of linear equations over polynomials. *Theoretical Computer Science*, 39:69–88, 1985.

Ü. Kotta, A. Leiback, and M. Halás. Non-commutative determinants in nonlinear control theory: Preliminary ideas. *10th Intl. Conf. on Control, Automation, Robotics and Vision Hanoi*, pages 815–820, 2008.

V. Levandovskyy and K. Schindelar. Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases. *Journal of Symbolic Computation*, 46(5):595 – 608, 2011.

J. Middeke. A polynomial-time algorithm for the Jacobson form for matrices of differential operators. Technical Report 08-13, Research Institute for Symbolic Computation (RISC), Linz, Austria, 2008.

T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *Journal of Symbolic Computation*, 35(4):377–401, 2003.

M. Newman. *Integral Matrices*. Academic Press, New York, 1972.

O. Ore. Linear equations in non-commutative fields. *The Annals of Mathematics*, 32(3): 463–477, 1931.

O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34:480–508, 1933.

C. Pernet and W. Stein. Fast computation of Hermite normal forms of random integer matrices. *Journal of Number Theory*, 130:1675–1683, 2010.

V. Popov. Invariant description of linear, time-invariant controllable systems. *SIAM J. Control*, 10:252–264, 1972.

J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Computing Machinery*, 27:701–717, 1980.

H. J. S. Smith. On systems of linear indeterminate equations and congruences. *Philos. Trans. Royal Soc. London*, 151:293–326, 1861.

A. Storjohann. Computation of Hermite and Smith normal forms of matrices. Master's thesis, University of Waterloo, 1994.

Arne Storjohann. High-order lifting and integrality certification. *J. Symb. Comput.*, 36 (3-4):613–648, 2003.

G. Villard. Generalized subresultants for computing the Smith normal form of polynomial matrices. *Journal of Symbolic Computation*, 20:269–286, 1995.

J.H.M. Wedderburn. Non-commutative domains of integrity. *Journal für die reine und angewandte Mathematik*, 167:129–141, 1932.

E. Zerz. An algebraic analysis approach to linear time-varying systems. *IMA Journal of Mathematical Control and Information*, 23:113–126, 2006.