Computing Popov Form of Ore Polynomial Matrices

Patrick Davies Howard Cheng
Department of Mathematics and Computer Science
University of Lethbridge, Canada

Abstract

We show that the computation of the Popov form of Ore polynomial matrices can be formulated as a problem of computing the left nullspace of such matrices. While this technique is already known for polynomial matrices, the extension to Ore polynomial matrices is not immediate because multiplication of the matrix entries is not commutative. A number of results for polynomial matrices are extended to Ore polynomial matrices in this paper. This in turn allows nullspace algorithms to be used in Popov form computations when the input matrix has full row rank. In particular, recent fraction-free and modular algorithms for nullspace computation can be used in exact arithmetic setting where coefficient growth is a concern. In the case when the input matrix does not have full row rank, we show that if a degree bound on the minimal unimodular multiplier is known, the Popov form computation can also be reduced to left nullspace computation.

1 Introduction

Ore polynomials provide a general setting for describing linear differential, difference and q-difference operators [14]. Systems of equations defined by these operators can be represented by matrices of Ore polynomials. In this paper we look at the problem of transforming such matrices into a normal form known as the Popov form. If a matrix is in Popov form, its leading coefficient is triangular so that one may rewrite high-order operators (e.g.

derivatives) in terms of lower ones (Example 2.5). Algorithms for computing the Popov form and the associated unimodular multiplier can also be applied to the computation of greatest common right divisors (GCRDs) and least common left multiples (LCLMs) [1, 5, 9, 10, 11], which represent the intersection and the union of the solution spaces of systems of equations.

Algorithms for computing the Popov form for polynomial matrices are well known [8, 12], but there have been few works on the computation of Popov form for Ore polynomial matrices. The problem was studied in [7] using row reductions, but efficient computation of Popov forms is not considered. In practice, row reductions can introduce significant coefficient growth which must be controlled. This is important in the case of Ore polynomials as coefficient growth is introduced in two ways—from multiplying on the left by powers of the indeterminate and from elimination by cross-multiplication. In the special case of shift polynomial matrices, the fraction-free [1, 5] and modular [6] algorithm can be used to compute a weak Popov form while controlling coefficient growth, but they cannot be used to compute the Popov form directly.

The existing fraction-free and modular algorithms [1, 5, 6] in fact compute a minimal polynomial basis of the left nullspace of any Ore polynomial matrix, such that the basis is represented by an Ore polynomial matrix in Popov form. In this paper, we show that the problem of computing the Popov form and the associated unimodular transformation matrix can be reduced to the problem of computing a left nullspace in Popov form when the input matrix has full row rank. When the input matrix does not have full row rank, the unimodular multiplier is no longer unique. In this case, we define a unique minimal multiplier and show that if a bound on the degree of the minimal multiplier is known, the reduction can still be applied.

The technique of reducing the computation of normal forms such as row-reduced form and Popov form is well known for polynomial matrices [2, 3, 4, 13]. Unfortunately, the proofs of many of the results rely on the fact that the entries of the matrices commute. The main contribution of our work is to extend the results to Ore polynomial matrices and provide proofs that do not rely on the commutativity of matrix elements.

2 Preliminaries

2.1 Notation

For any matrix $\mathbf{A}$, we denote its elements by $\mathbf{A}_{i,j}$. For any sets of row and column indices I and J, we denote by $\mathbf{A}_{I,J}$ the submatrix of $\mathbf{A}$ consisting of the rows and columns indexed by I and J. For convenience, we use I_c to denote the complement of the set I, and $*$ for I and J to denote the sets of all rows and columns, respectively. For any vector of non-negative integers $\vec{\omega} = (\omega_1, \ldots, \omega_p)$, we denote by $|\vec{\omega}| = \sum_{i=1}^{p} \omega_i$. We define $\vec{e} = (1, \ldots, 1)$ of the appropriate dimension. We denote by $\mathbf{I}_m$ the $m \times m$ identity matrix.

2.2 Definitions

We first give some definitions on Ore polynomial matrices. These definitions are similar to those given in previous works [1, 5].

In this paper, we will examine Ore polynomial rings with coefficients in a field $\mathbb{K}$. That is, the ring $\mathbb{K}[Z; \sigma, \delta]$ with σ an automorphism, δ a derivation and with the multiplication rule

$$Z \cdot a = \sigma(a)Z + \delta(a)$$

for all $a \in \mathbb{K}$. When $\delta = 0$, we call the polynomials *shift polynomials.*

Let $\mathbb{K}[Z; \sigma, \delta]^{m \times n}$ be the ring of $m \times n$ Ore polynomial matrices over $\mathbb{K}[Z; \sigma, \delta]$. We shall adapt the following conventions for the remainder of this paper. Let $\mathbf{F}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times n}$ and $N = \deg \mathbf{F}(Z)$. An Ore polynomial matrix $\mathbf{F}(Z)$ is said to have *row degree* $\vec{\mu} = \operatorname{rdeg} \mathbf{F}(Z)$ if the ith row has degree μ_i. The *leading row coefficient* of $\mathbf{F}(Z)$, denoted $\mathrm{LC}_{row}(\mathbf{F}(Z))$, is the matrix whose entries are the coefficients of Z^N of the corresponding elements of $Z^{N \cdot \vec{e} - \vec{\mu}} \cdot \mathbf{F}(Z)$. An Ore polynomial matrix $\mathbf{F}(Z)$ is *row-reduced* if $\mathrm{LC}_{row}(\mathbf{F}(Z))$ has maximal row rank. We also recall that the *rank* of $\mathbf{F}(Z)$ is the maximum number of $\mathbb{K}[Z; \sigma, \delta]$-linearly independent rows of $\mathbf{F}(Z)$, and that $\mathbf{U}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times m}$ is *unimodular* if there exists $\mathbf{V}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times m}$ such that $\mathbf{V}(Z) \cdot \mathbf{U}(Z) = \mathbf{U}(Z) \cdot \mathbf{V}(Z) = \mathbf{I}_m$.

Definition 2.1 (Pivot Index) *Let* $\mathbf{F}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times n}$ *with row degree* $\vec{\mu}$. *We define the* pivot index Π_i *of the* i*th row as*

$$\Pi_i = \begin{cases} \min_{1 \le j \le n} \left\{ j : \deg \mathbf{F}(Z)_{i,j} = \mu_i \right\} & \mu_i \ge 0, \\ 0 & \textit{otherwise.} \end{cases} \tag{1}$$

□

Definition 2.2 (Popov Normal Form) *Let* $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ *with pivot indices* $\Pi_1,\ldots,\Pi_m$ *and row degree* $\vec{\mu}$*. Then* $\mathbf{F}(Z)$ *is in* Popov form *if it may be partitioned as*

$$\mathbf{F}(Z) = \begin{bmatrix} \mathbf{0} \\ \mathbf{F}(Z)_{J_c,*} \end{bmatrix}, \tag{2}$$

where $J = (1,\ldots,n-r)$ *and* $r = rank\, \mathbf{F}(Z)$*, and for all* $i,j \in J_c$ *we have*

(a) $\Pi_i < \Pi_j$ *whenever* $i < j$*;*

(b) $\mathbf{F}(Z)_{i,\Pi_i}$ *is monic;*

(c) If $k = \Pi_j$ *for some* $j \neq i$*, then* $\deg \mathbf{F}(Z)_{i,k} < \mu_j$*.*

□

If a matrix is in Popov form, its *pivot set* is defined as $\{\Pi_i \ : \ \Pi_i > 0\}$.

Remark 2.3 *If* $\mathbf{F}(Z)$ *is in Popov form, then the definition of pivot indices also implies that*

$$\deg \mathbf{F}(Z)_{i,k} \begin{cases} = \mu_i & k = \Pi_i \\ \leq \min(\mu_i - 1, \mu_j - 1) & k < \Pi_i \textit{ and } k = \Pi_j \textit{ for some } j \neq i \\ \leq \min(\mu_i, \mu_j - 1) & k > \Pi_i \textit{ and } k = \Pi_j \textit{ for some } j \neq i \\ \leq \mu_i - 1 & k < \Pi_i \textit{ and } k \neq \Pi_j \textit{ for all } j \neq i \\ \leq \mu_i & k > \Pi_i \textit{ and } k \neq \Pi_j \textit{ for all } j \neq i\ . \end{cases} \tag{3}$$

Also, a matrix in Popov form is also in row-reduced form. □

Every matrix $\mathbf{F}(Z)$ can be transformed into a unique matrix in Popov form using the following elementary row operations:

(a) interchange two rows;

(b) multiply a row by a nonzero element in $\mathbb{K}$;

(c) add a polynomial multiple of one row to another.

Formally, we may view a sequence of elementary row operations as a *unimodular transformation matrix* $\mathbf{U}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times m}$ with the result of these operations given by $\mathbf{T}(Z) = \mathbf{U}(Z)\cdot\mathbf{F}(Z)$. We recall the following result from [1, Theorem 2.2] and [5, Theorem 3.1].

Theorem 2.4 *For any $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ there exists a unimodular matrix $\mathbf{U}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times m}$, with $\mathbf{T}(Z) = \mathbf{U}(Z)\cdot\mathbf{F}(Z)$ having $r \le \min\{m,n\}$ nonzero rows, rdeg $\mathbf{T}(Z) \le$ rdeg $\mathbf{F}(Z)$, and where the submatrix consisting of the r nonzero rows of $\mathbf{T}(Z)$ is row-reduced. Moreover, the unimodular multiplier satisfies the degree bound*

$$\textit{rdeg}\ \mathbf{U}(Z) \le \vec{\nu} + (|\vec{\mu}| - |\vec{\nu}| - \alpha)\cdot\vec{e} \tag{4}$$

where $\vec{\mu} = \max(\vec{0}, \textit{rdeg}\ \mathbf{F}(Z))$, $\vec{\nu} = \max(\vec{0}, \textit{rdeg}\ \mathbf{T}(Z))$, and $\alpha = \min_j\{\mu_j\}$. □

Example 2.5 *Consider the differential algebraic system*

$$\begin{array}{rcrcrcl}
y_1''(t) + (t+2)y_1(t) & + & y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0\\
y_1''(t) + y_1'(t) + 3y_1(t) & + & y_2^{(3)}(t) + 2y_2'(t) - y_2(t) & + & y_3^{(3)}(t) - 2t^2y_3(t) & = & 0\\
y_1'(t) + y_1(t) & + & y_2^{(3)}(t) + 2ty_2'(t) - y_2(t) & + & y_3^{(4)}(t) & = & 0.
\end{array} \tag{5}$$

Let D denote the differential operator on $\mathbb{Q}(t)$ such that $D\cdot f(t) = \frac{d}{dt}f(t)$. Then the matrix form of (5) is:

$$\begin{bmatrix} D^2+(t+2) & D^2+1 & D+1\\ D^2+D+3 & D^3+2D-1 & D^3-2t^2\\ D+1 & D^3+2tD+1 & D^4 \end{bmatrix}\cdot\begin{bmatrix} y_1(t)\\ y_2(t)\\ y_3(t)\end{bmatrix} = \mathbf{0}. \tag{6}$$

The leading row coefficient (matrix of coefficients of the highest power of the corresponding row) is upper triangular. This allows us to rewrite the highest derivative in each row as a combination of other derivatives. For example, we can eliminate the highest derivatives of $y_2(t)$ as follows:

$$\begin{aligned}
y_2^{(3)}(t) =&- y_1''(t) - y_1'(t) - 3y_1(t) - 2y_2'(t) + y_2(t) - y_3^{(3)}(t) + 2t^2y_3(t)\\
=&- ((t+2)y_1(t) - y_2''(t) - y_2(t) - y_3'(t) - y_3(t)) - y_1'(t) - 3y_1(t)\\
&- 2y_2'(t) + y_2(t) - y_3^{(3)}(t) + 2t^2y_3(t)\\
=&- y_1'(t) - (t+5)y_1(t) + y_2''(t) - 2y_2'(t) + 2y_2(t) - y_3^{(3)}(t) + y_3'(t)\\
&+ (2t^2+1)y_3(t).
\end{aligned}$$

□

3 General Approach

Given an $m \times n$ matrix $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$, we wish to compute a unimodular matrix $\mathbf{U}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times m}$ and $\mathbf{T}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ such that

$$\mathbf{U}(Z) \cdot \mathbf{F}(Z) = \mathbf{T}(Z), \tag{7}$$

where $\mathbf{T}(Z)$ is in Popov form.

Given an Ore polynomial matrix $\mathbf{G}(Z)$, the fraction-free and modular algorithms [1, 5, 6] can be used to compute a minimal polynomial basis $\mathbf{M}(Z)$ of the left nullspace of $\mathbf{G}(Z)$ such that $\mathbf{M}(Z) \cdot \mathbf{G}(Z) = \mathbf{0}$ and $\mathbf{M}(Z)$ is in Popov form. Using these algorithms, we compute the left nullspace of the matrix

$$\begin{bmatrix} \mathbf{F}(Z) \cdot Z^b \\ -\mathbf{I}_n. \end{bmatrix} \tag{8}$$

Then the nullspace $\mathbf{M}(Z)$ can be partitioned as $[\mathbf{U}(Z) \;\; \mathbf{T}(Z) \cdot Z^b]$ such that

$$\begin{bmatrix} \mathbf{U}(Z) & \mathbf{T}(Z) \cdot Z^b \end{bmatrix} \cdot \begin{bmatrix} \mathbf{F}(Z) \cdot Z^b \\ -\mathbf{I}_n \end{bmatrix} = \mathbf{0}. \tag{9}$$

The matrix $\mathbf{U}(Z)$ obtained in this manner is unimodular.

Lemma 3.1 *Suppose that* $\begin{bmatrix} \mathbf{U}(Z) & \mathbf{T}(Z) \end{bmatrix}$ *is a basis of the left nullspace of* $\begin{bmatrix} \mathbf{F}(Z) \\ -\mathbf{I}_n \end{bmatrix}$. *Then* $\mathbf{U}(Z)$ *is unimodular.*

Proof. Note that the rows of $\begin{bmatrix} \mathbf{I}_m & \mathbf{F}(Z) \end{bmatrix}$ belong to the left nullspace of $\begin{bmatrix} \mathbf{F}(Z) \\ -\mathbf{I}_n \end{bmatrix}$. Since $\begin{bmatrix} \mathbf{U}(Z) & \mathbf{T}(Z) \end{bmatrix}$ is a basis of the left nullspace, there exists $\mathbf{V}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times m}$ such that $\mathbf{V}(Z) \cdot \mathbf{U}(Z) = \mathbf{I}_m$. In other words, $\mathbf{U}(Z)$ has a left inverse.

To see that $\mathbf{V}(Z)$ is also a right inverse, we note that $\mathbf{U}(Z) \cdot \mathbf{V}(Z) \cdot \mathbf{U}(Z) = \mathbf{U}(Z)$. Therefore,

$$(\mathbf{U}(Z) \cdot \mathbf{V}(Z) - \mathbf{I}_m) \cdot \mathbf{U}(Z) = \mathbf{0}. \tag{10}$$

Now

$$m = \text{rank } \mathbf{I}_m = \text{rank } (\mathbf{V}(Z) \cdot \mathbf{U}(Z)) \leq \text{rank } \mathbf{U}(Z) \leq m \tag{11}$$

It follows that $\mathbf{U}(Z)$ has full row rank. Thus, (10) implies that $\mathbf{U}(Z) \cdot \mathbf{V}(Z) - \mathbf{I}_m = \mathbf{0}$, so that $\mathbf{V}(Z)$ is also a right inverse of $\mathbf{U}(Z)$. Since $\mathbf{U}(Z)$ has a two-sided inverse, it is unimodular. □

Furthermore, if $b > \deg \mathbf{U}(Z)$, this also implies that $\mathbf{T}(z)$ is in Popov form since the leading coefficients are "contributed" by $\mathbf{T}(z)$. Thus, our goal is to determine an upper bound on $\deg \mathbf{U}(Z)$.

A similar approach has also been used to compute the row-reduced form and the Popov form of polynomial matrices [2, 3, 4, 13].

4 Degree Bound in the Full Row Rank Case

In the case when the input matrix $\mathbf{F}(Z)$ has full row rank, we follow the approach of [4] in order to obtain a bound for $\deg \mathbf{U}(Z)$. Our main contribution is the generalization of the proofs to the case of Ore polynomial matrices.

We first prove some results which relate the degrees of the input matrix $\mathbf{F}(Z)$, the unimodular multiplier $\mathbf{U}(Z)$, and the transformed matrix $\mathbf{T}(Z)$.

Lemma 4.1 *Suppose $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m \times n}$ has full row rank, and let $\mathbf{T}_1(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m \times n}$ be a row-reduced form of $\mathbf{F}(Z)$. Suppose that $\mathbf{T}_2(Z) = \mathbf{U}_2(Z) \cdot \mathbf{F}(Z)$ for some unimodular matrix $\mathbf{U}_2(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m \times m}$, with $\vec{\gamma} = rdeg\ \mathbf{T}_2(Z)$. There exists a unimodular matrix $\mathbf{V}(Z)$ such that $\mathbf{T}_2(Z) = \mathbf{V}(Z) \cdot \mathbf{T}_1(Z)$ and $\deg \mathbf{V}(Z)_{i,j} \le \gamma_i - \nu_j$ where $\vec{\nu} = rdeg\ \mathbf{T}_1(Z)$.*

Proof. Since $\mathbf{T}_1(Z)$ is a row-reduced form of $\mathbf{F}(Z)$, there exists a unimodular matrix $\mathbf{U}_1(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m \times m}$ such that $\mathbf{U}_1(Z) \cdot \mathbf{F}(Z) = \mathbf{T}_1(Z)$. Setting $\mathbf{V}(Z) = \mathbf{U}_2(Z) \cdot \mathbf{U}_1(Z)^{-1}$ gives $\mathbf{T}_2(Z) = \mathbf{V}(Z) \cdot \mathbf{T}_1(Z)$. Since $\mathbf{V}(Z)$ is a product of unimodular matrices, it is unimodular.

Since $\mathbf{T}_1(Z)$ is row-reduced, we can apply the predictable degree property [1, Lemma A.1(a)] to obtain

$$\deg \mathbf{V}(Z)_{i,j} + \deg \mathbf{T}_1(Z)_{j,\cdot} \le \deg \mathbf{T}_2(Z)_{i,\cdot}, \tag{12}$$

which implies that $\deg \mathbf{V}(Z)_{i,j} \le \gamma_i - \nu_j$. □

Theorem 4.2 *Suppose that $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m \times n}$ has full row rank. Let $\mathbf{V}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m \times m}$ be unimodular and let $\mathbf{T}(Z) = \mathbf{V}(Z) \cdot \mathbf{F}(Z)$ with $\vec{\gamma} = rdeg\ \mathbf{T}(Z)$. There exists a unimodular matrix $\mathbf{U}(Z)$ such that $\mathbf{U}(Z) \cdot \mathbf{F}(Z) = \mathbf{T}(Z)$ and*

$$rdeg\ \mathbf{U}(Z) \le \vec{\gamma} + (|\vec{\mu}| - \alpha) \cdot \vec{e}, \tag{13}$$

where $\vec{\mu} = rdeg\ \mathbf{F}(Z)$ and $\alpha = \min_j\{\mu_j\}$.

Proof. By Theorem 2.4, there exists a unimodular matrix $\mathbf{U}_1(Z)$ such that $\mathbf{T}_1(Z) = \mathbf{U}_1(Z) \cdot \mathbf{F}(Z)$ is row-reduced and

$$\text{rdeg}\ \mathbf{U}_1(Z) \leq \vec{\nu} + (|\vec{\mu}| - |\vec{\nu}| - \alpha) \cdot \vec{e}, \tag{14}$$

with $\vec{\nu} = \text{rdeg}\ \mathbf{T}_1(Z)$. By Lemma 4.1, there exists a unimodular matrix $\mathbf{U}_2(Z)$ such that $\mathbf{T}(Z) = \mathbf{U}_2(Z) \cdot \mathbf{T}_1(Z) = \mathbf{U}_2(Z) \cdot \mathbf{U}_1(Z) \cdot \mathbf{F}(Z)$. Setting $\mathbf{U}(Z) = \mathbf{U}_2(Z) \cdot \mathbf{U}_1(Z)$ gives

$$\mathbf{U}(Z) \cdot \mathbf{F}(Z) = \mathbf{T}(Z).$$

For the degree bound, note that

$$\begin{aligned} \deg \mathbf{U}(Z)_{i,j} &\leq \max_{1 \leq k \leq m} \deg \mathbf{U}_2(Z)_{i,k} + \deg \mathbf{U}_1(Z)_{k,j} && (15) \\ &\leq \max_{1 \leq k \leq m} (\gamma_i - \nu_k) + (\nu_k + |\vec{\mu}| - |\vec{\nu}| - \alpha) && (16) \\ &\leq \gamma_i + |\vec{\mu}| - \alpha. && (17) \end{aligned}$$

□

We have only stated the existence of unimodular matrices satisfying certain degree bounds in the previous results. We now show that such unimodular matrices are also unique.

Lemma 4.3 *Suppose that* $\mathbf{F}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times n}$ *has full row rank. Given* $\mathbf{T}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times n}$*, the solution* $\mathbf{U}(Z) \in \mathbb{K}[Z; \sigma, \delta]^{m \times m}$ *to the equation*

$$\mathbf{U}(Z) \cdot \mathbf{F}(Z) = \mathbf{T}(Z) \tag{18}$$

is unique (if it exists).

Proof. Let $\mathbf{U}_1(Z)$ and $\mathbf{U}_2(Z)$ be two matrices such that

$$\mathbf{U}_1(Z) \cdot \mathbf{F}(Z) = \mathbf{T}(Z) = \mathbf{U}_2(Z) \cdot \mathbf{F}(Z). \tag{19}$$

Then $(\mathbf{U}_1(Z) - \mathbf{U}_2(Z)) \cdot \mathbf{F}(Z) = \mathbf{0}$. Since $\mathbf{F}(Z)$ has full row rank, it follows that $\mathbf{U}_1(Z) - \mathbf{U}_2(Z) = \mathbf{0}$ and hence $\mathbf{U}_1(Z) = \mathbf{U}_2(Z)$. □

Since $\mathbf{F}(Z)$ has full row rank, the uniqueness of the unimodular multiplier gives us a bound on the degree of the unimodular multiplier.

Theorem 4.4 *Suppose that* $\mathbf{F}(Z)$ *has full row rank. If* $\mathbf{T}(Z) = \mathbf{U}(Z) \cdot \mathbf{F}(Z)$ *for some unimodular matrix* $\mathbf{U}(Z)$ *then* $\mathbf{U}(Z)$ *satisfies the degree bound (4).*

Proof. This is an easy consequence of Theorem 4.2 and Lemma 4.3. □

Finally, we give a degree bound on $\mathbf{U}(Z)$ and provide a method to compute the Popov form of $\mathbf{F}(Z)$ and the associated unimodular multiplier $\mathbf{U}(Z)$.

Theorem 4.5 *Suppose that* $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ *has full row rank and has row degree* $\vec{\mu}$. *Let* $b > |\vec{\mu}| - \min_j\{\mu_j\}$, *and suppose* $\begin{bmatrix}\mathbf{U}(Z) & \mathbf{R}(Z)\end{bmatrix}$ *is a basis in Popov form of the left nullspace of* $\begin{bmatrix}\mathbf{F}(Z)\cdot Z^b \\ -\mathbf{I}_n\end{bmatrix}$. *Let* $\mathbf{T}(Z) = \mathbf{R}(Z)\cdot Z^{-b}$. *Then*

(a) $\mathbf{U}(Z)$ *is unimodular;*

(b) $\mathbf{T}(Z) = \mathbf{U}(Z)\cdot\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$*;*

(c) $\mathbf{T}(Z)$ *is in Popov form.*

Proof. Part (a) is immediate from Lemma 3.1. For (b), we see that $\mathbf{U}(Z)\cdot\mathbf{F}(Z)\cdot Z^b = \mathbf{R}(Z)$, so $\mathbf{T}(Z) = \mathbf{U}(Z)\cdot\mathbf{F}(Z)$. To prove (c), we see from Theorem 4.4 that

$$\text{rdeg } \mathbf{U}(Z) \le \vec{\nu} + (|\vec{\mu}| - \alpha)\cdot\vec{e} \tag{20}$$

where $\vec{\mu} = \text{rdeg } \mathbf{F}(Z)$, $\vec{\nu} = \text{rdeg } \mathbf{T}(Z)$, and $\alpha = \min_j\{\mu_j\}$. Therefore,

$$\text{rdeg } \mathbf{U}(Z) \le \text{rdeg } \mathbf{R}(Z) + (|\vec{\mu}| - \alpha - b)\cdot\vec{e} < \text{rdeg } \mathbf{R}(Z). \tag{21}$$

Thus, the leading coefficient of $\begin{bmatrix}\mathbf{U}(Z) & \mathbf{R}(Z)\end{bmatrix}$ is the same as the leading coefficient of $\begin{bmatrix}\mathbf{0} & \mathbf{R}(Z)\end{bmatrix}$. It follows that $\mathbf{R}(Z)$ and hence $\mathbf{T}(Z)$ is in Popov form. □

From the theorem above, we see that the computation of Popov form and the associated unimodular matrix can be reduced to left nullspace computation.

5 Minimal Multipliers

In the case when the input matrix $\mathbf{F}(Z)$ does not have full row rank, the situation is considerably more complicated. In fact, a unimodular multiplier of arbitrarily high degree exists. To see this, suppose

$$\mathbf{T}(Z) = \begin{bmatrix}\mathbf{0} \\ \mathbf{T}(Z)_{J_c,*}\end{bmatrix} = \mathbf{U}(Z)\cdot\mathbf{F}(Z) \tag{22}$$

is the Popov form of $\mathbf{F}(Z)$. It follows that one may add any polynomial multiple of the rows of $\mathbf{U}(Z)_{J,*}$ to the other rows of $\mathbf{U}(Z)$ and still obtain a unimodular multiplier $\mathbf{U}'(Z)$ satisfying $\mathbf{T}(Z) = \mathbf{U}'(Z) \cdot \mathbf{F}(Z)$.

In this section, we show that all unimodular multipliers satisfying $\mathbf{T}(Z) = \mathbf{U}(Z) \cdot \mathbf{F}(Z)$ are related, and that there is a unique multiplier that has minimal column degrees and is normalized in some way. Before we prove the main results, we first give an important result related to "division" of Ore polynomial matrices. Intuitively, this allows to "reduce" one Ore polynomial matrix by another one that is in Popov form to obtain a unique remainder. This is an analogue of [3, Lemma 3.5].

Lemma 5.1 *Let $\mathbf{B}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{n\times n}$ be a full row rank matrix in Popov form with row degree $\vec{\beta}$. Then for any $\mathbf{A}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ with row degree $\vec{\gamma}$, there exist unique matrices $\mathbf{Q}(Z), \mathbf{R}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ such that*

$$\mathbf{A}(Z) - \mathbf{Q}(Z) \cdot \mathbf{B}(Z) = \mathbf{R}(Z), \tag{23}$$

where for all i, j, $\deg \mathbf{R}(Z)_{i,j} < \beta_j$ and $\deg \mathbf{Q}(Z)_{i,j} \leq \gamma_i - \beta_j$.

Proof. It suffices to prove this in the case $m = 1$ as we may consider each row of (23) independently.

We first show the existence of $\mathbf{Q}(Z)$ and $\mathbf{R}(Z)$. Let $K = \{k : \deg \mathbf{A}(Z)_{1,k} \geq \beta_k\}$, and $d = \deg \mathbf{A}(Z)_{1,K}$. Define $t \in K$ to be the pivot index of $\mathbf{A}(Z)_{1,K}$. Thus,

$$\mathbf{A}(Z)_{1,t} = aZ^d + \cdots \tag{24}$$

for some $a \in \mathbb{K}$. If

$$\mathbf{B}(Z)_{t,t} = bZ^{\beta_t} + \cdots \tag{25}$$

for some $b \in \mathbb{K}$. Let

$$\hat{\mathbf{R}}_{\mathbf{1}}(Z) = \mathbf{A}(Z) - \hat{\mathbf{Q}}_{\mathbf{1}}(Z) \cdot \mathbf{B}(Z) \tag{26}$$

where $\hat{\mathbf{Q}}_{\mathbf{1}}(Z) = \begin{bmatrix} 0 \cdots 0 & \frac{a}{\sigma^{d-\beta_t}(b)} Z^{d-\beta_t} & 0 \cdots 0 \end{bmatrix}$ with the nonzero element in the t^{th} column. It is easy to see that $\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,t} < d$.

Since $\mathbf{B}(Z)$ is in Popov form,

$$\deg \mathbf{B}(Z)_{t,s} \leq \begin{cases} \beta_t & \text{if } s \geq t, \\ \beta_t - 1 & \text{otherwise.} \end{cases} \tag{27}$$

From the degree bounds on $\mathbf{A}(Z)_{1,K}$, we see that for $s \in K$ we have

$$\deg \hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} \leq \begin{cases} d & \text{if } s > t, \\ d-1 & \text{otherwise.} \end{cases} \tag{28}$$

For $s \notin K$, we have

$$\begin{aligned} \deg \hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} &= \deg \left[\mathbf{A}(Z) - \hat{\mathbf{Q}}_{\mathbf{1}}(Z) \cdot \mathbf{B}(Z)\right]_{1,s} \\ &\leq \max(\deg \mathbf{A}(Z)_{1,s}, \deg [\hat{\mathbf{Q}}_{\mathbf{1}}(Z) \cdot \mathbf{B}(Z)]_{1,s}). \end{aligned} \tag{29}$$

If $\deg \hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} \leq \deg \mathbf{A}(Z)_{1,s}$, then $\deg \hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} < \beta_s$ by definition of K. Otherwise,

$$\deg \hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} = \deg [\hat{\mathbf{Q}}_{\mathbf{1}}(Z) \cdot \mathbf{B}(Z)]_{1,s} \leq \begin{cases} (d-\beta_t) + \beta_t = d & \text{if } s > t, \\ (d-\beta_t) + \beta_t - 1 = d-1 & \text{otherwise.} \end{cases} \tag{30}$$

Let $\hat{K} = \{k : \deg \hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,k} \geq \beta_k\}$. We see that either $\deg \hat{\mathbf{R}}_{\mathbf{1}}(Z) < d$, or $\deg \hat{\mathbf{R}}_{\mathbf{1}}(Z) = d$ and the pivot index of $\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,\hat{K}}$ must be greater than t. We also note that it is possible that $\hat{K} \neq K$.

Continuing in this way we may construct $\hat{\mathbf{R}}_{\mathbf{2}}(Z), \hat{\mathbf{R}}_{\mathbf{3}}(Z), \ldots,$ so that after each step either the degree is decreased or the pivot index is increased. Therefore, in a finite number of steps we will have

$$\hat{\mathbf{R}}_{\mathbf{k}}(Z) = \mathbf{A}(Z) - \left[\hat{\mathbf{Q}}_{\mathbf{1}}(Z) + \cdots + \hat{\mathbf{Q}}_{\mathbf{k}}(Z)\right] \cdot \mathbf{B}(Z), \tag{31}$$

where $\deg \hat{\mathbf{R}}_{\mathbf{k}}(Z)_{1,j} < \beta_j$ for all j. Finally, setting $\mathbf{Q}(Z) = \hat{\mathbf{Q}}_{\mathbf{1}}(Z) + \cdots + \hat{\mathbf{Q}}_{\mathbf{k}}(Z)$, $\mathbf{R}(Z) = \hat{\mathbf{R}}_{\mathbf{k}}(Z)$ gives us the desired divisor and remainder matrices of (23).

To show uniqueness, suppose that we have

$$\begin{aligned} \mathbf{A}(Z)_{1,*} &= \mathbf{Q}_{\mathbf{1}}(Z) \cdot \mathbf{B}(Z) + \mathbf{R}_{\mathbf{1}}(Z) \\ &= \mathbf{Q}_{\mathbf{2}}(Z) \cdot \mathbf{B}(Z) + \mathbf{R}_{\mathbf{2}}(Z) \end{aligned}$$

for some $\mathbf{Q}_{\mathbf{1}}(Z)$, $\mathbf{Q}_{\mathbf{2}}(Z)$, $\mathbf{R}_{\mathbf{1}}(Z)$, and $\mathbf{R}_{\mathbf{2}}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{1\times n}$. Letting $\hat{\mathbf{Q}}(Z) = \mathbf{Q}_{\mathbf{1}}(Z) - \mathbf{Q}_{\mathbf{2}}(Z)$ and $\hat{\mathbf{R}}(Z) = \mathbf{R}_{\mathbf{2}}(Z) - \mathbf{R}_{\mathbf{1}}(\mathbf{Z})$ gives

$$\hat{\mathbf{R}}(Z) = \hat{\mathbf{Q}}(Z) \cdot \mathbf{B}(Z) \tag{32}$$

with $\deg \hat{\mathbf{R}}(Z)_{1,j} < \beta_j$. Let k be such that $\deg \hat{\mathbf{R}}(Z)_{1,k} = \deg \hat{\mathbf{R}}(\mathbf{Z})$. Since $\mathbf{B}(Z)$ is row reduced, the predictable degree property [1, Lemma A.1(a)] implies that

$$\deg \hat{\mathbf{Q}}(\mathbf{Z})_{1,k} \leq \deg \hat{\mathbf{R}}(Z)_{1,k} - \beta_k < 0, \tag{33}$$

so that $\hat{\mathbf{Q}}(\mathbf{Z})_{1,k} = 0$ whenever $\deg \hat{\mathbf{R}}(Z)_{1,k} = \deg \hat{\mathbf{R}}(\mathbf{Z})$. Now, let $K = \{k : \deg \hat{\mathbf{R}}(Z)_{1,k} < \deg \hat{\mathbf{R}}(\mathbf{Z})\}$. If K is non-empty, consider the equation

$$\hat{\mathbf{R}}(Z)_{1,K} = \hat{\mathbf{Q}}(Z)_{1,K} \cdot \mathbf{B}(Z)_{K,K}. \tag{34}$$

A similar argument shows that $\hat{\mathbf{Q}}(Z)_{1,k} = 0$ whenever $\deg \hat{\mathbf{R}}(\mathbf{Z})_{1,k} = \deg \hat{\mathbf{R}}(\mathbf{Z})_{1,K}$. Continuing in this way it can be seen that $\hat{\mathbf{Q}}(Z) = \hat{\mathbf{R}}(Z) = \mathbf{0}$, so that the matrices $\mathbf{Q}(Z)$ and $\mathbf{R}(Z)$ in (23) are unique.

Finally, we prove the degree bound for $\mathbf{Q}(Z)$. For any $1 \leq i \leq m$, let $L_i = \{j : \gamma_i \geq \beta_j\}$. Then for $j \notin L_i$ we have $\gamma_i < \beta_j$ and therefore $\mathbf{Q}(Z)_{i,j} = 0$ because $\mathbf{Q}(Z)$ is unique. If $j \in L_i$, we have

$$\deg(\mathbf{Q}(Z)_{i,L_i} \cdot \mathbf{B}(Z)_{L_i,L_i}) = \deg(\mathbf{A}(Z)_{i,L_i} - \mathbf{R}(Z)_{i,L_i}) \leq \gamma_i. \tag{35}$$

Applying the predictable degree property, we have $\deg(\mathbf{Q}(Z)_{i,L_i} \cdot \mathbf{B}(Z)_{L_i,L_i}) \geq \deg \mathbf{Q}(Z)_{i,j} + \beta_j$, for all $j \in L_i$. □

We can now show the main result in this section which shows the relationship among all unimodular multipliers. This result is an analogue of [3, Theorem 3.3].

Theorem 5.2 *Let $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ with row rank r. Let $\mathbf{U}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times m}$ be unimodular such that $\mathbf{U}(Z) \cdot \mathbf{F}(Z) = \mathbf{T}(Z)$, with $\mathbf{T}(Z) = \begin{bmatrix} 0 \\ \mathbf{T}(Z)_{J_c,*} \end{bmatrix}$ the unique Popov form of $\mathbf{F}(Z)$.*

(a) A unimodular matrix $\mathbf{U}(Z)$ is unique up to multiplication on the left by matrices of the form

$$\mathbf{W}(Z) = \begin{bmatrix} \mathbf{W}(Z)_{J,J} & 0 \\ \mathbf{W}(Z)_{J_c,J} & \mathbf{I}_r \end{bmatrix}, \tag{36}$$

where $\mathbf{W}(Z)_{J,J} \in \mathbb{K}[Z;\sigma,\delta]^{(m-r)\times(m-r)}$ is unimodular.

(b) *There exists a unique multiplier* $\mathbf{U}(Z)$ *such that* $\mathbf{U}(Z)_{J,*}$ *is a minimal polynomial basis in Popov form for the left nullspace of* $\mathbf{F}(Z)$ *with pivot set* K*, and*

$$\deg \mathbf{U}(Z)_{j,k} < \max_{\ell \in J} \deg \mathbf{U}(Z)_{\ell,k} \tag{37}$$

for all $k \in K, j \in J_c$.

(c) *Under all multipliers mentioned in (a), the sum of the row degrees of the unique multiplier* $\mathbf{U}(Z)$ *of (b) is minimal.*

Proof. To prove (a), let $\mathbf{U_1}(Z)$ and $\mathbf{U_2}(Z)$ be two such unimodular multipliers for the Popov form of $\mathbf{F}(Z)$. Then $\mathbf{U_1}(Z)_{J,*}, \mathbf{U_2}(Z)_{J,*}$, are bases of the left nullspace of $\mathbf{F}(Z)$. Thus there exists a unimodular multiplier $\mathbf{W}(Z)_{J,J}$ such that

$$\mathbf{U_1}(Z)_{J,*} = \mathbf{W}(Z)_{J,J}\mathbf{U_2}(Z)_{J,*}. \tag{38}$$

By the uniqueness of $\mathbf{T}(Z)_{J_c,*}$, the rows of $\mathbf{U_2}(Z)_{J_c,*} - \mathbf{U_1}(Z)_{J_c,*}$ are in the nullspace of $\mathbf{F}(Z)$, so there exists a matrix $\mathbf{W}(Z)_{J_c,J}$ such that

$$\mathbf{U_2}(Z)_{J_c,*} = \mathbf{U_1}(Z)_{J_c,*} + \mathbf{W}(Z)_{J_c,J}\mathbf{U_1}(Z)_{J,*}. \tag{39}$$

This gives the form of the multipliers as stated in (a).

For (b), assume that $\mathbf{U}(Z)_{J,*}$ is the unique Popov minimal polynomial basis for the left nullspace with pivot set K. Given any multiplier $\mathbf{U_0}(Z)$ we may divide $\mathbf{U_0}(Z)_{J_c,K}$ on the right by $\mathbf{U}(Z)_{J,K}$:

$$\mathbf{U_0}(Z)_{J_c,K} = \mathbf{W}(Z)_{J_c,J}\mathbf{U}(Z)_{J,K} + \mathbf{U}(Z)_{J_c,K}. \tag{40}$$

By Lemma 5.1, (37) is satisfied. Since $\mathbf{U}(Z)_{J_c,K}$ is the unique matrix such that (37) is satisfied, the generic form of a multiplier given in (a) implies that

$$\mathbf{U}(Z)_{J_c,*} = \mathbf{U_0}(Z)_{J_c,*} - \mathbf{W}(Z)_{J_c,J}\mathbf{U}(Z)_{J,*}. \tag{41}$$

Thus, the minimal multiplier $\mathbf{U}(Z)$ is well defined and unique. This proves (b).

To prove (c), let $\mathbf{U_0}(Z)$ be a second unimodular multiplier. From the general form of the multipliers, the sum of the row degrees of J and J_c can be minimized independently. Since the degrees in J are minimized by choosing a minimal polynomial basis, we are only concerned about the rows in J_c. We want to show that

$$|\text{rdeg } \mathbf{U_0}(Z)_{J_c,*}| \geq |\text{rdeg } \mathbf{U}(Z)_{J_c,*}|. \tag{42}$$

Let $\vec{\beta} = \text{rdeg } \mathbf{U}(Z)_{J,*}$, $\vec{\mu} = \text{rdeg } \mathbf{U_0}(Z)_{J_c,K}$, and $\vec{\gamma} = \text{rdeg } \mathbf{U_0}(Z)_{J_c,K_c}$. The degree sum for $\mathbf{U_0}(Z)_{J_c,*}$ is $\sum_j \max(\mu_j, \gamma_j)$. By Lemma 5.1, we have quotient $\mathbf{W}(Z)_{J_c,J}$ such that

$$\mathbf{U}(Z)_{J_c,*} = \mathbf{U_0}(Z)_{J_c,*} - \mathbf{W}(Z)_{J_c,J}\mathbf{U}(Z)_{J,*} \tag{43}$$

with $\deg \mathbf{W}(Z)_{i,j} \leq \mu_i - \beta_j$. Therefore we have, for $1 \leq i \leq m$ and $j \in J_c$,

$$\deg \mathbf{U}(Z)_{i,j} \leq \max(\max(\mu_i, \gamma_i), \mu_i) = \max(\mu_i, \gamma_i). \tag{44}$$

Thus the degree sum of the J_c rows is not increased by the normalizing division, and gives (c). □

The unique multiplier given in Theorem 5.2 (b) is called the *minimal multiplier.*

Remark 5.3 *We note that if* $\mathbf{U}(Z)$ *is the minimal multiplier for* $\mathbf{F}(Z)$ *and* $\vec{\beta}$ *is the degree of the minimal polynomial basis, we have*

$$\deg \mathbf{U}(Z)_{j,k} \leq \begin{cases} \beta_j & \textit{if } j \in J, \\ \beta_j - 1 & \textit{if } j \in J_c \textit{ and } k \in K. \end{cases} \tag{45}$$

Since $\beta_i \leq (m-1)N$ *where* $N = \deg \mathbf{F}(Z)$ *[1, Theorem A.2].* □

In order to give a bound on $\deg \mathbf{U}(Z)$, it remains to obtain a bound for $\deg \mathbf{U}(Z)_{J_c,K_c}$.

6 Concluding Remarks and Open Problems

We have given a bound on $\deg \mathbf{U}(Z)$ when the input matrix has full row rank. This in turn allows us to reduce the problem of computing the Popov form and the associated unimodular transformation as a left nullspace computation. Thus, nullspace algorithms which control coefficient growth can be applied.

In practice, the bound on $\deg \mathbf{U}(Z)$ may be too pessimistic. Because the complexity of the nullspace algorithms depend on the degree of the input matrix [1, 5, 6], having a bound that is too large will decrease the performance of these algorithms. An alternate approach is suggested in [4] in which (9) is solved with a small starting value of b. The value of b is increased if the matrix $\mathbf{T}(Z)$ obtained from the nullspace is not in Popov form. In the cases where the degree bound on $\mathbf{U}(Z)$ is very pessimistic this will provide a faster algorithm.

Unfortunately we have not obtained a bound on $\deg \mathbf{U}(Z)_{J_c,K_c}$. The main difficulty is that in the case of polynomial matrices, the proofs for bounds on this part of the unimodular multiplier use the notions of inverse, determinants, and adjoints of matrices [3]. These notions are not available to us because the matrix entries are non-commutative. Some proofs also rely on results on matrix fractions. We believe that some of the results can be generalized by studying formal left fractions of Ore polynomials, but there will be difficulties generalizing notions such as determinants and adjoints.

References

[1] B. Beckermann, H. Cheng, and G. Labahn. Fraction-free row reduction of matrices of Ore polynomials. *Journal of Symbolic Computation*, 41(5):513–543, 2006.

[2] B. Beckermann, G. Labahn, and G. Villard. Shifted normal forms of polynomial matrices. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, pages 189–196. ACM, 1999.

[3] B. Beckermann, G. Labahn, and G. Villard. Normal forms of general polynomial matrices. *Journal of Symbolic Computation*, 41(6):708–737, 2006.

[4] Th. G. Beelen, G. J. van den Hurk, and C. Praagman. A new method for computing a column reduced polynomial matrix. *Systems & Control Letters*, 10:217–224, 1988.

[5] H. Cheng. *Algorithms for Normal Forms for Matrices of Polynomials and Ore Polynomials.* PhD thesis, University of Waterloo, 2003.

[6] H. Cheng and G. Labahn. Output-sensitive modular algorithms for row reduction of matrices of Ore polynomials. *Submitted to the Waterloo Workshop on Computer Algebra*, 2006.

[7] M. Giesbrecht, G. Labahn, and Y. Zhang. Computing valuation popov forms. In *Workshop on Computer Algebra Systems and their Applications (CASA'05)*, 2005.

[8] T. Kailath. *Linear Systems*. Prentice-Hall, 1980.

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

[10] Z. Li. A subresultant theory for ore polynomials with applications. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, pages 132–139. ACM, 1998.

[11] Z. Li and I. Nemes. A modular algorithm for computing greatest common right divisors of ore polynomials. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pages 282–289. ACM, 1997.

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

[13] W. H. L. Neven and C. Praagman. Column reduction of polynomial matrices. *Linear Algebra and Its Applications*, 188,189:569–589, 1993.

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