Unimodular Completion of Polynomial Matrices

Wei Zhou and George Labahn
Cheriton School of Computer Science
University of Waterloo,
Waterloo, Ontario, Canada
{w2zhou,glabahn}@uwaterloo.ca

ABSTRACT

Given a rectangular matrix $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$ with $m < n$ of univariate polynomials over a field $\mathbb{K}$ we give an efficient algorithm for computing a unimodular completion of $\mathbf{F}$. Our algorithm is deterministic and computes such a completion, when it exists, with cost $O^{\sim}(n^{\omega} s)$ field operations from $\mathbb{K}$. Here s is the average of the m largest column degrees of $\mathbf{F}$ and ω is the exponent on the cost of matrix multiplication. Here $O^{\sim}$ is big-O but with log factors removed. If a unimodular completion does not exist for $\mathbf{F}$, our algorithm computes a unimodular completion for a right cofactor of a column basis of $\mathbf{F}$, or equivalently, computes a completion that preserves the generalized determinant.

Categories and Subject Descriptors: I.1.2 [Symbolic and Algebraic Manipulation]: Algorithms; F.2.2 [Analysis of Algorithms and Problem Complexity]: Nonnumerical Algorithms and Problems

General Terms: Algorithms, Theory

Keywords: Order Basis, Minimal Kernel Basis, Unimodular Matrices, Unimodular Completion

1. INTRODUCTION

Let $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$ with $m < n$ be a full-rank rectangular matrix. We consider the unimodular completion problem of finding a second rectangular matrix $\mathbf{G} \in \mathbb{K}[x]^{(n-m)\times n}$ such that $\begin{bmatrix} \mathbf{F} \\ \mathbf{G} \end{bmatrix}$ is unimodular. Here a square matrix of univariate polynomials is unimodular if its determinant is a nonzero constant (and so also has an inverse consisting of polynomials). In fact, we consider the more general problem of finding $\mathbf{G} \in \mathbb{K}[x]^{(n-m)\times n}$ such that the $\mathbf{F}$ and $\begin{bmatrix} \mathbf{F} \\ \mathbf{G} \end{bmatrix}$ have the same *generalized determinant*. Here the generalized determinant denotes the product of the nonzero diagonal elements of its Smith form. The standard unimodular completion problem is then the special case where the generalized determinant of $\mathbf{F}$ is 1.

ISSAC'14, July 23–25, 2014, Kobe, Japan.

In general unimodular completion is a useful basic operation in many matrix computations [10]. For example, in the case of a single row (i.e. $m = 1$) unimodular completion plays a key role in proofs for Hermite and Smith normal forms. In the case of rectangular matrices of multivariate polynomials, the problem has more storied history because of its role in solving Serre's conjecture that projective modules over polynomial rings are free [8]. Serre's conjecture was proved independently by Quillen and Suslin in 1976 using unimodular completion [12]. Later on their nonconstructive methods were replaced by constructive methods, for example that of Logar and Sturmfels [9]. Unimodular completion also appears in non commutative domains, specifically where their use includes the reduction of mathematical systems to ones having fewer functions and parameters [5]. Additional applications in multidimensional systems theory, including a description of a Maple package which implements the Quillen-Suslin theorem, can be found in [6].

Unimodular completions do not exist for all rectangular matrices. For example, the matrix $[0, x]$ cannot be completed to a 2×2 unimodular matrix. In the case where $\mathbf{F}$ is a single row, a unimodular completion exists if and only if all the entries in $\mathbf{F}$ are relatively prime [10]. More generally we can show that a unimodular completion of $\mathbf{F}$ exists if and only if there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{F} \cdot \mathbf{U} = [I_m, 0]$. For simplicity and without loss of generality, we focus our discussion on the situation where the unimodular completion always exists. For an input matrix that cannot be completed to a unimodular matrices, we can always factor it as $\mathbf{F} = \mathbf{T}\mathbf{G}$ using the column basis algorithm from [15], something which can be done efficiently. Then the right factor $\mathbf{G}$ can be unimodularly completed. However, an even simpler way is to apply our algorithm directly on the input matrix, as the algorithm works effectively on any input matrix to compute a completion that preserves the generalized determinant.

The algorithm we present in this paper has a cost of $O^{\sim}(n^{\omega} s)$ field operations, where s is the average of the m largest column degrees of $\mathbf{F}$. Our approach is to embed our matrix into an *order basis* problem [1]. We take advantage of the fact that order bases are closely related to unimodular matrices when one reverses the order of column coefficients. More precisely, we first reverse coefficients of $\mathbf{F}$, then compute a kernel basis $\mathbf{M}$ of this new object, and a left order basis $\mathbf{Q}$ of $\mathbf{M}$. Reversing coefficients in $\mathbf{Q}$ then gives a unimodular completion of $\mathbf{F}$. A major challenge lies in determining the right shifts and orders so that the pieces both fit together and give a low complexity.

2. PRELIMINARIES

In this section we give the basic cost model, notations, and the basic definitions and properties of *shifted degree*, *kernel basis*, *column basis,* and *order basis* which are needed for our discussion and algorithm.

2.1 Cost model

Algorithms are analyzed by bounding the number of arithmetic operations in the coefficient field $\mathbb{K}$ on an algebraic random access machine. We will frequently use the fact that the cost of multiplying two polynomial matrices with dimension n and degree bounded by d is $O^{\sim}(n^{\omega}d)$ field operations from $\mathbb{K}$, where ω is the exponent of matrix multiplication. We refer to the book by [11] for more details and references about polynomial and matrix multiplication.

2.2 Notations

For convenience we adopt the following notations in this paper.

Comparing Unordered Lists For two lists $\vec{a} \in \mathbb{Z}^n$ and $\vec{b} \in \mathbb{Z}^n$, let $\bar{a} = [\bar{a}_1, \ldots, \bar{a}_n] \in \mathbb{Z}^n$ and $\bar{b} = [\bar{b}_1, \ldots, \bar{b}_n] \in \mathbb{Z}^n$ be the lists consists of the entries of $\vec{a}$ and $\vec{b}$ but sorted in increasing order.

$$\begin{cases} \vec{a} \geq \vec{b} & \text{if } \bar{a}_i \geq \bar{b}_i \text{ for all } i \in [1, \ldots, n] \\ \vec{a} \leq \vec{b} & \text{if } \bar{a}_i \leq \bar{b}_i \text{ for all } i \in [1, \ldots, n] \\ \vec{a} > \vec{b} & \text{if } \vec{a} \geq \vec{b} \text{ but } \bar{a}_j \neq \bar{b}_j \\ \vec{a} < \vec{b} & \text{if } \vec{a} \leq \vec{b} \text{ but } \bar{a}_j \neq \bar{b}_j \end{cases}$$

Uniform Shift of a List For a list $\vec{a} = [a_1, \ldots, a_n] \in \mathbb{Z}^n$ and $c \in \mathbb{Z}$, we write $\vec{a} + c$ to denote $\vec{a} + [c, \ldots, c] = [a_1 + c, \ldots, a_n + c]$, with subtraction handled similarly.

Compare a List with an Integer For $\vec{a} = [a_1, \ldots, a_n] \in \mathbb{Z}^n$ and $c \in \mathbb{Z}$, we write $\vec{a} < c$ to denote $\vec{a} < [c, \ldots, c]$, and similarly for $>, \leq, \geq, =$.

2.3 Shifted degrees

Our methods depend extensively on the concept of *shifted* degrees of polynomial matrices [3]. For a column vector $\mathbf{p} = [p_1, \ldots, p_n]^T$ of univariate polynomials over a field $\mathbb{K}$, its column degree, denoted by $\operatorname{cdeg} \mathbf{p}$, is the maximum of the degrees of the entries of $\mathbf{p}$, that is,

$$\operatorname{cdeg} \mathbf{p} = \max_{1 \leq i \leq n} \deg p_i.$$

The *shifted column degree* generalizes this standard column degree by taking the maximum after shifting the degrees by a given integer vector that is known as a *shift.* More specifically, the shifted column degree of $\mathbf{p}$ with respect to a shift $\vec{s} = [s_1, \ldots, s_n] \in \mathbb{Z}^n$, or the *$\vec{s}$-column degree* of $\mathbf{p}$ is

$$\operatorname{cdeg}_{\vec{s}} \mathbf{p} = \max_{1 \leq i \leq n} [\deg p_i + s_i] = \operatorname{cdeg} (x^{\vec{s}} \cdot \mathbf{p}),$$

where

$$x^{\vec{s}} = \operatorname{diag} \left(x^{s_1}, x^{s_2}, \ldots, x^{s_n} \right).$$

For a matrix $\mathbf{P}$, we use $\operatorname{cdeg} \mathbf{P}$ and $\operatorname{cdeg}_{\vec{s}} \mathbf{P}$ to denote respectively the list of its column degrees and the list of its shifted $\vec{s}$-column degrees. When $\vec{s} = [0, \ldots, 0]$, the shifted column degree specializes to the standard column degree. The shifted row degree is defined in a similar way.

Shifted degrees have been used previously in polynomial matrix computations and in generalizations of some matrix normal forms [4]. The shifted column degree is equivalent to the notion of *defect* commonly used in the literature.

Along with shifted degrees we also make use of the notion of a polynomial matrix being column reduced. A polynomial matrix $\mathbf{A} \in \mathbb{K}[x]^{m \times n}$ is column reduced if the leading column coefficient matrix, that is the matrix

$$\operatorname{lcoeff}_{\vec{d}} \mathbf{A} = [\operatorname{coeff}(a_{ij}, x, d_j)]_{1 \leq i \leq m, 1 \leq j \leq n}, \text{ with } \vec{d} = \operatorname{cdeg} \mathbf{A},$$

has full rank. A polynomial matrix $\mathbf{A}$ is $\vec{s}$-column reduced if $x^{\vec{s}} \cdot \mathbf{A}$ is column reduced.

The usefulness of the shifted degrees can be seen from their applications in polynomial matrix computation problems [13, 14, 16]. One of its uses is illustrated by the following lemma, which follows directly from the definition of shifted degree.

LEMMA 2.1. *If the $\vec{u}$-column degrees of $\mathbf{A} \in \mathbb{K}[x]^{m \times n}$ are bounded by the corresponding entries of an integer list $\vec{v} \in \mathbb{Z}^n$, (or equivalently, the $-\vec{v}$-row degrees of $\mathbf{A}$ are bounded by $-\vec{u}$) and the $\vec{v}$-column degrees of $\mathbf{B} \in \mathbb{K}[x]^{n \times k}$ are bounded by $\vec{w} \in \mathbb{Z}^k$, then the $\vec{u}$-column degrees of $\mathbf{AB}$ are bounded by $\vec{w}$.*

An essential subroutine needed in our algorithm, also based on the use of the shifted degrees, is the efficient multiplication of a pair of matrices $\mathbf{A} \cdot \mathbf{B}$ with unbalanced degrees [13, Theorem 5.6]. The notation $\sum \vec{s}$, for any list $\vec{s}$, denotes the sum of all entries in $\vec{s}$.

THEOREM 2.2. *Let $\mathbf{A} \in \mathbb{K}[x]^{m \times n}$ with $m \leq n$, $\vec{s} \in \mathbb{Z}^n$ a shift with entries bounding the column degrees of $\mathbf{A}$ and $\check{\xi}$, a bound on the sum of the entries of $\vec{s}$. Let $\mathbf{B} \in \mathbb{K}[x]^{n \times k}$ with $k \in O(m)$ and the sum θ of its $\vec{s}$-column degrees satisfying $\theta \in O(\check{\xi})$. Then we can multiply $\mathbf{A}$ and $\mathbf{B}$ with a cost of $O^{\sim}(n^{\omega} t)$, where $t = \check{\xi}/n$.*

2.4 Kernel bases and column bases

Let $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ be a matrix of polynomials over a field $\mathbb{K}$. The kernel of $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ is the $\mathbb{K}[x]$-module

$$\{\mathbf{p} \in \mathbb{K}[x]^n \mid \mathbf{F} \cdot \mathbf{p} = 0\}$$

with a kernel basis of $\mathbf{F}$ being a basis of this module.

DEFINITION 2.3. *Given $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$, a polynomial matrix $\mathbf{N} \in \mathbb{K}[x]^{n \times *}$ is a $\vec{s}$-minimal (right) kernel basis of $\mathbf{F}$ if $\mathbf{N}$ is a kernel basis of $\mathbf{F}$ and $\mathbf{N}$ is $\vec{s}$-column reduced. We also call a $\vec{s}$-minimal (right) kernel basis of $\mathbf{F}$ a $(\mathbf{F}, \vec{s})$-kernel basis.*

In this paper we require two essential properties of shifted minimal kernel bases : a bound on the size of the minimal kernel and the cost of computing such a minimal kernel. Both results come from [16].

THEOREM 2.4. *Suppose $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ and $\vec{s} \in \mathbb{Z}^n_{\geq 0}$ is a shift with entries bounding the corresponding column degrees of $\mathbf{F}$. Then the sum of the $\vec{s}$-column degrees of any $\vec{s}$-minimal kernel basis of $\mathbf{F}$ is bounded by $\xi = \sum \vec{s}$.*

THEOREM 2.5. *Let $\mathbf{F} \in \mathbb{K}^{m \times n}$ and $\vec{s}$ be a shift bounding the corresponding column degrees of $\mathbf{F}$. Then a $\vec{s}$-minimal kernel basis of $\mathbf{F}$ can be computed in $O^{\sim}(n^{\omega} s)$ field operations from $\mathbb{K}$, where s is the average of the m largest column degrees of $\mathbf{F}$.*

A column basis of $\mathbf{F}$ is a basis for the $\mathbb{K}[x]$-module

$$\{\mathbf{F}\mathbf{p} \mid \mathbf{p} \in \mathbb{K}[x]^n\ \}\ .$$

Such a basis can be represented as a full rank matrix $\mathbf{T} \in \mathbb{K}[x]^{m\times r}$ whose columns are the basis elements. Equivalently, there exists a unimodular matrix $\mathbf{U}$ that transforms the matrix $\mathbf{F}$ to $\mathbf{FU} = [\mathbf{T}, 0]$ with a full rank matrix $\mathbf{T}$ defined as a column basis of $\mathbf{F}$.

The cost of column basis computation for $\mathbf{F} \in \mathbb{K}[z]^{m\times n}$ is given in [15] with the cost given as $\mathcal{O}^{\sim}\left(nm^{\omega-1}\hat{s}\right)$ field operations in $\mathbb{K}$, where $\hat{s}$ is the average column degree of $\mathbf{F}$.

2.5 Order bases

Let $\mathbb{K}$ be a field, $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$ a matrix of polynomials and $\vec{\sigma}$ a list non-negative integer.

Definition 2.6. *A vector of polynomials $\mathbf{p} \in \mathbb{K}[x]^{n\times 1}$ has* order $(\mathbf{F}, \vec{\sigma})$ *(or* order $\vec{\sigma}$ *with respect to $\mathbf{F}$) if $\mathbf{F}\cdot\mathbf{p} \equiv \mathbf{0}$ mod $x^{\vec{\sigma}}$, that is,*

$$\mathbf{F}\cdot\mathbf{p} = x^{\vec{\sigma}}\mathbf{r}$$

for some $\mathbf{r} \in \mathbb{K}[x]^{m\times 1}$.

The set of all order $(\mathbf{F}, \vec{\sigma})$ vectors is a $\mathbb{K}[x]$-module denoted by $\langle(\mathbf{F}, \vec{\sigma})\rangle$.

Note that the matrix $\mathbf{F}$ can also be a matrix of power series [1], but restricting it to matrix of polynomials is sufficient for our purpose in this paper. Also note that the order $\vec{\sigma}$ may not be uniform.

An *order basis* $\mathbf{P}$ of $\mathbf{F}$ with order $\vec{\sigma}$ and shift $\vec{s}$, or an $(\mathbf{F}, \vec{\sigma}, \vec{s})$-order basis, or simply an $(\mathbf{F}, \vec{\sigma}, \vec{s})$-basis, is a polynomial matrix whose columns form a basis for the module $\langle(\mathbf{F}, \vec{\sigma})\rangle$ having minimal $\vec{s}$-column degrees [1, 2]. Again, note that a $\vec{s}$-column reduced basis of $\langle(\mathbf{F}, \vec{\sigma})\rangle$ has the minimal $\vec{s}$-column degrees among all bases of $\langle(\mathbf{F}, \vec{\sigma})\rangle$.

We will compute order bases with unbalanced shift using Algorithm 2 from [14] with the following cost.

Theorem 2.7. *For an input matrix $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$, if the shift $\vec{s}$ satisfies $\vec{s} \geq 0$ and $\sum \vec{s} \in O(m\sigma)$, then a $(\mathbf{F}, \sigma, -\vec{s})$-basis can be computed with a cost of $O^{\sim}(n^{\omega}a)$ field operations, where $a = m\sigma/n$.*

We will need a special case of Theorem 5.1 in [2] which for completeness is stated below.

Theorem 2.8. *For a matrix $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$, an order vector $\vec{\sigma}$, and a shift vector $\vec{s}$, if $\mathbf{P}$ is a $(\mathbf{F}, \vec{\sigma}, \vec{s})$-basis with $\vec{s}$-column degrees $\vec{t}$, and $\mathbf{Q}$ is a $(\mathbf{FP}, \vec{\tau}, \vec{t})$ -basis with $\vec{t}$-column degrees $\vec{u}$, where $\vec{\tau} \geq \vec{\sigma}$ component-wise, then $\mathbf{PQ}$ is a $(\mathbf{F}, \vec{\tau}, \vec{s})$-basis with $\vec{s}$-column degrees $\vec{u}$.*

In this paper we also will need the following lemma from [15, 13] which shows that a left kernel basis of a right kernel basis is contained in an order basis of a right kernel basis.

Lemma 2.9. *For a matrix $\mathbf{A} \in \mathbb{K}[x]^{m\times n}$, and a shift vector $\vec{s}$, if $\mathbf{N}$ is a $(\mathbf{A}, \vec{s})$-kernel basis with $\operatorname{cdeg}_{\vec{s}}\mathbf{N} = \vec{b}$ and $\mathbf{P}$ be a $\left(\mathbf{N}^T, \vec{b}+1, -\vec{s}\right)$-basis. Partition $\mathbf{P} = [\mathbf{P}_1, \mathbf{P}_2]$ where $\mathbf{P}_1$ consists of all columns $\mathbf{p}$ with $\operatorname{cdeg}_{-\vec{s}}\mathbf{p} \leq 0$. Then $\mathbf{P}_1$ is a $(\mathbf{N}^T, -\vec{s})$-kernel basis.*

We remark that the condition $\operatorname{cdeg}_{-\vec{s}}\mathbf{p} \leq 0$ is the same as specifying $\deg p_i \leq s_i$ for all i.

2.6 The existence of unimodular completion

We know that row vectors whose entries are relatively prime can be completed to unimodular matrices. We also have a more general criterion on the existence of unimodular completion for matrices.

Lemma 2.10. *A unimodular completion of $\mathbf{F}$ exists if and only if $\mathbf{F}$ has unimodular column bases.*

Proof. If $\mathbf{F}$ has a non-unimodular column basis $\mathbf{A}$, then $\operatorname{diag}([\mathbf{A}, I])$ is always a factor of $\begin{bmatrix}\mathbf{F}\\ \mathbf{B}\end{bmatrix}$ for any polynomial matrix $\mathbf{B}$, implying that the matrix $\begin{bmatrix}\mathbf{F}\\ \mathbf{B}\end{bmatrix}$ is non-unimodular. On the other hand, if $\mathbf{F}$ has a unimodular column basis, then recall that there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{FU} = [I_m, 0]$, where I_m is a column basis of $\mathbf{F}$. This gives $\mathbf{F} = [I_m, 0]\,\mathbf{U}^{-1}$ after rearranging, that is, $\mathbf{F}$ must be consists of the top m rows of $\mathbf{U}^{-1}$. The matrix $\mathbf{U}^{-1}$ is therefore a unimodular completion of the matrix $\mathbf{F}$. $\square$

The proof of Lemma 2.10 shows that a unimodular completion of $\mathbf{F}$ can be obtained from the unimodular matrix $\mathbf{U}$ that transforms $\mathbf{F}$ to its column bases. However, we may not be able to compute this $\mathbf{U}$ efficiently since its degree might be too large. More specifically, $\mathbf{U}$ contains a kernel basis of $\mathbf{F}$ that may have degree $\xi = \sum \vec{s}$, while each of the remaining columns of $\mathbf{U}$ may also have degree ξ.

3. REVERSING OPERATIONS

Our procedure relies heavily on operations that reverse the order of coefficients of polynomial matrices. Reverse operations have been used in the past for computing matrix normal forms using order basis computations. Here we extend the reverse operations to work with shifted degrees. We show how reverse operations can be applied systematically to polynomial matrices with certain shifted degrees, and then provide some properties of the reverse operations.

For a polynomial $p = p_0 + p_1x + \cdots + p_ux^u \in \mathbb{K}[x]$ with degree bounded by u, the order of its coefficients can be reversed as

$$\operatorname{rev}(p, u) = p(x^{-1})\cdot x^u = p_u + p_{u-1}x + \cdots + p_1x^{u-1} + p_0x^u.$$

This can be extended to column vectors and row vectors with shifted degrees.

Definition 3.1. *Let $\vec{u} = [u_1, \ldots u_n] \in \mathbb{Z}^n$ be a degree shift, and $\mathbf{a} = [a_1, \ldots, a_n]^T \in \mathbb{K}[x]^{n\times 1}$, a column vector with $\vec{u}$-column degree bounded by v. We define*

$$\operatorname{colRev}(\mathbf{a}, \vec{u}, v) = x^{-\vec{u}}\mathbf{a}(x^{-1})\ x^v = \begin{bmatrix}\operatorname{rev}(a_1, v-u_1)\\ \vdots\\ \operatorname{rev}(a_n, v-u_n)\end{bmatrix}.$$

Similarly for a row vector $\mathbf{b} \in \mathbb{K}[x]^{1\times n}$ with $\operatorname{rdeg}_{\vec{u}}\mathbf{b} \leq v$, where $\vec{u} = [u_1, \ldots u_n] \in \mathbb{Z}^n$ is a degree shift, we define

$$\operatorname{rowRev}(\mathbf{b}, \vec{u}, v) = \operatorname{colRev}(\mathbf{b}^T, \vec{u}, v)^T = x^v\mathbf{b}(x^{-1})\ x^{-\vec{u}}.$$

Example 3.2. *If $\mathbf{f} = \left[10+x, 5+x+2x^2\right]$, $\vec{u} = [-1, -2]$, and $v = 0$, then*

$$\begin{aligned}\operatorname{rowRev}(\mathbf{f}, \vec{u}, v) &= x^0\left[10+x^{-1}, 5+x^{-1}+2x^{-2}\right]\begin{bmatrix}x & \\ & x^2\end{bmatrix}\\ &= \left[10x+1, 5x^2+x+2\right].\end{aligned}$$

We can extend the reverse operation further to polynomial matrices.

Definition 3.3. *Let* $\vec{u} = [u_1, \dots u_n] \in \mathbb{Z}^n$ *be a degree shift and* $\mathbf{A} \in \mathbb{K}[x]^{n\times k}$ *with* $\vec{u}$*-column degrees bounded by* $\vec{v} = [v_1, \dots, v_k] \in \mathbb{Z}^k$*. Define*

$$\begin{aligned} \operatorname{colRev}(\mathbf{A}, \vec{u}, \vec{v}) &= [\operatorname{colRev}(\mathbf{A}, \vec{u}, v_1), \dots, \operatorname{colRev}(\mathbf{A}, \vec{u}, v_k)] \\ &= x^{-\vec{u}} \mathbf{A}(x^{-1})\, x^{\vec{v}}. \end{aligned}$$

Similarly, for $\vec{u} \in \mathbb{Z}^n$ *and* $\mathbf{B} \in \mathbb{K}[x]^{k\times n}$ *with* $\vec{u}$*-row degrees bounded component-wise by* $\vec{v} \in \mathbb{Z}^k$*,*

$$\begin{aligned} \operatorname{rowRev}(\mathbf{B}, \vec{u}, \vec{v}) &= \begin{bmatrix} \operatorname{rowRev}(\mathbf{B}, \vec{u}, v_1) \\ \vdots \\ \operatorname{rowRev}(\mathbf{B}, \vec{u}, v_k) \end{bmatrix} \\ &= \operatorname{colRev}(\mathbf{B}^T, \vec{u}, \vec{v})^T \\ &= x^{\vec{v}} \mathbf{B}(x^{-1})\, x^{-\vec{u}}. \end{aligned}$$

It is not difficult to see that

$$\operatorname{rowRev}(\mathbf{B}, \vec{u}, \vec{v}) = \operatorname{colRev}(\mathbf{B}, -\vec{v}, -\vec{u}).$$

It is useful to note that any degree bound remains the same after the reverse operations.

Lemma 3.4. *If* $\mathbf{A} \in \mathbb{K}[x]^{n\times k}$ *has* $\operatorname{cdeg}_{\vec{u}}\mathbf{A} \le \vec{v}$*, then* $\mathbf{A}^c = \operatorname{colRev}(\mathbf{A}, \vec{u}, \vec{v})$ *also has* $\operatorname{cdeg}_{\vec{u}}\mathbf{A}^c \le \vec{v}$*.*

As one would expect, applying two reverse operations gives back the original input.

Lemma 3.5. *The following equalities holds:*

$$\begin{aligned} \operatorname{colRev}(\operatorname{colRev}(\mathbf{A}, \vec{u}, \vec{v}), \vec{u}, \vec{v}) &= \mathbf{A} \\ \operatorname{rowRev}(\operatorname{rowRev}(\mathbf{B}, \vec{u}, \vec{v}), \vec{u}, \vec{v}) &= \mathbf{B}. \end{aligned}$$

The following lemmas show the commutativity between reverse operations and multiplications.

Lemma 3.6. *If* $\mathbf{A} \in \mathbb{K}[x]^{m\times n}$ *has* $\operatorname{cdeg}_{\vec{u}}\mathbf{A} \le \vec{v}$*, and* $\mathbf{B} \in \mathbb{K}[x]^{n\times k}$ *has* $\operatorname{cdeg}_{\vec{v}}\mathbf{B} \le \vec{w}$*, then*

$$\operatorname{colRev}(\mathbf{A}, \vec{u}, \vec{v}) \operatorname{colRev}(\mathbf{B}, \vec{v}, \vec{w}) = \operatorname{colRev}(\mathbf{AB}, \vec{u}, \vec{w})$$

has $\vec{u}$*-column degrees bounded by* $\vec{w}$*.*

Lemma 3.7. *If* $\mathbf{A} \in \mathbb{K}[x]^{m\times n}$ *has* $\operatorname{rdeg}_{\vec{u}}\mathbf{A} \le \vec{v}$*, and* $\mathbf{B} \in \mathbb{K}[x]^{n\times k}$ *has* $\operatorname{cdeg}_{-\vec{u}}\mathbf{B} \le \vec{w}$*, then*

$$\operatorname{rowRev}(\mathbf{A}, \vec{u}, \vec{v}) \operatorname{colRev}(\mathbf{B}, -\vec{u}, \vec{w}) = \operatorname{colRev}(\mathbf{AB}, -\vec{v}, \vec{w}).$$

More details on these reverse operations are found in [13].

There is a natural relationship between a shifted minimal kernel basis and the reverse operation.

Lemma 3.8. *Let* $\vec{u} \in \mathbb{Z}^n$ *and* $\mathbf{A} \in \mathbb{K}[x]^{m\times n}$ *with* $(-\vec{u})$*-row degrees bounded by* $\vec{a}$*. If* $\mathbf{A}^r = \operatorname{rowRev}(\mathbf{A}, -\vec{u}, \vec{a})$ *then a matrix* $\mathbf{N} \in \mathbb{K}[x]^{n\times k}$ *with* $\vec{u}$*-column degrees* $\vec{b}$ *is a* $(\mathbf{A}, \vec{u})$*-kernel basis if and only if* $\mathbf{N}^c = \operatorname{colRev}\left(\mathbf{N}, \vec{u}, \vec{b}\right)$ *is a* $(\mathbf{A}^r, \vec{u})$*-kernel basis*

Proof. First note that any vector $\mathbf{q}$ with $\operatorname{cdeg}_{\vec{u}}\mathbf{q} = \alpha$ is in the kernel of $\mathbf{A}$ if and only if $\mathbf{q}^c = \operatorname{colRev}(\mathbf{q}, \vec{u}, \alpha)$ is in the kernel of $\mathbf{A}^r$, since by Lemma 3.7 $\mathbf{A} \cdot \mathbf{q} = 0$ implies

$$\mathbf{A}^r \cdot \mathbf{q}^c = \operatorname{colRev}(\mathbf{A} \cdot \mathbf{q}, -\vec{a}, \alpha) = 0,$$

and $\mathbf{A}^r \cdot \mathbf{q}^c = 0$ implies

$$\mathbf{A} \cdot \mathbf{q} = \operatorname{colRev}(\mathbf{A}^r \cdot \mathbf{q}^c, -\vec{a}, \alpha) = 0.$$

It follows that any matrix $\mathbf{N}$ is a kernel basis of $\mathbf{A}$ if and only if $\mathbf{N}^c = \operatorname{colRev}(\mathbf{N}, \vec{u}, \operatorname{cdeg}_{\vec{u}}\mathbf{N})$ is a kernel basis of $\mathbf{A}^r$. Lemma 3.4 then ensures that the minimality also holds at the same time. $\square$

4. UNIMODULAR COMPLETION

In this section, we look at how a unimodular completion can be done using a combination of kernel basis computations, order basis computations, and reverse operations.

We will show in Lemma 4.1 a close relationship between order bases and unimodular matrices, namely, suitable reverse operations can be applied to order bases to obtain unimodular matrices. This suggests that the problem of finding a unimodular completion of $\mathbf{F}$ is equivalent to finding some order basis containing a reversed $\mathbf{F}$. In addition, Lemma 2.9 shows how a kernel basis can be embedded in an order basis, that is, if we can make the reversed $\mathbf{F}$ a kernel basis of some matrix $\mathbf{M}$, then there is an order basis of $\mathbf{M}$ that contains the reversed $\mathbf{F}$. A natural choice for $\mathbf{M}$ is a kernel basis of the reversed $\mathbf{F}$. We actually have two choices here. We can either reverse the coefficients of $\mathbf{F}$, as we do in Theorem 4.4, or we can reverse the coefficients of a kernel basis of $\mathbf{F}$.

First let us look at how an order basis can lead to a unimodular matrix.

Lemma 4.1. *Given any matrix* $\mathbf{A} \in \mathbb{K}[x]^{m\times n}$ *and* $\vec{u} \in \mathbb{Z}^n$ *a degree shift, if* $\mathbf{P}$ *is an* $(\mathbf{A}, \vec{\sigma}, \vec{u})$*-basis with* $\operatorname{cdeg}_{\vec{u}}\mathbf{P} = \vec{v}$*. Then* $\mathbf{P}^c = \operatorname{colRev}(\mathbf{P}, \vec{u}, \vec{v})$ *is unimodular.*

Proof. Note first that the identity matrix is an $(\mathbf{A}, 0, \vec{u})$-basis, which has $\vec{u}$-column degrees $\vec{u}$ and determinant 1. An $(\mathbf{A}, \vec{\sigma}, \vec{u})$-basis $\mathbf{Q}$ can then be constructed iteratively based on Theorem 2.8 and using the algorithms from [1, 7], which only increase the $\vec{u}$-column degrees of the basis by multiplying some columns by x each time. The minimality of order bases ensures that $\operatorname{cdeg}_{\vec{u}}\mathbf{Q} = \operatorname{cdeg}_{\vec{u}}\mathbf{P} = \vec{v}$. As the $\vec{u}$-column degrees of the basis are increased from $\vec{u}$ to $\vec{v}$, its determinant of $\mathbf{Q}$ therefore increased from 1 to $x^{\sum \vec{v} - \sum \vec{u}}$. Since any two $(\mathbf{A}, \vec{\sigma}, \vec{u})$-bases are unimodularly equivalent, we get

$$\det(\mathbf{P}) = \det(\mathbf{QU}) = c \cdot x^{\sum \vec{v} - \sum \vec{u}}$$

for some unimodular matrix $\mathbf{U} \in \mathbb{K}[x]^{n\times n}$ and nonzero constant $c \in \mathbb{K}$. Hence

$$\begin{aligned} \det(\mathbf{P}^c) &= \det\left(x^{-\vec{u}}\left(\mathbf{P}(x^{-1})\right) x^{\vec{v}}\right) \\ &= x^{-\sum \vec{u}} \cdot \det\left(\mathbf{P}(x^{-1})\right) \cdot x^{\sum \vec{v}} \\ &= c \cdot x^{\sum \vec{v}} \cdot x^{-\sum \vec{v} + \sum \vec{u}} \cdot x^{-\sum \vec{u}} = c \end{aligned}$$

and $\mathbf{P}^c$ is unimodular. $\square$

Example 4.2. *Let* $\mathbf{A} \in \mathbb{Z}_5[x]^{2\times 4}$ *be given by*

$$\begin{bmatrix} 1 & 0 & 2+2x & 3+4x \\ 0 & x^2 & 1+3x^4 & 1+4x+3x^4 \end{bmatrix}$$

and $\vec{u} = [-2, -3, -1, -1]$. *Then one can show that*

$$\mathbf{P} = \begin{bmatrix} 4x + 3x^2 & 4 + x + 3x^2 & x^3 & 0 \\ 1 & 2x^3 & 0 & x^4 \\ 4x & 4 + x & 0 & 0 \\ x & 1 & 0 & 0 \end{bmatrix}$$

is an $(\mathbf{A}, [3, 6], \vec{u})$*-basis with* $\mathrm{cdeg}_{\vec{u}}\mathbf{P} = [0, 0, 1, 1]$. *Reversing coefficients gives the unimodular matrix*

$$\mathbf{P}^c = \begin{bmatrix} 4x + 3 & 4x^2 + x + 3 & 1 & 0 \\ x^3 & 2 & 0 & 1 \\ 4 & 4x + 1 & 0 & 0 \\ 1 & x & 0 & 0 \end{bmatrix}.$$

□

The following lemma shows the unimodular equivalence between any matrix $\mathbf{A}$ that has a unimodular column basis, and a left kernel basis of any right kernel basis of $\mathbf{A}$. This is needed later in Theorem 4.4 in order to replace $\mathbf{F}$ with a kernel basis that can be embedded in a unimodular matrix.

LEMMA 4.3. *Let* $\mathbf{A} \in \mathbb{K}[x]^{m\times n}$ *have a unimodular column basis and* $\mathbf{N} \in \mathbb{K}[x]^{n\times(n-m)}$ *be a right kernel basis of* $\mathbf{A}$. *If* $\mathbf{B}$ *is a left kernel basis of* $\mathbf{N}$ *then* $\mathbf{A} = \mathbf{U}\mathbf{B}$ *for a unimodular matrix* $\mathbf{U}$.

PROOF. This follows from [15, Lemma 3.3] which tells us that if $\mathbf{U}$ is a column basis of $\mathbf{A}$ then $\mathbf{A} = \mathbf{U}\mathbf{B}$. □

We are now ready to state a key result that allows a unimodular completion to be computed for a given input matrix $\mathbf{F}$. Basically, we compute a kernel basis of a reversed $\mathbf{F}$, then an order basis of the kernel basis can be reversed to provide a unimodular completion of $\mathbf{F}$.

THEOREM 4.4. *Let* $\mathbf{F}^r = \mathrm{rowRev}(\mathbf{F}, -\vec{u}, 0)$ *and* $\mathbf{M}$ *be a* $(\mathbf{F}^r, \vec{u})$*-kernel basis with* $\mathrm{cdeg}_{\vec{u}}\mathbf{M} = \vec{b}$. *Let* $\mathbf{P} = [\mathbf{P}_1, \mathbf{P}_2]$ *be a* $\left(\mathbf{M}^T, \vec{b} + 1, -\vec{u}\right)$*-basis, where* $\mathbf{P}_1$ *consists of all columns* $\mathbf{p}$ *with* $\mathrm{cdeg}_{-\vec{u}}\mathbf{p} \le 0$. *If* $\mathbf{P}_2^r = \mathrm{colRev}(\mathbf{P}_2, -\vec{u}, \mathrm{cdeg}_{-\vec{u}}\mathbf{P}_2)$, *then* $\begin{bmatrix} \mathbf{F} \\ \mathbf{P}_2^{rT} \end{bmatrix}$ *is a unimodular completion of* $\mathbf{F}$.

PROOF. Let $\mathbf{P}_1^r = \mathrm{colRev}(\mathbf{P}_1, -\vec{u}, \vec{v})$ where $\vec{v} = \mathrm{cdeg}_{-\vec{u}}\mathbf{P}_1$ is the shifted degree of $\mathbf{P}_1$. We know from Lemma 4.1 that $[\mathbf{P}_1^r, \mathbf{P}_2^r]$ is unimodular. Let $\mathbf{M}^r = \mathrm{colRev}\left(\mathbf{M}, \vec{u}, \vec{b}\right)$. Then from Lemma 3.8 we know $\mathbf{M}^r$ is a $(\mathbf{F}, \vec{s})$-kernel basis and $\mathbf{P}_1^r$ is a $\left((\mathbf{M}^r)^T, -\vec{u}\right)$-kernel basis. Hence, by Lemma 4.3, $\mathbf{F} = \mathbf{U}(\mathbf{P}_1^r)^T$ for some unimodular matrix $\mathbf{U}$. Therefore

$$\begin{bmatrix} \mathbf{F} \\ \mathbf{P}_2^{rT} \end{bmatrix} = \begin{bmatrix} \mathbf{U} & 0 \\ 0 & I \end{bmatrix} \cdot \begin{bmatrix} \mathbf{P}_1^{rT} \\ \mathbf{P}_2^{rT} \end{bmatrix}$$

hence is itself unimodular. □

EXAMPLE 4.5. *Let* $\mathbf{F} \in \mathbb{Z}_5[x]^{2\times 4}$ *be given by*

$$\begin{bmatrix} -2x + 1 & 2x^3 & -2 & 2 \\ -x^2 + 2x & -x^3 + 2 & -x + 2 & x - 1 \end{bmatrix}$$

with shift $\vec{u} = [2, 3, 1, 1]$. *Then the transpose of a* $\vec{u}$*-minimal kernel basis for the row reversed polynomial matrix,* $\mathbf{F}^r$, *is given by*

$$\mathbf{M}^T = \begin{bmatrix} 1 & 0 & 2 + 2x & 4x + 3 \\ 0 & x^2 & 1 + 3x^4 & 1 + 4x + 3x^4 \end{bmatrix}$$

with $\vec{b} = \mathrm{cdeg}_{\vec{u}}\mathbf{M} = [2, 5]$. *An* $(\mathbf{M}^T, \vec{b} + 1, -\vec{u})$*-order basis is given by*

$$\mathbf{P} = \begin{bmatrix} 4x + 3x^2 & 4 + x + 3x^2 & x^3 & 0 \\ 1 & 2x^3 & 0 & x^4 \\ 4x & 4 + x & 0 & 0 \\ x & 1 & 0 & 0 \end{bmatrix}$$

from Example 4.2. Reversing the last two columns of $\mathbf{P}$ *and taking transposes give a unimodular completion*

$$\mathbf{P}_2^{rT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

□

Theorem 4.4 provides a way to correctly compute a unimodular completion of $\mathbf{F}$. To improve the computational efficiency, it is helpful to separate the rows of $\mathbf{M}^T$ and just work with one subset of rows at a time. This is possible by the following lemma.

LEMMA 4.6. *Let* $\mathbf{F}^r = \mathrm{rowRev}(\mathbf{F}, -\vec{u}, 0)$ *and* $\mathbf{M}$ *be a* $(\mathbf{F}^r, \vec{u})$*-kernel basis with* $\mathrm{cdeg}_{\vec{u}}\mathbf{M} = \vec{b}$ *and partitioned as* $\mathbf{M} = [\mathbf{M}_1, \mathbf{M}_2]$. *Let* $\mathbf{P}_1$ *be a* $\left(\mathbf{M}_1^T, \mathrm{cdeg}_{\vec{u}}\mathbf{M}_1 + 1, -\vec{u}\right)$*-basis partitioned as* $\mathbf{P}_1 = [\mathbf{N}_1, \mathbf{Q}_1]$, *where* $\mathbf{N}_1$ *consists of all columns* $\mathbf{p}$ *of* $\mathbf{P}_1$ *with* $\mathrm{cdeg}_{-\vec{u}}\mathbf{p} \le 0$. *Let* $\vec{t} = \mathrm{cdeg}_{-\vec{u}}\mathbf{N}_1$ *and* $\mathbf{P}_2$ *be a* $\left(\mathbf{M}_2^T\mathbf{N}_1, \mathrm{cdeg}_{\vec{u}}\mathbf{M}_2 + 1, \vec{t}\right)$*-basis partitioned as* $\mathbf{P}_2 = [\mathbf{N}_2, \mathbf{Q}_2]$, *where* $\mathbf{N}_2$ *consists of all columns* $\mathbf{p}$ *of* $\mathbf{P}_2$ *with* $\mathrm{cdeg}_{-\vec{t}}\mathbf{p} \le 0$. *If* $\mathbf{R} = [\mathbf{N}_1\mathbf{Q}_2, \mathbf{Q}_1]$ *and* $\mathbf{R}^r = \mathrm{colRev}(\mathbf{R}, -\vec{u}, \mathrm{cdeg}_{-\vec{u}}\mathbf{R})$, *then* $\begin{bmatrix} \mathbf{F} \\ \mathbf{R}^{rT} \end{bmatrix}$ *is a unimodular completion of* $\mathbf{F}$.

PROOF. Let $\mathbf{P}_1^r = \mathrm{colRev}(\mathbf{P}_1, -\vec{s}, \mathrm{cdeg}_{-\vec{s}}\mathbf{P}_1)$ and $\mathbf{P}_2^r = \mathrm{colRev}\left(\mathbf{P}_2, \vec{t}, \mathrm{cdeg}_{\vec{t}}\mathbf{P}_2\right)$. From Lemma 4.1 we have that both $\mathbf{P}_1^r$ and $\mathbf{P}_2^r$ are unimodular and hence

$$\mathbf{P}_1^r \cdot \mathrm{diag}\left([\mathbf{P}_2^r, I]\right) = [\mathbf{N}_1^r\mathbf{N}_2^r, \mathbf{N}_1^r\mathbf{Q}_2^r, \mathbf{Q}_1] = [\mathbf{N}_1^r\mathbf{N}_2^r, \mathbf{R}^r]$$

is unimodular, where $\mathbf{N}_1\mathbf{N}_2$ is a kernel basis of $\mathbf{M}$. The result follows by the same reasoning as in the proof of Theorem 4.4. □

5. EFFICIENT COMPUTATION

Lemma 4.6 provides a way to correctly compute a unimodular completion of $\mathbf{F}$. Our next task is to make sure it can be computed efficiently and analyze its computational cost. We already know that a $(\mathbf{F}^r, \vec{s})$-kernel basis can be computed with a cost of $O^\sim(n^\omega s)$. Therefore, it only remains to check the cost of the order basis computations. Note that the non-uniform order makes our problem here a little more difficult. However, the output basis has its $-\vec{s}$-column degrees bounded by 1, which is a consequence of the fact $\mathbf{M}$ is a $\vec{s}$-minimal kernel basis, as shown in Lemma 5.4 below. But we first need a few general lemmas on the degree bounds of order bases and kernel bases.

First, the following lemma is a simple extension of Lemma 3.2 in [16] for dealing with nonuniform orders.

LEMMA 5.1. *Given $\mathbf{A} \in \mathbb{K}^{m\times n}[x]$, a shift $\vec{u} \in \mathbb{Z}^n$, and an order list $\vec{\sigma} \in \mathbb{Z}^m$, let $\vec{v}$ be the $\vec{u}$-column degrees of a $(\mathbf{A}, \vec{\sigma}, \vec{u})$-basis. Then*

$$\sum \vec{v} \ \le \ \sum \vec{u} + \sum \vec{\sigma}.$$

PROOF. The sum of the $\vec{u}$-column degrees is $\sum \vec{u}$ at order 0, since the identity matrix is a $(\mathbf{A}, 0, \vec{u})$-basis. This sum increases by 1 for each order increase of each row. The total number of order increases required for all rows is at most $\sum \vec{\sigma}$. Note that from Theorem 2.8, we can work with just one row at a time to increase its order in the order basis computation. □

The following lemma extends Theorem 2.4 to give a bound based on the shifted column degrees or shifted row degrees, instead of just the column degrees of the input matrix.

LEMMA 5.2. *If $\mathbf{A} \in \mathbb{K}^{m\times n}[x]$ has $\operatorname{rdeg}_{\vec{u}}\mathbf{A} \le \vec{v}$ or equivalently $\operatorname{cdeg}_{-\vec{v}}\mathbf{A} \le -\vec{u}$, then any $(\mathbf{A}, -\vec{u})$-kernel basis $\mathbf{B}$ satisfies*

$$\sum \operatorname{cdeg}_{-\vec{u}}\mathbf{B} \le \sum \vec{v} - \sum \vec{u}.$$

PROOF. Let $\mathbf{P} = [\mathbf{B}, \bar{\mathbf{B}}]$ be a $(\mathbf{A}, \vec{v} + \sigma, -\vec{u})$-basis containing a kernel basis, $\mathbf{B}$, of $\mathbf{A}$. Then

$$\sum \operatorname{cdeg}_{-\vec{u}}\mathbf{P} \le m\sigma + \sum \vec{v} - \sum \vec{u}. \tag{1}$$

by Lemma 5.1 From Lemma 2.1 we also know that

$$\sum \operatorname{cdeg}_{-\vec{u}}\bar{\mathbf{B}} \ge \sum \operatorname{cdeg}_{-\vec{v}}\mathbf{A}\bar{\mathbf{B}}.$$

In addition, we know

$$\operatorname{cdeg}\mathbf{A}\bar{\mathbf{B}} \ge \vec{v} + \sigma$$

since $\bar{\mathbf{B}}$ has order $(\mathbf{A}, \vec{v} + \sigma)$, implying

$$\sum \operatorname{cdeg}_{-\vec{v}}\mathbf{A}\bar{\mathbf{B}} \ge m\sigma$$

and so

$$\sum \operatorname{cdeg}_{-\vec{u}}\bar{\mathbf{B}} \ge m\sigma. \tag{2}$$

Combining (1) and (2), It follows that

$$\begin{aligned}\sum \operatorname{cdeg}_{-\vec{u}}\mathbf{B} &= \sum \operatorname{cdeg}_{-\vec{u}}\mathbf{P} - \sum \operatorname{cdeg}_{-\vec{u}}\bar{\mathbf{B}} \\ &\le \sum \vec{v} - \sum \vec{u}.\end{aligned}$$

□

Note that Lemma 5.2 specializes to Theorem 2.4 when $\vec{v} = 0$.

When the matrix $\mathbf{A}$ is also a $(\mathbf{B}^T, \vec{u})$-kernel basis, as in our case, the bound in fact becomes tight.

LEMMA 5.3. *Let $\mathbf{A} \in \mathbb{K}^{m\times n}[x]$ and $\mathbf{B} \in \mathbb{K}^{n\times(n-m)}[x]$. If $\mathbf{B}$ is a $(\mathbf{A}, -\vec{u})$-kernel basis with $\operatorname{cdeg}_{-\vec{u}}\mathbf{B} = \vec{w}$ and $\mathbf{A}^T$ is a $(\mathbf{B}^T, \vec{u})$-kernel basis with $\operatorname{rdeg}_{\vec{u}}\mathbf{A} = \vec{v}$, then*

$$\sum \vec{w} = \sum \vec{v} - \sum \vec{u}.$$

PROOF. This follows from Lemma 5.2, which gives

$$\sum \vec{w} \le \sum \vec{v} - \sum \vec{u}$$

and also

$$\sum \vec{v} \le \sum \vec{w} + \sum \vec{u}$$

in the reverse direction. □

From Lemma 2.9, we know that any $\left(\mathbf{M}^T, \vec{b} + 1, -\vec{s}\right)$-basis contains a $\left(\mathbf{M}^T, -\vec{s}\right)$-kernel basis whose $-\vec{s}$-column degrees are bounded by 0. The following lemma shows that the remaining part of the $\left(\mathbf{M}^T, \vec{b} + 1, -\vec{s}\right)$-basis has degrees bounded by 1.

LEMMA 5.4. *Let $\mathbf{F}^r = \operatorname{rowRev}(\mathbf{F}, -\vec{s}, 0)$ and $\mathbf{M}$ be a $(\mathbf{F}^r, \vec{s})$-kernel basis with $\operatorname{cdeg}_{\vec{s}}\mathbf{M} = \vec{b}$. Partition $\mathbf{P}$, a $\left(\mathbf{M}^T, \vec{b} + 1, -\vec{s}\right)$-basis, as $\mathbf{P} = [\mathbf{P}_1, \mathbf{P}_2]$ where where $\mathbf{P}_1$ consists of all columns $\mathbf{p}$ with $\operatorname{cdeg}_{-\vec{s}}\mathbf{p} \le 0$. Then*

$$\operatorname{cdeg}_{-\vec{b}-1}\mathbf{M}^T\mathbf{P}_2 = 0 \quad \textit{and} \quad \operatorname{cdeg}_{-\vec{s}}\mathbf{P}_2 = 1.$$

PROOF. We already know that $\mathbf{P}$ contains a $\left(\mathbf{M}^T, -\vec{s}\right)$-kernel basis $\mathbf{P}_1$. Furthermore as in the proof of Lemma 5.2 we have

$$\sum \operatorname{cdeg}_{-\vec{s}}\mathbf{P} = -\sum \vec{s} + \sum \vec{b} + n - m$$

while from Lemma 5.3 we have for the kernel basis $\mathbf{P}_1$ in $\mathbf{P}$

$$\sum \operatorname{cdeg}_{-\vec{s}}\mathbf{P}_1 = \sum \vec{b} - \sum \vec{s}$$

and therefore, $\sum \operatorname{cdeg}_{-\vec{s}}\mathbf{P}_2 = n - m$. From Lemma 2.1, it follows that

$$\sum \operatorname{cdeg}_{-\vec{b}}\mathbf{M}^T\mathbf{P}_2 \le \sum \operatorname{cdeg}_{-\vec{s}}\mathbf{P}_2 = n - m,$$

or equivalently,

$$\sum \operatorname{cdeg}_{-\vec{b}-1}\mathbf{M}^T\mathbf{P}_2 \le 0.$$

But since $\mathbf{P}_2$ is nonzero and has order $\left(\mathbf{F}, \vec{b} + 1\right)$, we have

$$\sum \operatorname{cdeg}_{-\vec{b}-1}\mathbf{M}^T\mathbf{P}_2 \ge 0.$$

It follows that

$$\sum \operatorname{cdeg}_{-\vec{b}-1}\mathbf{M}^T\mathbf{P}_2 = 0$$

hence $\operatorname{cdeg}_{-\vec{b}-1}\mathbf{M}^T\mathbf{P}_2 = 0$ or $\operatorname{cdeg}_{-\vec{b}}\mathbf{M}^T\mathbf{P}_2 = 1$. Combining this with

$$\sum \operatorname{cdeg}_{-\vec{b}}\mathbf{M}^T\mathbf{P}_2 \le \sum \operatorname{cdeg}_{-\vec{s}}\mathbf{P}_2 = n - m$$

we then get $\operatorname{cdeg}_{-\vec{s}}\mathbf{P}_2 = 1$. □

We are now ready to look at the procedure for computing a $\left(\mathbf{M}^T, \vec{b} + 1, -\vec{s}\right)$-basis, given in Algorithm Algorithm 1. The situation here is similar to the situation in computing a left kernel basis in the column basis computation from [15]. That is, the order $\vec{b}+1$, or equivalently, the $\vec{s}$-row degrees of $\mathbf{M}^T$ may be unbalanced and can have degree as large as $\sum \vec{s}$. We therefore follow the same process as in the computation of column bases [15].

We assume without loss of generality that the rows of $\mathbf{M}^T$ are arranged in decreasing $\vec{s}$-row degrees and divide $\mathbf{M}^T$ into $\lceil \log k \rceil$ row blocks according to the $\vec{s}$-row degrees of its rows. Let

$$\mathbf{M}^T = \begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \\ \vdots \\ \mathbf{M}_{\lceil \log k \rceil} \end{bmatrix}^T$$

with $\mathbf{M}_{\log k}, \mathbf{M}_{\log k-1}, \cdots, \mathbf{M}_2, \mathbf{M}_1$ having $\vec{s}$-row degrees in the range

$[0, 2\xi/k]$, $(2\xi/k, 4\xi/k]$, $(4\xi/k, 8\xi/k]$, ..., $(\xi/4, \xi/2]$, $(\xi/2, \xi]$

respectively. Let $\sigma_i = \lceil \xi/2^{i-1} \rceil + 1$ and $\vec{\sigma}_i = [\sigma_i, \dots, \sigma_i]$ with the same dimension as the row dimension of $\mathbf{M}_i$, and

$$\vec{\sigma} = \left[\vec{\sigma}_{\lceil \log k \rceil}, \vec{\sigma}_{\lceil \log k \rceil - 1}, \dots, \vec{\sigma}_1\right]$$

be the order in the order basis computation. For simplicity, instead of using $\mathbf{M}^T$ as the input matrix, we use

$$\hat{\mathbf{M}} = \begin{bmatrix} \hat{\mathbf{M}}_1 \\ \vdots \\ \hat{\mathbf{M}}_{\lceil \log k \rceil} \end{bmatrix} = x^{\vec{\sigma} - \vec{b} - 1} \begin{bmatrix} \mathbf{M}_1 \\ \vdots \\ \mathbf{M}_{\lceil \log k \rceil} \end{bmatrix} = x^{\vec{\sigma} - \vec{b} - 1} \mathbf{M}^T$$

instead, so that the order of our problem in each block is uniform and a $\left(\hat{\mathbf{M}}, \vec{\sigma}, -\vec{s}\right)$-basis is a $\left(\mathbf{M}^T, \vec{b} + 1, -\vec{s}\right)$-basis.

We now do a series of order basis computations in order to compute a unimodular completion of $\mathbf{F}$ based on Lemma 4.6.

1. Let $\vec{s}_1 = \vec{s}$. First we compute an $\left(\hat{\mathbf{M}}_1, \vec{\sigma}_1, -\vec{s}_1\right)$-order basis using Algorithm 2 of [14], which can be done with a cost of $O^\sim(n^\omega s)$. Partition $\mathbf{P}_1 = [\mathbf{N}_1, \mathbf{Q}_1]$, where $\mathbf{N}_1$ is a $\left(\hat{\mathbf{M}}_1, -\vec{s}_1\right)$-kernel basis. Set $\tilde{\mathbf{N}}_1 = \mathbf{N}_1$ and $\vec{s}_2 = -\operatorname{cdeg}_{-\vec{s}} \mathbf{N}_1$.
2. Compute an $\left(\hat{\mathbf{M}}_2 \tilde{\mathbf{N}}_1, \vec{\sigma}_2, -\vec{s}_2\right)$-order basis and partition $\mathbf{P}_2 = [\mathbf{N}_2, \mathbf{Q}_2]$ with $\mathbf{N}_2$ a $\left(\hat{\mathbf{M}}_2, -\vec{s}_2\right)$-kernel basis. Set $\tilde{\mathbf{N}}_2 = \tilde{\mathbf{N}}_1 \mathbf{N}_2$ and $\vec{s}_3 = -\operatorname{cdeg}_{-\vec{s}_2} \mathbf{N}_2$. Note that $\tilde{\mathbf{N}}_2$ is a $-\vec{s}$-minimal kernel basis of $\begin{bmatrix} \hat{\mathbf{M}}_1 \\ \hat{\mathbf{M}}_2 \end{bmatrix}$ with $\vec{s}_3 = -\operatorname{cdeg}_{-\vec{s}} \tilde{\mathbf{N}}_2$.
3. Continue this process, an $\left(\hat{\mathbf{M}}_i \tilde{\mathbf{N}}_{i-1}, \vec{\sigma}_i, -\vec{s}_i\right)$-order basis $\mathbf{P}_i$ is computed at step i. Partition $\mathbf{P}_i = [\mathbf{N}_i, \mathbf{Q}_i]$ with $\mathbf{N}_i$ an $\left(\hat{\mathbf{M}}_i \tilde{\mathbf{N}}_{i-1}, -\vec{s}_i\right)$-kernel basis, where $\vec{s}_i = -\operatorname{cdeg}_{-\vec{s}} \tilde{\mathbf{N}}_{i-1} = -\operatorname{cdeg}_{-\vec{s}_{i-1}} \mathbf{N}_{i-1}$. Then
$$\tilde{\mathbf{N}}_i = \prod_{j=1}^{i} \mathbf{N}_i = \tilde{\mathbf{N}}_{i-1} \mathbf{N}_i$$
is a $-\vec{s}$-minimal kernel basis of the first i blocks of $\mathbf{M}^T$. In particular, $\tilde{\mathbf{N}}_{\lceil \log k \rceil}$ is a $\left(\mathbf{M}^T, -\vec{s}\right)$-kernel basis.
4. Let $\mathbf{R} = \left[\mathbf{Q}_1, \tilde{\mathbf{N}}_1 \mathbf{Q}_2, \dots, \tilde{\mathbf{N}}_{\lceil \log k \rceil - 2} \mathbf{Q}_{\lceil \log k \rceil - 1}, \tilde{\mathbf{N}}_{\lceil \log k \rceil - 1} \mathbf{Q}_{\lceil \log k \rceil}\right]$, and $\mathbf{R}^r = \operatorname{colRev}(\mathbf{R}, -\vec{s}, \operatorname{cdeg}_{-\vec{s}} \mathbf{R})$. Then from Lemma 4.6 we can conclude that $\left[\mathbf{F}^T, \mathbf{R}^r\right]$ is a unimodular matrix.

Algorithm 1 unimodularCompletion($\mathbf{F}$)

Input: $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ with full row rank; $\vec{s}$ is initially set to the column degrees of $\mathbf{F}$. It keeps track of the degrees.

Output: $\mathbf{G} \in \mathbb{K}[x]^{(n-m) \times n}$ such that $\begin{bmatrix} \mathbf{F} \\ \mathbf{G} \end{bmatrix}$ is unimodular.

$\vec{s} := \operatorname{cdeg} \mathbf{F}$;
$\mathbf{F}^r := \operatorname{rowRev}(\mathbf{F}, -\vec{s}, 0)$;
$\mathbf{M} := \operatorname{MinimalKernelBasis}(\mathbf{F}^r, \vec{s})$; $\vec{b} := \operatorname{cdeg}_{\vec{s}} \mathbf{M}$; $k := n - m$;
Organize $\left[\mathbf{M}_1^T, \mathbf{M}_2^T, \cdots, \mathbf{M}_{\lceil \log k \rceil - 1}^T, \mathbf{M}_{\lceil \log k \rceil}^T\right] := \mathbf{M}$, with $\mathbf{M}_{\lceil \log k \rceil}, \mathbf{M}_{\lceil \log k \rceil - 1}, \cdots, \mathbf{M}_2, \mathbf{M}_1$ having $\vec{s}$-row degrees in the ranges $[0, 2\xi/k]$, $(2\xi/k, 4\xi/k]$, ..., $(\xi/4, \xi/2]$, $(\xi/2, \xi]$.
for i **from** 1 **to** $\lceil \log k \rceil$ **do**
  $\vec{\sigma}_i := \left[\xi/2^{i-1} + 1, \dots, \xi/2^{i-1} + 1\right]$, with the number of entries matches the row dimension of $\mathbf{M}_i$;
end for
$\vec{\sigma} := \left[\vec{\sigma}_{\lceil \log k \rceil}, \vec{\sigma}_{\lceil \log k \rceil - 1}, \dots, \vec{\sigma}_1\right]$;
$\hat{\mathbf{M}} := x^{\vec{\sigma} - \vec{b} - 1} \mathbf{M}$;
$\mathbf{N}_0 := I_n$; $\tilde{\mathbf{N}}_0 := I_n$;
for i **from** 1 **to** $\lceil \log k \rceil$ **do**
  $\vec{s}_i := -\operatorname{cdeg}_{-\vec{s}_{i-1}} \mathbf{N}_{i-1}$; (note $\vec{s}_1 = \vec{s}$)
  $\mathbf{P}_i := \operatorname{UnbalancedFastOrderBasis}\left(\hat{\mathbf{M}}_i \tilde{\mathbf{N}}_{i-1}, \vec{\sigma}_i, -\vec{s}_i\right)$;
  $[\mathbf{N}_i, \mathbf{Q}_i] := \mathbf{P}_i$, where $\mathbf{N}_i$ is a $\left(\hat{\mathbf{M}}_i, -\vec{s}_i\right)$-kernel basis;
  $\tilde{\mathbf{N}}_i := \tilde{\mathbf{N}}_{i-1} \cdot \mathbf{N}_i$;
  $\mathbf{R} := \left[\mathbf{R}, \tilde{\mathbf{N}}_{i-1} \mathbf{Q}_i\right]$;
end for
$\mathbf{R}^r := \operatorname{colRev}(\mathbf{R}, -\vec{s}, \operatorname{cdeg}_{-\vec{s}} \mathbf{R})$;
return $(\mathbf{R}^r)^T$

5.1 Computational Cost

The cost of Algorithm 1 is dominated by the kernel basis computation, order basis computations, and the multiplications $\hat{\mathbf{M}}_i \tilde{\mathbf{N}}_{i-1}$, $\tilde{\mathbf{N}}_{i-1} \mathbf{N}_i$, and $\tilde{\mathbf{N}}_{i-1} \mathbf{Q}_i$. From Theorem 2.5 we know the kernel basis computation can be done with a cost of $O^\sim(n^\omega s)$. To determine the cost of order basis computations and multiplications, it is helpful to first look at the size of $\vec{s}_i$.

LEMMA 5.5. *The shifted degrees* $\vec{s}_i = -\operatorname{cdeg}_{-\vec{s}} \tilde{\mathbf{N}}_{i-1} = -\operatorname{cdeg}_{-\vec{s}_{i-1}} \mathbf{N}_{i-1}$ *satisfy* $\sum \vec{s}_i \le \xi$.

PROOF. Recall that $\tilde{\mathbf{N}}_{i-1}$ is a $-\vec{s}$-minimal kernel basis of a matrix $\mathbf{A}$ consists of a subset of rows of $\mathbf{M}^T$, which has $\operatorname{cdeg}_{\vec{s}} \mathbf{M} = \vec{b}$, or $\operatorname{rdeg}_{\vec{s}} \mathbf{M}^T = \vec{b}$. Hence by Lemma 5.2

$$\sum -\vec{s}_i = \operatorname{cdeg}_{-\vec{s}} \tilde{\mathbf{N}}_{i-1} \le \sum \operatorname{rdeg}_{\vec{s}} \mathbf{A} - \sum \vec{s} \le \sum \vec{b} - \sum \vec{s},$$

which gives

$$\sum \vec{s}_i \le \sum \vec{s} - \sum \vec{b} \le \sum \vec{s} = \xi.$$

Here recall that $\vec{b} = \operatorname{cdeg}_{\vec{s}} \mathbf{M} \ge 0$ since $\vec{s} \ge 0$ and $\vec{b} \le \sum \vec{s}$ by Theorem 2.4. □

The order basis computation UnbalancedFastOrderBasis in Algorithm 1 uses the algorithm for computing order basis with unbalanced shift from [13, 14].

LEMMA 5.6. *An* $\left(\hat{\mathbf{M}}_i\tilde{\mathbf{N}}_{i-1}, \vec{\sigma}_i, -\vec{s}_i\right)$*-order basis can be computed with a cost of* $O^{\sim}(n^\omega s)$.

PROOF. From the construction of $\hat{\mathbf{M}}_i$, the matrix $\hat{\mathbf{M}}_i$ and $\hat{\mathbf{M}}_i\tilde{\mathbf{N}}_{i-1}$ have less than 2^i rows, and for simplicity can be assumed to be 2^i rows by appending zero rows. We also have $\sigma_i = \lceil \xi/2^{i-1} \rceil + 1 \in \Theta(\xi/2^i)$. From Lemma 5.5 we also have $\sum \vec{s}_i \le \xi$. Therefore, the conditions of Theorem 2.7 are satisfied, and Algorithm 2 from [14] for order basis computation with unbalanced shift can be used with a cost of $O^{\sim}(n^\omega s)$. □

LEMMA 5.7. *The multiplications* $\hat{\mathbf{M}}_i\tilde{\mathbf{N}}_{i-1}$ *can be done with a cost of* $O^{\sim}(n^\omega s)$.

PROOF. The dimension of $\hat{\mathbf{M}}_i$ is bounded by $2^i \times n$ and

$$\sum \mathrm{rdeg}_{\vec{s}} \hat{\mathbf{M}}_i \le 2^i \cdot \xi/2^{i-1} \in O(\xi).$$

As in the proof of Lemma 5.5 we also have $\mathrm{cdeg}_{-\vec{s}} \tilde{\mathbf{N}}_{i-1} \le 0$, or equivalently, $\mathrm{rdeg}\, \tilde{\mathbf{N}}_{i-1} \le \vec{s}$. We can now use Theorem 2.2 to multiply $\tilde{\mathbf{N}}_{i-1}^T$ and $\hat{\mathbf{M}}_i^T$ with a cost of $O^{\sim}(n^\omega s)$. □

LEMMA 5.8. *The multiplication* $\tilde{\mathbf{N}}_{i-1}\mathbf{N}_i$ *can be done with a cost of* $O^{\sim}(n^\omega s)$.

PROOF. We know $\mathrm{cdeg}_{-\vec{s}} \tilde{\mathbf{N}}_{i-1} = -\vec{s}_i$, and $\mathrm{cdeg}_{-\vec{s}_i} \mathbf{N}_i = -\vec{s}_{i+1} \le 0$. In other words, $\mathrm{rdeg}\, \mathbf{N}_i \le \vec{s}_i$, and $\mathrm{rdeg}_{\vec{s}_i} \tilde{\mathbf{N}}_{i-1} \le \vec{s}$. We also have $\sum \vec{s}_i \le \xi$ from Lemma 5.5. Hence we can again use Theorem 2.2 to multiply $\mathbf{N}_i^T$ and $\tilde{\mathbf{N}}_{i-1}^T$ with a cost of $O^{\sim}(n^\omega s)$. □

LEMMA 5.9. *The multiplication* $\tilde{\mathbf{N}}_{i-1}\mathbf{Q}_i$ *can be done with a cost of* $O^{\sim}(n^\omega s)$.

PROOF. We know

$$\mathrm{cdeg}_{-\vec{s}_i} \mathbf{Q}_i \le \max \mathrm{cdeg}_{\vec{s}} \mathbf{P} = 1,$$

or equivalently,

$$\mathrm{rdeg}\, \mathbf{Q}_i \le \vec{s}_i + 1.$$

But we also know that this $\mathbf{Q}_i$ from the order basis computation has a factor xI. Therefore, $\mathrm{rdeg}\,(\mathbf{Q}_i/x) \le \vec{s}_i$. In addition, $\mathrm{rdeg}_{\vec{s}_i} \tilde{\mathbf{N}}_{i-1} \le \vec{s}$ as before. We again have $\sum \vec{s}_i \le \xi$ from Lemma 5.5. So we can again use Theorem 2.2 to multiply $\mathbf{Q}_i^T$ and $\tilde{\mathbf{N}}_{i-1}^T$ with a cost of $O^{\sim}(n^\omega s)$. □

THEOREM 5.10. *A unimodular completion of* $\mathbf{F}$ *can be computed with a cost of* $O^{\sim}(n^\omega s)$ *field operations.*

6. CONCLUSION

In this paper, we have presented an efficient deterministic algorithm for a unimodular completion of a matrix of polynomnials. Our algorithm computes a unimodular completion of an input matrix $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$, $m < n$ with a cost of $O^{\sim}(n^\omega s)$, where s is the average of the m largest column degrees of the input matrix. Future directions of interest include efficient deterministic unimodular completion in domains such as matrices of multivariate polynomials and matrices of differential or, more generally, of Ore operators.

References

[1] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3):804–823, 1994.

[2] B. Beckermann and G. Labahn. Recursiveness in matrix rational interpolation problems. *Journal of Computational and Applied Math*, 5-34, 1997.

[3] B. Beckermann, G. Labahn, and G. Villard. Shifted normal forms of polynomial matrices. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC'99, pages 189–196, 1999.

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

[5] T. Cluzeau and A Quadrat. Isomorphisms and Serre's reduction of linear systems. In *Proceedings of the 8th International Workshop on Multidimensional Systems*, 2013.

[6] A. Fabianska and A. Quadrat. Applications of the Quillen-Suslin theorem to multidimensional systems theory. In H. Park and G. Regensburger, editors, *Radon Series on Computational and Applied Mathematics*, pages 23–106. Walter de Gruyter, Berlin, 2007.

[7] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation, Philadelphia, Pennsylvania, USA*, pages 135–142. ACM Press, 2003.

[8] T.Y. Lam. *Serre's Conjecture*, volume 635 of *Lecture Notes in Mathematics*. Springer-Verlag, 1978.

[9] A. Logar and B. Sturmfels. Algorithms for the Quillen-Suslin theorem. *Journal of Algebra*, 145:231–239, 1992.

[10] M. Newman. *Integral Matrices*. Springer, 1972.

[11] J. von zur Gathen and J Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2nd edition edition, 2003.

[12] D.C. Youla and P.F. Pickel. The Quillen-Suslin theorm and the structure of n-dimensional elementary polynomial matrices. *IEEE Tranactions on Circuits and Systems*, 31(6):513–518, 1984.

[13] W. Zhou. *Fast Order Basis and Kernel Basis Computation and Related Problems*. PhD thesis, University of Waterloo, 2012.

[14] W. Zhou and G. Labahn. Efficient algorithms for order basis computation. *Journal of Symbolic Computation*, 47:793–819, 2012.

[15] W. Zhou and G. Labahn. Computing column bases of polynomial matrices. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC'13, pages 379–386. ACM, 2013.

[16] W. Zhou, G. Labahn, and A. Storjohann. Computing minimal nullspace bases. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC'12, pages 375–382. ACM, 2012.