Computing Popov Form of General Ore Polynomial Matrices

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

George Labahn
David R. Cheriton School of Computer Science
University of Waterloo, Canada

Abstract

The computation of the Popov form of Ore polynomial matrices is 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. Fraction-free and modular algorithms for nullspace computation can be used in exact arithmetic setting where coefficient growth is a concern. When specialized to ordinary polynomial matrices, our results simplify the proofs for the computation of Popov form while keeping the same worst case complexity.

1 Introduction

Ore polynomial matrices provide a general setting for describing systems of linear differential, difference and q-difference operators [12]. 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, one may rewrite high-order operators (e.g. derivatives) in terms of lower ones (Example 2.5). Algorithms for computing the Popov form for polynomial matrices are well known [9, 10], but there have been few works on the computation of Popov form for Ore polynomial matrices. The problem was studied in [8] using row reductions, which can introduce significant coefficient growth which must be controlled. This is important for Ore polynomials as coefficient growth is introduced in two ways—from multiplying by powers of the indeterminate and from elimination by cross-multiplication.

Fraction-free and modular algorithms [1, 5] exist to compute a minimal polynomial basis of the left nullspace of Ore polynomial matrices, such that the basis is given by an Ore polynomial matrix in Popov form. 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. The case when the input matrix has full row rank has been examined in a previous work [6, 7]. When the input matrix does not have full row rank, the unimodular multiplier is not unique. Instead, we define a unique minimal multiplier and show the reduction can still be applied by giving a degree bound for the minimal multiplier.

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, 11]. 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. For the special case of ordinary polynomial matrices, we obtain the same worst case complexity as those obtained previously [3] with simpler proofs.

2 Notations and Definitions

We first give some notations and definitions similar to those given in previous works [1].

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.

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 and δ a derivation, so that the multiplication rule holds for all $a \in \mathbb{K}$:

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

Let $\mathbb{K}[Z; \sigma, \delta]^{m \times n}$ be the ring of $m \times n$ Ore polynomial matrices over $\mathbb{K}[Z; \sigma, \delta]$. 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* $\vec{\mu} = \text{rdeg } \mathbf{F}(Z)$ if the ith row has degree μ_i. The *leading row coefficient* of $\mathbf{F}(Z)$, denoted $\text{LC}_{row}(\mathbf{F}(Z))$, 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 $\text{LC}_{row}(\mathbf{F}(Z))$ 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 ith 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 $r = \text{rank } \mathbf{F}(Z)$, 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 $\{\Pi_i \ : \ \Pi_i > 0\}$.*

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].

Theorem 2.3 *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*

$$\textit{rdeg } \mathbf{U}(Z) \le \vec{\nu} + (|\vec{\mu}| - |\vec{\nu}| - \alpha) \cdot \vec{e} \tag{3}$$

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

We also recall the predictable degree property for Ore polynomial matrices [1, Lemma A.1(a)]. This result is used a number of times in our proofs.

Lemma 2.4 (Predictable Degree Property) *Let* $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ *with* $\vec{\mu} = rdeg\,\mathbf{F}(Z)$. *Then* $\mathbf{F}(Z)$ *is row-reduced if and only if, for all* $\mathbf{Q}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{1\times m}$,

$$\deg \mathbf{Q}(Z)\mathbf{F}(Z) = \max_j(\mu_j + \deg \mathbf{Q}(Z)_{1,j}. \tag{4}$$

Example 2.5 *Consider the differential algebraic system*

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

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:*

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

The matrix of operators is in Popov form with row degree $(2,3,4)$ *and pivot set* $\{1,2,3\}$. *Notice that we can now convert every highest derivative into ones of lower order. For example, we can eliminate the highest derivatives of* $y_2(t)$ *as*

$$y_2'''(t) = -y_1'(t) - 3y_1(t) - 2y_2'(t) + y_2(t) - y_3'''(t) + 2t^2y_3(t). \tag{7}$$

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 $\mathbf{U}(Z)\cdot\mathbf{F}(Z) = \mathbf{T}(Z)$, where $\mathbf{T}(Z)$ is in Popov form. The fraction-free and modular algorithms [1, 5] can be used to compute a minimal polynomial basis $\mathbf{M}(Z)$ of the left nullspace of a Ore polynomial matrix such that $\mathbf{M}(Z)$ is in Popov form. Using these algorithms, we compute the left nullspace of the matrix $\begin{bmatrix}\mathbf{F}(Z)\cdot Z^b & -\mathbf{I}_n.\end{bmatrix}^T$. Then the nullspace $\mathbf{M}(Z)$ can be partitioned as $[\mathbf{U}(Z) \;\; \mathbf{T}(Z)\cdot Z^b]$ such that

$$\begin{bmatrix}\mathbf{U}(Z) & \mathbf{T}(Z)\cdot Z^b\end{bmatrix} \cdot \begin{bmatrix}\mathbf{F}(Z)\cdot Z^b \\ -\mathbf{I}_n\end{bmatrix} = \mathbf{0}. \tag{8}$$

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. 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 $\mathbf{V}(Z)\cdot\mathbf{U}(Z) = \mathbf{I}_m$. Thus, $\mathbf{U}(Z)$ has a left inverse. Now, $\mathbf{U}(Z)\cdot\mathbf{V}(Z)\cdot\mathbf{U}(Z) = \mathbf{U}(Z)$. Therefore,

$$(\mathbf{U}(Z)\cdot\mathbf{V}(Z) - \mathbf{I}_m)\cdot\mathbf{U}(Z) = \mathbf{0}. \tag{9}$$

Since $m = \text{rank}\,\mathbf{I}_m = \text{rank}\,(\mathbf{V}(Z)\cdot\mathbf{U}(Z)) \le \text{rank}\,\mathbf{U}(Z) \le m$, $\mathbf{U}(Z)$ has full row rank. Thus, (9) 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. □

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, 11].

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 $\deg \mathbf{U}(Z)$. We first prove some results which relate the degrees of the input matrix $\mathbf{F}(Z)$, the unimodular multiplier $\mathbf{U}(Z)$, and any matrix $\mathbf{T}(Z)$ resulting from the row transformation specified by $\mathbf{U}(Z)$.

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 $\vec{\gamma} = \text{rdeg}\ \mathbf{T}_2(Z)$. 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 $\vec{\nu} = \text{rdeg}\ \mathbf{T}_1(Z)$.*

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, Lemma 2.4 gives

$$\deg \mathbf{V}(Z)_{i,j} + \deg \mathbf{T}_1(Z)_{j,\cdot} \le \deg \mathbf{T}_2(Z)_{i,\cdot}, \tag{10}$$

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 $\vec{\gamma} = \text{rdeg}\ \mathbf{T}(Z)$. There exists a unimodular matrix $\mathbf{U}(Z)$ such that $\mathbf{U}(Z)\cdot\mathbf{F}(Z) = \mathbf{T}(Z)$ and rdeg $\mathbf{U}(Z) \le \vec{\gamma} + (|\vec{\mu}| - \alpha)\cdot\vec{e}$, where $\vec{\mu} = \text{rdeg}\ \mathbf{F}(Z)$ and $\alpha = \min_j\{\mu_j\}$.*

Proof. By [1, Theorem 2.2], 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 rdeg $\mathbf{U}_1(Z) \le \vec{\nu} + (|\vec{\mu}| - |\vec{\nu}| - \alpha)\cdot\vec{e}$, 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

$$\deg \mathbf{U}(Z)_{i,j} \le \max_{1\le k\le m} \deg \mathbf{U}_2(Z)_{i,k} + \deg \mathbf{U}_1(Z)_{k,j} \le \max_{1\le k\le m} (\gamma_i - \nu_k) + (\nu_k + |\vec{\mu}| - |\vec{\nu}| - \alpha) \le \gamma_i + |\vec{\mu}| - \alpha.$$

□

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 $\mathbf{U}(Z)\cdot\mathbf{F}(Z) = \mathbf{T}(Z)$ is unique (if it exists).*

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

$$\mathbf{U}_1(Z)\cdot\mathbf{F}(Z) = \mathbf{T}(Z) = \mathbf{U}_2(Z)\cdot\mathbf{F}(Z). \tag{11}$$

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 by Theorem 4.2 and Lemma 4.3.

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 (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 $\begin{bmatrix}\mathbf{F}(Z)\cdot Z^b & -\mathbf{I}_n\end{bmatrix}^T$. 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 $\operatorname{rdeg}\mathbf{U}(Z) \le \vec{\nu} + (|\vec{\mu}| - \alpha)\cdot\vec{e}$ where $\vec{\mu} = \operatorname{rdeg}\mathbf{F}(Z)$, $\vec{\nu} = \operatorname{rdeg}\mathbf{T}(Z)$, and $\alpha = \min_j\{\mu_j\}$. Therefore, $\operatorname{rdeg}\mathbf{U}(Z) \le \operatorname{rdeg}\mathbf{R}(Z) + (|\vec{\mu}| - \alpha - b)\cdot\vec{e} < \operatorname{rdeg}\mathbf{R}(Z)$. 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. □

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. Suppose $\mathbf{T}(Z) = \begin{bmatrix}\mathbf{0} & \mathbf{T}(Z)_{J_c,*}\end{bmatrix}^T = \mathbf{U}(Z)\cdot\mathbf{F}(Z)$ is the Popov form of $\mathbf{F}(Z)$. 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 fact, all unimodular multipliers satisfying $\mathbf{T}(Z) = \mathbf{U}(Z)\cdot\mathbf{F}(Z)$ are related, and there is a unique multiplier that has minimal column degrees and is normalized in some way. We first give a result related to "division" of Ore polynomial matrices. This allows us 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*

$$\mathbf{A}(Z) - \mathbf{Q}(Z)\cdot\mathbf{B}(Z) = \mathbf{R}(Z), \tag{12}$$

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

Proof. It suffices to prove this in the case $m = 1$ as we may consider each row of (12) independently.

We first show the existence of $\mathbf{Q}(Z)$ and $\mathbf{R}(Z)$. Let $K = \{k : \deg\mathbf{A}(Z)_{1,k} \ge \beta_k\}$, and $d = \deg\mathbf{A}(Z)_{1,K}$. Let $t \in K$ be the pivot index of $\mathbf{A}(Z)_{1,K}$. Thus, $\mathbf{A}(Z)_{1,t} = aZ^d + \cdots$ for some $a \in \mathbb{K}$. If $\mathbf{B}(Z)_{t,t} = bZ^{\beta_t} + \cdots$ for some $b \in \mathbb{K}$. Let $\hat{\mathbf{R}}_{\mathbf{1}}(Z) = \mathbf{A}(Z) - \hat{\mathbf{Q}}_{\mathbf{1}}(Z)\cdot\mathbf{B}(Z)$ 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,

$$\deg\mathbf{B}(Z)_{t,s} \le \begin{cases}\beta_t & \text{if } s \ge t,\\ \beta_t - 1 & \text{otherwise.}\end{cases} \tag{13}$$

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

$$\deg\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} \le \begin{cases}d & \text{if } s > t,\\ d-1 & \text{otherwise.}\end{cases} \tag{14}$$

For $s \notin K$, we have $\deg\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} \le \max(\deg\mathbf{A}(Z)_{1,s}, \deg[\hat{\mathbf{Q}}_{\mathbf{1}}(Z)\cdot\mathbf{B}(Z)]_{1,s})$. If $\deg\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} \le \deg\mathbf{A}(Z)_{1,s}$, then $\deg\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} < \beta_s$ by definition of K. Otherwise,

$$\deg\hat{\mathbf{R}}_{\mathbf{1}}(Z)_{1,s} = \deg[\hat{\mathbf{Q}}_{\mathbf{1}}(Z)\cdot\mathbf{B}(Z)]_{1,s} \le \begin{cases}(d-\beta_t)+\beta_t = d & \text{if } s > t,\\ (d-\beta_t)+\beta_t - 1 = d-1 & \text{otherwise.}\end{cases} \tag{15}$$

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 $\hat{\mathbf{R}}_{\mathbf{k}}(Z) = \mathbf{A}(Z) - \left[\hat{\mathbf{Q}}_{\mathbf{1}}(Z) + \cdots + \hat{\mathbf{Q}}_{\mathbf{k}}(Z)\right] \cdot \mathbf{B}(Z)$, 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 (12).

To show uniqueness, suppose that we have $\mathbf{A}(Z)_{1,*} = \mathbf{Q}_{\mathbf{1}}(Z) \cdot \mathbf{B}(Z) + \mathbf{R}_{\mathbf{1}}(Z) = \mathbf{Q}_{\mathbf{2}}(Z) \cdot \mathbf{B}(Z) + \mathbf{R}_{\mathbf{2}}(Z)$ 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 $\hat{\mathbf{R}}(Z) = \hat{\mathbf{Q}}(Z) \cdot \mathbf{B}(Z)$ 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, Lemma 2.4 implies that $\deg \hat{\mathbf{Q}}(\mathbf{Z})_{1,k} \leq \deg \hat{\mathbf{R}}(Z)_{1,k} - \beta_k < 0$, 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 $\hat{\mathbf{R}}(Z)_{1,K} = \hat{\mathbf{Q}}(Z)_{1,K} \cdot \mathbf{B}(Z)_{K,K}$. 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 (12) 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

$$\deg(\mathbf{Q}(Z)_{i,L_i} \cdot \mathbf{B}(Z)_{L_i,L_i}) = \deg(\mathbf{A}(Z)_{i,L_i} - \mathbf{R}(Z)_{i,L_i}) \leq \gamma_i. \tag{16}$$

Lemma 2.4 gives $\deg(\mathbf{Q}(Z)_{i,L_i} \cdot \mathbf{B}(Z)_{L_i,L_i}) \geq \deg \mathbf{Q}(Z)_{i,j} + \beta_j$, 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

$$\mathbf{W}(Z) = \begin{bmatrix} \mathbf{W}(Z)_{J,J} & 0 \\ \mathbf{W}(Z)_{J_c,J} & \mathbf{I}_r \end{bmatrix}, \tag{17}$$

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

$$\deg \mathbf{U}(Z)_{j,k} < \max_{\ell \in J} \deg \mathbf{U}(Z)_{\ell,k} \tag{18}$$

(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 $\mathbf{U}_{\mathbf{1}}(Z)$ and $\mathbf{U}_{\mathbf{2}}(Z)$ be two such unimodular multipliers for the Popov form of $\mathbf{F}(Z)$. Then $\mathbf{U}_{\mathbf{1}}(Z)_{J,*}, \mathbf{U}_{\mathbf{2}}(Z)_{J,*}$, are bases of the left nullspace of $\mathbf{F}(Z)$. Thus there exists a unimodular multiplier $\mathbf{W}(Z)_{J,J}$ such that $\mathbf{U}_{\mathbf{1}}(Z)_{J,*} = \mathbf{W}(Z)_{J,J}\mathbf{U}_{\mathbf{2}}(Z)_{J,*}$. By the uniqueness of $\mathbf{T}(Z)_{J_c,*}$, the rows of $\mathbf{U}_{\mathbf{2}}(Z)_{J_c,*} - \mathbf{U}_{\mathbf{1}}(Z)_{J_c,*}$ are in the nullspace of $\mathbf{F}(Z)$, so there exists a matrix $\mathbf{W}(Z)_{J_c,J}$ such that $\mathbf{U}_{\mathbf{2}}(Z)_{J_c,*} = \mathbf{U}_{\mathbf{1}}(Z)_{J_c,*} + \mathbf{W}(Z)_{J_c,J}\mathbf{U}_{\mathbf{1}}(Z)_{J,*}$.

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 $\mathbf{U}_{\mathbf{0}}(Z)$ we may divide $\mathbf{U}_{\mathbf{0}}(Z)_{J_c,K}$ on the right by $\mathbf{U}(Z)_{J,K}$ to get $\mathbf{U}_{\mathbf{0}}(Z)_{J_c,K} = \mathbf{W}(Z)_{J_c,J}\mathbf{U}(Z)_{J,K} + \mathbf{U}(Z)_{J_c,K}$. By Lemma 5.1, (18) is satisfied. Since $\mathbf{U}(Z)_{J_c,K}$ is the unique matrix such that (18) is satisfied, the generic form of a multiplier given in (a) implies that $\mathbf{U}(Z)_{J_c,*} = \mathbf{U}_{\mathbf{0}}(Z)_{J_c,*} - \mathbf{W}(Z)_{J_c,J}\mathbf{U}(Z)_{J,*}$. Thus, the minimal multiplier $\mathbf{U}(Z)$ is well defined and unique.

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 $|\text{rdeg } \mathbf{U_0}(Z)_{J_c,*}| \geq |\text{rdeg } \mathbf{U}(Z)_{J_c,*}|$. 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 $\mathbf{U}(Z)_{J_c,*} = \mathbf{U_0}(Z)_{J_c,*} - \mathbf{W}(Z)_{J_c,J}\mathbf{U}(Z)_{J,*}$ with $\deg \mathbf{W}(Z)_{i,j} \leq \mu_i - \beta_j$. Therefore we have, for $1 \leq i \leq m$ and $j \in J_c$, $\deg \mathbf{U}(Z)_{i,j} \leq \max(\max(\mu_i, \gamma_i), \mu_i) = \max(\mu_i, \gamma_i)$. 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*.

Theorem 5.3 *Let $\mathbf{U}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times m}$ be the minimal multiplier for $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$ as in Theorem 5.2, and $\vec{\mu} = rdeg\ \mathbf{F}(Z)$. Then*

$$\deg \mathbf{U}(Z) \leq |\vec{\mu}| - \min_j\{\mu_j\}. \tag{19}$$

Proof. Let $\mathbf{T}(Z)$, J, and K be defined as in Theorem 5.2. We first note that if $\vec{\beta}$ is the row degree of the minimal polynomial basis, we have

$$\deg \mathbf{U}(Z)_{j,k} \leq \begin{cases} \beta_j & \text{if } j \in J, \\ \beta_j - 1 & \text{if } j \in J_c \text{ and } k \in K. \end{cases} \tag{20}$$

Since $\beta_i \leq |\vec{\mu}| - \min_j\{\mu_j\}$, it remains to obtain a bound for $\deg \mathbf{U}(Z)_{J_c,K_c}$.

Let $\mathbf{V}(Z) = \mathbf{U}(Z)^{-1}$ with row degree $\vec{\gamma}$. Then we have $\mathbf{F}(Z) = \mathbf{V}(Z)\cdot\mathbf{T}(Z)$, or $\mathbf{F}(Z) = \mathbf{V}(Z)_{*,J_c}\cdot\mathbf{T}(Z)_{J_c,*}$ because $\mathbf{T}(Z)_{J,*} = \mathbf{0}$. We wish to obtain a degree bound for $\mathbf{V}(Z)$ and relate it to $\deg \mathbf{U}(Z)$.

Since $\mathbf{T}(Z)_{J_c,*}$ is in Popov form and hence row-reduced, Lemma 2.4 gives a degree bound on $\mathbf{V}(Z)_{*,J_c}$: $\deg \mathbf{V}(Z)_{i,j} \leq \mu_i - \gamma_j \leq \mu_i$ for all $1 \leq i \leq m$, $j \in J_c$.

Let $r = \text{rank } \mathbf{F}(Z)$. Since $\mathbf{V}(Z)\cdot\mathbf{U}(Z) = \mathbf{I}$, we have

$$\mathbf{I}_{m-r} - \mathbf{V}(Z)_{K,J_c}\cdot\mathbf{U}(Z)_{J_c,K} = \mathbf{V}(Z)_{K,J}\cdot\mathbf{U}(Z)_{J,K} \tag{21}$$

$$-\mathbf{V}(Z)_{K_c,J_c}\cdot\mathbf{U}(Z)_{J_c,K} = \mathbf{V}(Z)_{K_c,J}\cdot\mathbf{U}(Z)_{J,K}. \tag{22}$$

In each of the above equations, the degree bound of row i on the left-hand side is at most $\mu_i + |\vec{\mu}| - \min_j\{\mu_j\}$. On the right-hand side, $\mathbf{U}(Z)_{J,K}$ is in Popov form and hence row-reduced. Lemma 2.4 again gives

$$\mu_i + |\vec{\mu}| - \min_j\{\mu_j\} \geq \deg \mathbf{V}(Z)_{i,j} + |\vec{\mu}| - \min_j\{\mu_j\}, \tag{23}$$

or

$$\mathbf{V}(Z)_{i,j} \leq \mu_i \tag{24}$$

for all $1 \leq i \leq m$ and $j \in J$. Combining with the above, we see that $\text{rdeg } \mathbf{V}(Z) \leq \vec{\mu}$.

To obtain a degree bound for $\mathbf{U}(Z)$, we observe that the row-reduced form of $\mathbf{V}(Z)$ is the identity matrix and $\mathbf{U}(Z)$ is the unique unimodular transformation matrix for $\mathbf{V}(Z)$. Applying [1, Theorem 2.2]

$$\text{rdeg } \mathbf{U}(Z) \leq (|\vec{\mu}| - \min_j\{\mu_j\})\cdot\vec{e}, \tag{25}$$

and the theorem follows. □

Remark 5.4 *The degree bound obtained this way is not as accurate as the one in the commutative case in [3]. However, our proofs are simpler and our bounds are not worse than those obtained in [3, Corollary 5.5] in the worst case when the rank of the input matrix is not known in advance.*

Thus, the same value of b is sufficient even when the input matrix does not have full row rank. In particular, we do not need to know the rank of the input matrix in advance.

Theorem 5.5 *Theorem 4.5 is true for any $\mathbf{F}(Z) \in \mathbb{K}[Z;\sigma,\delta]^{m\times n}$.*

6 Conclusion

We have given a bound on the minimal multiplier, which 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 the minimal multiplier may be too pessimistic. Because the complexity of the nullspace algorithms depend on the degree of the input matrix [1, 5], having a bound that is too large will decrease the performance of these algorithms. An alternate approach is suggested in [4] in which (8) 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 the minimal multiplier is very pessimistic this will provide a faster algorithm.

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 and G. Labahn. Output-sensitive modular algorithms for row reduction of matrices of Ore polynomials. *Computer Algebra 2006: Latest Advances in Symbolic Algorithms*, pages 43–66, 2007.

[6] P. Davies and H. Cheng. Computing popov form of Ore polynomial matrices. Technical report, Department of Mathematics and Computer Science, University of Lethbridge, Sep 2006.

[7] P. Davies, H. Cheng, and G. Labahn. Computing Popov form of Ore polynomial matrices. *Communications in Computer Algebra, ISSAC 2007 Poster Abstracts*, 41(2):49–50, 2007.

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

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

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

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

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