A New Algorithm for General Factorizations of Multivariate Polynomial Matrices

Dong Lu
KLMM, UCAS, Academy of
Mathematics and Systems Science,
Chinese Academy of Sciences
Beijing, China 100190
donglu@amss.ac.cn

Xiaodong Ma
College of Science, China
Agricultural University
Beijing, China 100083
maxiaodong@cau.edu.cn

Dingkang Wang
KLMM, UCAS, Academy of
Mathematics and Systems Science,
Chinese Academy of Sciences
Beijing, China 100190
dwang@mmrc.iss.ac.cn

ABSTRACT

We investigate how to factorize a multivariate polynomial matrix into the product of two matrices. There are two major parts. The first is a factorization theorem, which asserts that a multivariate polynomial matrix whose lower order minors satisfy certain conditions admits a matrix factorization. Our theory is a generalization to the previous results given by Lin et.al [16] and Liu et.al [17]. The second is the implementation for factorizing polynomial matrices. According to the proof of factorization theorem, we construct a main algorithm which extends the range of polynomial matrices that can be factorized. In this algorithm, two critical steps are involved in how to compute a zero left prime matrix and a unimodular matrix. Firstly, based on the famous Quillen-Suslin theorem, a new sub-algorithm is presented to obtain a zero left prime matrix by calculating the bases of the syzygies of two low-order polynomial matrices. Experiments show that it is more efficient than the algorithm constructed by Wang and Kwong [31]. Secondly, some auxiliary information provided by the above new sub-algorithm is used to construct a unimodular matrix. As a consequence, the main algorithm extends the application range of the constructive algorithm in [17]. We implement all the algorithms proposed above on the computer algebra system *Singular* and give a nontrivial example to show the process of the main algorithm.

CCS CONCEPTS

• **Computing methodologies → Symbolic and algebraic algorithms**;

KEYWORDS

Multivariate polynomial matrices, Matrix factorization, Reduced minors, Zero left prime matrix, Unimodular matrix

ACM Reference format:
Dong Lu, Xiaodong Ma, and Dingkang Wang. 2017. A New Algorithm for General Factorizations of Multivariate Polynomial Matrices. In *Proceedings of ISSAC '17, Kaiserslautern, Germany, July 25-28, 2017,* 8 pages.
https://doi.org/10.1145/3087604.3087607

1 INTRODUCTION

Since multivariate polynomial matrix factorizations have a wide range of applications in multidimensional circuits, systems and controls, and other related areas [1, 8], they have attracted much attention over the past several decades. Thereby, great progress has been made on multivariate polynomial matrix factorizations.

Let $k[z_1]$ be a principal ideal domain, where k is a field. Then we can construct an efficient algorithm based on elementary transformations to factorize univariate polynomial matrices. The authors in [7, 22] have completely solved the bivariate case by using Hermite Smith reduction over the rational function field of one variable. Although many papers such as [6, 9, 11, 32] have studied the multivariate cases with $n \geq 3$, the factorization problem has been unsolved for almost 30 years. Following Youla and Gnavi's work on the basic structure of multivariate ($n \geq 3$) system theory [32], some factorization theories and algorithms for some classes of multivariate polynomial matrices have been developed.

Charoenlarpnopparut and Bose in [2] first proposed an algorithm for calculating the zero prime matrix factorization of a multivariate polynomial matrix by using the Gröbner bases of modules when all reduced minors of this matrix generate a unit ideal. In some special cases, Lin in [12, 14] solved the problem of zero prime matrix factorization. Meanwhile, Lin and Bose put forward the Lin-Bose's conjecture [15]: the absence of any common zeros in all reduced minors of a matrix is a sufficient condition for the existence of zero prime matrix factorization. This conjecture was proved in [18, 25, 30], which plays an important role in our paper. Furthermore, Fabiańska and Quadrat in [24] demonstrated that the QUILLENSUSLIN package contains the first implementation of Lin-Bose's conjecture (Pommaret's theorem).

In 2005, Wang et.al proposed a method which completely solved the problem of minor prime matrix factorization [31]. Although many results have been achieved on zero or minor matrix factorization, little progress has been made in solving factor prime matrix factorization [19, 20, 29]. Thus, it is

ISSAC '17, July 25-28, 2017, Kaiserslautern, Germany
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5064-8/17/07. . . $15.00
https://doi.org/10.1145/3087604.3087607

essential to propose some new methods to factorize a large class of multivariate polynomial matrices.

The main idea of this paper comes from [16, 17]. Let $\mathbf{C}[\mathbf{z}] = \mathbf{C}[z_1, \dots, z_n]$ be the ring of polynomials in variables $z_1, \dots, z_n$ with coefficients in the complex number field $\mathbf{C}$. Let $F(\mathbf{z})$ be an $l \times m$ $(l \leq m)$ full rank matrix with entries in $\mathbf{C}[\mathbf{z}]$, and $d_l(F)$ be the greatest common divisor of all $l \times l$ minors of $F(\mathbf{z})$. Assuming that $d(\mathbf{z}) = z_1 - f(z_2, \dots, z_n)$ is a divisor of $d_l(F)$, Lin et.al in [16] proved that $F(\mathbf{z})$ has a matrix factorization w.r.t. $d(\mathbf{z})$ when the rank of matrix $F(f, z_2, \dots, z_n)$ is $l-1$ for every $(z_2, \dots, z_n) \in \mathbf{C}^{n-1}$. Moreover, they provided a constructive algorithm for factorizing this class of multivariate polynomial matrices. In [17], Liu et.al focused on the lower order minors of matrices, and proved that the necessary and sufficient condition of $\text{rank}(F(f, z_2, \dots, z_n)) = l - 1$ for every $(z_2, \dots, z_n) \in \mathbf{C}^{n-1}$ is $d(\mathbf{z})$ and all $(l-1) \times (l-1)$ minors of $F(\mathbf{z})$ generate $\mathbf{C}[\mathbf{z}]$. However, there are still many multivariate polynomial matrices that can be factorized without satisfying this condition. This implies that it would be significant to generalize the theorems and algorithms in [16, 17].

Let $\mathbf{R} = k[\mathbf{z}]$ be the set of polynomials in variables $\mathbf{z}$ with coefficients in an arbitrary field k, and $F \in \mathbf{R}^{l \times m}$ be of full rank with $d^r(\mathbf{z}) \mid d_l(F)$, where r is a positive integer. Assume that $d(\mathbf{z})$ and all $(l-r_0) \times (l-r_0)$ minors of F generate $\mathbf{R}$ and $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$, where $1 \leq r_0 < \min\{l, r\}$. The following questions arise: Does $F(\mathbf{z})$ have a matrix factorization w.r.t. $d^{r_0}(\mathbf{z})$? If so, how can we factorize it?

In order to solve the first problem, we propose a factorization theorem to ensure that $F(\mathbf{z})$ can be factorized w.r.t. $d^{r_0}(\mathbf{z})$. Using the proof of factorization theorem, we construct the main algorithm. Two essential steps in the main algorithm are involved to construct a zero left prime matrix and a unimodular matrix. We propose a new sub-algorithm to construct a zero left prime matrix by using Quillen-Suslin theorem, and a unimodular matrix by using the additional information provided by this sub-algorithm. Then the second problem is solved.

This paper is organized as follows. In Section 2, we outline some knowledge about multivariate polynomial matrix factorizations and propose two problems that we shall consider. Theoretical results and generalization are presented in Section 3, which will help us summarize how to factorize multivariate polynomial matrices. The main algorithm is given in Section 4. Two sub-algorithms for constructing a zero left prime matrix and a unimodular matrix are discussed in Section 4.1 and Section 4.2, respectively. In Section 5, we implement all algorithms proposed in this paper, and a simple example is given to illustrate the calculation process of the main algorithm. The conclusions are provided in Section 6.

2 PRELIMINARIES AND PROBLEMS

In the following, we shall denote k a field; $\bar{k}$ an algebraically closed field extension of k; $\mathbf{z}$ the n variables $z_1, \dots, z_n$; $\mathbf{R} = k[\mathbf{z}]$ and $\hat{\mathbf{R}} = k(\mathbf{z})$ the set of polynomials and rational functions in variables $\mathbf{z}$ with coefficients in k respectively; $\mathbf{R}^{l \times m}$ the set of $l \times m$ matrices with entries in $\mathbf{R}$, etc. For a nonzero matrix $F(\mathbf{z}) \in \mathbf{R}^{l \times m}$, let $\text{rank}(F)$ be the rank of $F(\mathbf{z})$. When $l = m$, we use $\det(F)$ to denote the determinant of $F(\mathbf{z})$. For $1 \leq i \leq \text{rank}(F)$, let $d_i(F)$ be the greatest common divisor of all $i \times i$ minors of $F(\mathbf{z})$, with the convention that $d_i(F) := 0$ if $\text{rank}(F) < i$. $f(\mathbf{z}) \mid d_i(F)$ means that $f(\mathbf{z})$ is a factor of $d_i(F)$. Let $I \subseteq \mathbf{R}$ be an ideal, then we call $V(I)$ the affine variety defined by I. Superscript $^{\mathbf{T}}$ denotes transposition.

Throughout this paper, the argument $(\mathbf{z})$ is omitted whenever its omission does not cause confusion, for example, we denote $F(\mathbf{z})$ by F for simplicity. Without loss of generality, the size of a given matrix is assumed to be $l \times m$ with $l \leq m$.

In order to study the factorization of multivariate polynomial matrices, we will review some useful notions and known results which play a central role in multivariate system theory, and then use an example to put forward two problems we are considering.

2.1 Definitions and Important Results

Definition 2.1. Let F be a nonzero matrix in $\mathbf{R}^{l \times m}$, the rank of F is r if there exists an $r \times r$ nonzero minor, and all $i \times i$ $(i > r)$ minors vanish identically.

Definition 2.2. Let $F \in \mathbf{R}^{l \times m}$ be of full rank, then F is said to be a zero left prime (ZLP) matrix, if all $l \times l$ minors of F generate $\mathbf{R}$.

We refer to [32] for more details of the definitions of zero left prime (ZLP) matrix, minor left prime (MLP) matrix and factor left prime (FLP) matrix.

Let W be an $\mathbf{R}$-module with presentation $\mathbf{R}^{1 \times l} \xrightarrow{\phi} \mathbf{R}^{1 \times m} \to W \to 0$, where ϕ is defined by $M \in \mathbf{R}^{l \times m}$. We introduce the concept of the *Fitting ideals* of a finitely presented module over $\mathbf{R}$.

Definition 2.3. (See [5]) With the above notations, the *ith Fitting ideal* $Fitt_i(W)$ of W is the ideal of $\mathbf{R}$ generated by the $(m-i) \times (m-i)$ minors of M, with the conventions that $Fitt_i(W) := 0$ if $m - i > l$, and $Fitt_i(W) := \mathbf{R}$ for $i \geq m$.

Definition 2.4. Let $F \in \mathbf{R}^{l \times m}$ be of full rank, and $h(\mathbf{z}) \mid d_l(F)$. We say that F admits a matrix factorization w.r.t. $h(\mathbf{z})$, if F can be factorized as $F = GF_1$ such that $G \in \mathbf{R}^{l \times l}$, $F_1 \in \mathbf{R}^{l \times m}$, and $\det(G) = h(\mathbf{z})$.

If F_1 is a ZLP matrix in Definition 2.4, then $F = GF_1$ is said to be a ZLP matrix factorization. For simplicity of presentation, we use the following notation [11].

Definition 2.5. Let $F \in \mathbf{R}^{l \times m}$ be of full rank, $a_1, \dots, a_s$ denote all $l \times l$ minors of F. Extracting $d_l(F)$ from a_j yields $a_j = d_l(F) \cdot b_j$, $j = 1, \dots, s$, then $b_1, \dots, b_s$ are called the *reduced minors* of F.

LEMMA 2.6. *Let $\tilde{A} = [\tilde{N}, \tilde{D}]$ and $A = [D^{\mathbf{T}}, N^{\mathbf{T}}]^{\mathbf{T}}$ be of full rank, where $\tilde{N}, N \in \mathbf{R}^{l \times m}$, $\tilde{D} \in \mathbf{R}^{l \times l}$ and $D \in \mathbf{R}^{m \times m}$. Suppose that $\tilde{A}A = 0_{l \times m}$, then* $\det(\tilde{D}) \neq 0 \Leftrightarrow \det(D) \neq 0$.

Lin has proved Lemma 2.6 in [13]. He also showed that reduced minor is an important invariant for multivariate polynomial matrices in [11].

Lemma 2.7. *Assume that* $\tilde{D}^{-1}\tilde{N} = ND^{-1}$, *where* $\tilde{D}^{-1} \in \hat{\mathbf{R}}^{l\times l}$, $D^{-1} \in \hat{\mathbf{R}}^{m\times m}$, $\tilde{N}, N \in \mathbf{R}^{l\times m}$. *Let* $b_1, \ldots, b_t$ *and* $\tilde{b}_1, \ldots, \tilde{b}_t$ *denote all reduced minors of* $[\tilde{N}, \tilde{D}]$ *and* $[D^{\mathbf{T}}, N^{\mathbf{T}}]^{\mathbf{T}}$ *respectively, then* $b_j = \pm\tilde{b}_j$, $j = 1, \ldots, t$, *the sign depends on the index* j.

In 1955, J.P. Serre raised the question whether any finitely generated projective module over a polynomial ring is free. This question, referred to as Serre's conjecture, was proved independently by D. Quillen [26] and A. Suslin [28] in 1976. In 2007, Fabiańska and Quadrat developed a constructive version of the Quillen-Suslin theorem in [24].

Lemma 2.8 (quillen-suslin theorem). *Assume that* $W \in \mathbf{R}^{s\times l}$ *is a ZLP matrix, where* $s < l$. *Then a square unimodular matrix* $U \in \mathbf{R}^{l\times l}$ *can be constructed such that* W *is its first* s *rows.*

A square matrix U is a **unimodular** matrix if and only if $\det(U)$ is a nonzero constant in k. In 2001, Lin and Bose proposed Lin-Bose's conjecture when they considered a generalization of Serre's conjecture in [15]. Before long, Pommaret first solved the Lin-Bose's conjecture in [25].

Lemma 2.9. *Let* $F \in \mathbf{R}^{l\times m}$ *be of full rank, and all reduced minors of* F *generate* $\mathbf{R}$. *Then there exists a ZLP matrix factorization* $F = GF_1$ *such that* $\det(G) = d_l(F)$ *and* F_1 *is a ZLP matrix, where* $G \in \mathbf{R}^{l\times l}$ *and* $F_1 \in \mathbf{R}^{l\times m}$.

2.2 Problems

In the following, the matrix type we consider is as follows: $F \in \mathbf{R}^{l\times m}$ is of full rank, and $d^r(\mathbf{z}) \mid d_l(F)$ with $d(\mathbf{z}) = z_1 - f(z_2, \ldots, z_n)$, where r is a positive integer and f is a polynomial in $k[z_2, \ldots, z_n]$. We first introduce an important result in [17].

Lemma 2.10. *With above notations. If* $d(\mathbf{z})$ *and all* $(l-1)\times(l-1)$ *minors of* F *generate* $\mathbf{C}[\mathbf{z}]$, *then* F *admits a matrix factorization w.r.t.* $d(\mathbf{z})$.

Now we consider the following example. Let

$$F = \begin{bmatrix} z_1^2 - z_1z_2 + z_3^2 - 1 & z_3^2 + z_3 & (z_3+1)^2 \\ z_1z_2 - z_2^2 & z_2z_3 - z_1z_3 & z_2 - z_1 \\ z_3 - 1 & z_3 & z_3 + 1 \end{bmatrix},$$

where $\det(F) = -z_1z_3^2(z_1 - z_2)^2$. Let $d(\mathbf{z}) = z_1 - z_2$, it is easy to verify that $d(\mathbf{z})$ is a common divisor of all 2×2 minors of F. This implies that $d(\mathbf{z})$ and all 2×2 minors of F do not generate $\mathbf{C}[\mathbf{z}]$, so we **cannot** factorize F w.r.t. $d(\mathbf{z})$ by using Lemma 2.10. Nevertheless, F has a matrix factorization $F = GF_1$ w.r.t. $d^2(\mathbf{z})$, where

$$G = \begin{bmatrix} d(\mathbf{z}) & 0 & z_3+1 \\ 0 & d(\mathbf{z}) & 0 \\ 0 & 0 & 1 \end{bmatrix}, F_1 = \begin{bmatrix} z_1 & 0 & 0 \\ z_2 & -z_3 & -1 \\ z_3 - 1 & z_3 & z_3 + 1 \end{bmatrix}.$$

Assume that $d(\mathbf{z})$ and all the $(l-r_0)\times(l-r_0)$ minors of F generate $\mathbf{R}$ and $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$, where $1 \leq r_0 < \min\{l, r\}$. The above example reminds us to consider the following problems: 1. Does F have a matrix factorization w.r.t. $d^{r_0}(\mathbf{z})$? 2. If so, how can we factorize it?

3 THEORETICAL RESULTS

Our task in this section is to solve Problem 1.

3.1 Factorization Theorem

In the following we will show that F can be factorized w.r.t. $d^{r_0}(\mathbf{z})$. Before giving the main factorization theorem, we introduce two lemmas.

Lemma 3.1. *Let* $Q \in \mathbf{R}^{l\times m}$ *and* P *be an* $\mathbf{R}$*-module finitely presented by* Q. *If* $\mathrm{rank}(Q) = l - r_0$ *and* $Fitt_{m-l+r_0}(P) = \mathbf{R}$, *then there is a ZLP matrix* $H \in \mathbf{R}^{r_0\times l}$ *such that* $HQ = 0_{r_0\times m}$.

Proof. We divide our proof into three steps. First, we construct a special $r_0 \times l$ full rank matrix H_0 such that $H_0Q = 0_{r_0\times m}$. In view of $\mathrm{rank}(Q) = l - r_0$, we could assume that the first $(l - r_0)$ row vectors $\vec{q}_1, \ldots, \vec{q}_{l-r_0}$ of Q are $\mathbf{R}$-linear independent. This implies that $\vec{q}_1, \ldots, \vec{q}_{l-r_0}$ and $\vec{q}_{l-r_0+k}$ are $\mathbf{R}$-linear dependent for $1 \leq k \leq r_0$. Thus $\vec{h}_kQ = 0_{1\times m}$ for some row vector $\vec{h}_k = [h_{k1}, \ldots, h_{k(l-r_0)}, 0, \ldots, 0, h_{k(l-r_0+k)}, 0, \ldots, 0] \in \mathbf{R}^{1\times l}$, where $h_{k(l-r_0+k)} \neq 0$. It follows that a full rank matrix $H_0 \in \mathbf{R}^{r_0\times l}$ can be constructed such that $H_0Q = 0_{r_0\times m}$, where

$$H_0 = \begin{bmatrix} h_{11} & \cdots & h_{1(l-r_0)} & h_{1(l-r_0+1)} & & \\ \vdots & \ddots & \vdots & & \ddots & \\ h_{r_01} & \cdots & h_{r_0(l-r_0)} & & & h_{r_0l} \end{bmatrix}.$$

The next thing to do in the proof is to prove that all the reduced minors of H_0 generate $\mathbf{R}$. For simplicity, let $b_1, \ldots, b_\gamma$ denote all $r_0 \times r_0$ reduced minors of H_0, where $\gamma = \binom{l}{r_0}$. Let $Q_1, \ldots, Q_\eta$ denote all $l \times (l - r_0)$ submatrices of Q, and $b_{i1}, \ldots, b_{i\gamma}$ denote all $(l-r_0)\times(l-r_0)$ reduced minors of Q_i, where $1 \leq i \leq \eta$ and $\eta = \binom{m}{l-r_0}$.

Let $H_0 = [H_1, H_2]$, where H_1 is composed of the first $l - r_0$ columns of H_0 and $H_2 = \mathrm{diag}(h_{1(l-r_0+1)}, \ldots, h_{r_0l})$. It is clear that $\det(H_2) \neq 0$. Let $Q_i = [Q_{i1}^{\mathbf{T}}, Q_{i2}^{\mathbf{T}}]^{\mathbf{T}}$, where $Q_{i1} \in \mathbf{R}^{(l-r_0)\times(l-r_0)}$ and $Q_{i2} \in \mathbf{R}^{r_0\times(l-r_0)}$. If Q_i is not of full rank, then $b_{ij} \equiv 0$, $j = 1, \ldots, \gamma$. If Q_i is of full rank, then it follows from $H_0Q = 0_{r_0\times m}$ that

$$[H_1, H_2]\begin{bmatrix} Q_{i1} \\ Q_{i2} \end{bmatrix} = 0_{r_0\times(l-r_0)}. \quad (1)$$

By Lemma 2.6, $\det(Q_{i1}) \neq 0$. From equation (1) we have

$$H_2^{-1}H_1 = -Q_{i1}^{-1}Q_{i2}. \quad (2)$$

According to Lemma 2.7, H_0 and Q_i have the same reduced minors without considering the sign, i.e., $b_j = \pm b_{ij}$, $j = 1, \ldots, \gamma$. Therefore, all $(l-r_0)\times(l-r_0)$ reduced minors of Q are as follows: $\Delta_{11}b_1, \ldots, \Delta_{1\gamma}b_\gamma, \cdots, \Delta_{\eta1}b_1, \ldots, \Delta_{\eta\gamma}b_\gamma$, where $\Delta_{ij} \in \{\pm1, 0\}$. Recalling that $Fitt_{m-l+r_0}(P) = \mathbf{R}$, this implies that all $(l-r_0)\times(l-r_0)$ reduced minors of Q generate $\mathbf{R}$. Hence, we can conclude that $b_1, \ldots, b_\gamma$ must generate $\mathbf{R}$.

Finally, we proceed to prove this lemma. Using Lemma 2.9, there exist matrices $G \in \mathbf{R}^{r_0 \times r_0}$ and $H \in \mathbf{R}^{r_0 \times l}$ such that $H_0 = GH$, where $\det(G) = d_{r_0}(H_0)$ and H is a ZLP matrix. Combining $H_0 Q = 0_{r_0 \times m}$ and $\det(G) \neq 0$, we get $HQ = 0_{r_0 \times m}$. The proof is completed. □

Lemma 3.2. *Let $g(\mathbf{z}) \in \mathbf{R}$ and $f(\mathbf{z}) \in k[z_2, \ldots, z_n]$. Suppose that $g(f, z_2, \ldots, z_n) = 0$, then $z_1 - f(z_2, \ldots, z_n)$ is a divisor of $g(\mathbf{z})$.*

The proof is simple and omitted. Combining Lemma 3.1 and Lemma 3.2, we give a solution to Problem 1.

Theorem 3.3. *Let W be an $\mathbf{R}$-module finitely presented by F and $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$. If $Fitt_{m-l+r_0}(W)$ and $d(\mathbf{z})$ generate $\mathbf{R}$, then F admits a matrix factorization w.r.t. $d^{r_0}(\mathbf{z})$.*

Proof. First, we need to verify that the rank of $F(f, z_2, \ldots, z_n)$ is $l - r_0$. Since $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$ implies that $\langle d(\mathbf{z}) \rangle \supseteq Fitt_{m-l+r_0-1}(W)$, it follows that $\text{rank}(F(f, z_2, \ldots, z_n)) \leq l - r_0$. Let $\hat{W}$ be an $\mathbf{R}$-module finitely presented by $F(f, z_2, \ldots, z_n)$. We assert that $\text{rank}(F(f, z_2, \ldots, z_n))$ cannot be smaller than $l - r_0$. If otherwise, $Fitt_{m-l+r_0}(\hat{W}) = 0$. This implies that $\langle d(\mathbf{z}) \rangle \supseteq Fitt_{m-l+r_0}(W)$, then $Fitt_{m-l+r_0}(W)$ and $d(\mathbf{z})$ do not generate $\mathbf{R}$, which leads to a contradiction.

Second, our task is to claim that $Fitt_{m-l+r_0}(\hat{W}) = \mathbf{R}$. If the assertion would not hold, then there exists a point $\tilde{\mathbf{z}}_1 = (z_{12}, \ldots, z_{1n}) \in \bar{k}^{n-1}$ such that $\tilde{\mathbf{z}}_1 \in V(Fitt_{m-l+r_0}(\hat{W}))$. Let $z_{11} = f(\tilde{\mathbf{z}}_1)$, then $(z_{11}, z_{12}, \ldots, z_{1n})$ is a common zero of $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W)$. This contradicts the fact that $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W)$ generate $\mathbf{R}$.

We finally remark that F has a matrix factorization w.r.t. $d^{r_0}(\mathbf{z})$. Using Lemma 3.1, we get $HF(f, z_2, \ldots, z_n) = 0_{r_0 \times m}$, where $H(z_2, \ldots, z_n)$ is an $r_0 \times l$ ZLP matrix. Meanwhile, according to Quillen-Suslin theorem, it follows that an $l \times l$ unimodular matrix $U(z_2, \ldots, z_n)$ can be constructed such that H is its first r_0 rows. Let $\hat{F} = UF$, then the first r_0 rows of $\hat{F}(f, z_2, \ldots, z_n)$ are zero polynomials. By Lemma 3.2, the first r_0 rows of $\hat{F}$ have the common divisor $d(\mathbf{z})$, i.e., $\hat{F} = \Lambda F_1 =$

$$\begin{bmatrix} d(\mathbf{z}) & & & & \\ & \ddots & & & \\ & & d(\mathbf{z}) & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{bmatrix} \begin{bmatrix} g_{11} & \cdots & g_{1m} \\ \vdots & \ddots & \vdots \\ g_{r_0 1} & \cdots & g_{r_0 m} \\ g_{(r_0+1)1} & \cdots & g_{(r_0+1)m} \\ \vdots & \ddots & \vdots \\ g_{l1} & \cdots & g_{lm} \end{bmatrix},$$

where $g_{ij} \in \mathbf{R}$ and $\Lambda = \text{diag}(d(\mathbf{z}), \ldots, d(\mathbf{z}), 1, \ldots, 1)$ with $\det(\Lambda) = d^{r_0}(\mathbf{z})$. Consequently, we can now derive the factorization of F w.r.t. $d^{r_0}(\mathbf{z})$: $F = GF_1$, where $G = U^{-1}\Lambda$. □

Remark 1. *When $r_0 = 1$, Cluzeau and Quadrat proved the above theorem by using module theory in [3] (see pages 85-86). When $r_0 > 1$, Theorem 3.3 is an extension of the result in [3]. Our proof is based on matrix computation and control theory, which is different from module theory method in [3].*

3.2 Generalization

Let $d_k(\mathbf{z})$ denote the multivariate polynomial $z_k - h(z_1, \ldots, z_{k-1}, z_{k+1}, \ldots, z_n)$, where $1 \leq k \leq n$ and h is a polynomial in $k[z_1, \ldots, z_{k-1}, z_{k+1}, \ldots, z_n]$. Similar to the proof of Theorem 3.3, we can obtain the following corollary.

Corollary 3.4. *Let W be an $\mathbf{R}$-module finitely presented by F and $d_{ks}(\mathbf{z}) \mid d_{l-r_0+1}(F)$. If $Fitt_{m-l+r_0}(W)$ and $d_k(\mathbf{z})$ generate $\mathbf{R}$, then F admits a matrix factorization w.r.t. $d_k^{r_0}(\mathbf{z})$.*

When $r_0 = 1$, the authors in [17] proved that F has a matrix factorization w.r.t. $d^r(\mathbf{z})$ by r successive decompositions if $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W)$ generate $\mathbf{R}$. But how about the case when $r_0 > 1$ and $r_0 \mid r$?

Assume that $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W)$ generate $\mathbf{R}$ and $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$. Does F admit a matrix factorization w.r.t. $d^r(\mathbf{z})$ by $\frac{r}{r_0}$ successive decompositions?

Let $F_0 = F$. According to Theorem 3.3, there exist $G_0 \in \mathbf{R}^{l \times l}$ and $F_1 \in \mathbf{R}^{l \times m}$ such that $F_0 = G_0 F_1$, where $\det(G_0) = d^{r_0}(\mathbf{z})$. This implies that $d^{r-r_0}(\mathbf{z}) \mid d_l(F_1)$, so we can continue to factorize $F_1(\mathbf{z})$ w.r.t. $d^{r_1}(\mathbf{z})$ by using the same method, where $1 \leq r_1 < \min\{l, r - r_0\}$.

Proposition 3.5. *With the above notations and assuming that $d(\mathbf{z}) \mid d_{l-r_0+1}(F_1)$, then F_1 admits a matrix factorization w.r.t. $d^{r_0}(\mathbf{z})$.*

Proof. Let W_1 be an $\mathbf{R}$-module finitely presented by F_1. This proposition will be proved by showing that $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W_1)$ generate $\mathbf{R}$. If the statement would not hold, then $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W_1)$ have a common zero $\hat{\mathbf{z}}_0 \in \bar{k}^n$. Let $\hat{\mathbf{z}}_0 = (z_{01}, z_{02}, \ldots, z_{0n})$, where $z_{01} = f(z_{02}, \ldots, z_{0n})$. From $F_0(\hat{\mathbf{z}}_0) = G_0(\hat{\mathbf{z}}_0) F_1(\hat{\mathbf{z}}_0)$ we have that $\hat{\mathbf{z}}_0$ is a common zero of $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W)$, this contradicts the fact that $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W)$ generate $\mathbf{R}$. Thus, F_1 admits a matrix factorization w.r.t. $d^{r_0}(\mathbf{z})$: $F_1 = G_1 F_2$, where $G_1 \in \mathbf{R}^{l \times l}$, $F_2 \in \mathbf{R}^{l \times m}$ and $\det(G_1) = d^{r_0}(\mathbf{z})$. □

Using Proposition 3.5, it is not difficult to derive the following conclusion.

Corollary 3.6. *With the above notations and assuming that $d(\mathbf{z}) \mid d_{l-r_0+1}(F_i)$ for every $1 \leq i \leq \frac{r}{r_0} - 1$, then F_0 admits a matrix factorization w.r.t. $d^r(\mathbf{z})$ by $\frac{r}{r_0}$ successive decompositions, where F_i satisfies $F_{i-1} = G_{i-1} F_i$ for some $G_{i-1} \in \mathbf{R}^{l \times l}$ with $\det(G_{i-1}) = d^{r_0}(\mathbf{z})$ and $F_i \in \mathbf{R}^{l \times m}$.*

Let W_i $(1 \leq i \leq \frac{r}{r_0} - 1)$ be an $\mathbf{R}$-module finitely presented by F_i. Applying Corollary 3.6 to F_i, we do not need to verify whether or not $d(\mathbf{z})$ and $Fitt_{m-l+r_0}(W_i)$ generate $\mathbf{R}$. This implies that we can avoid some unnecessary computations during the decomposition process.

4 ALGORITHMS

The aim of this section is to solve Problem 2. With the help of Lemma 3.1 and Theorem 3.3, we can now get the following algorithm.

```
Algorithm 1: MF algorithm
Input  : $F \in \mathbf{R}^{l\times m}$ be of full rank, where $d^r(\mathbf{z}) \mid d_l(F)$
         and $d(\mathbf{z}) = z_1 - f(z_2, \ldots, z_n)$.
Output : the factorization of $F$ w.r.t. $d^{r_0}(\mathbf{z})$.
begin
    1. find $r_0$ such that $d(\mathbf{z})$ and all $(l-r_0)\times(l-r_0)$
       minors of $F$ generate $\mathbf{R}$ and $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$.
    if $r_0$ does not exist then
        return this method cannot factorize $F$;
    else
        2. construct an $r_0 \times l$ ZLP matrix $H(z_2, \ldots, z_n)$
           such that $HF(f, z_2, \ldots, z_n) = 0_{r_0\times m}$;
        3. construct an $l \times l$ unimodular matrix
           $U(z_2, \ldots, z_n)$ such that $H$ is its first $r_0$ rows;
        4. compute $F_1 \in \mathbf{R}^{l\times m}$ such that $UF = \Lambda F_1$,
           where $\Lambda = \mathrm{diag}(d(\mathbf{z}), \ldots, d(\mathbf{z}), 1, \ldots, 1)$ with
           $\det(\Lambda) = d^{r_0}(\mathbf{z})$;
        return $F = GF_1$, where $G = U^{-1}\Lambda$.
```

When $r_0 = 1$, our algorithm is the same as the algorithm in [16]. When $1 < r_0 < \min\{l, r\}$, more multivariate polynomial matrices can be factorized by using the **MF** algorithm. This implies that we extend previous algorithm to a larger range. Before proceeding further, let us remark on the **MF** algorithm.

(1) When $r_0 > 1$, it is difficult to construct a ZLP matrix H. Although Wang and Kwong in [31] used a method which is based on a basis of a free module to obtain H and Fabiańska and Quadrat get H by implementing the Lin-Bose's conjecture in [24], we will propose a new method to construct H, with details being presented in Section 4.1.

(2) There are many methods to construct an $l \times l$ unimodular matrix U [21, 23, 24]. Nevertheless, we construct U by using the auxiliary information provided by the algorithm in Section 4.1. See Section 4.2 for more details.

We are now in a position to construct an $r_0 \times l$ ZLP matrix H and an $l \times l$ unimodular matrix U. In the following subsections, we first propose a new algorithm to construct H in which some additional information will be given, then construct U by using these information.

4.1 Constructing a ZLP Matrix

Without loss of generality, we may assume $r_0 > 1$. From the proof of Lemma 3.1, we first compute an $r_0 \times l$ matrix $H_0(z_2, \ldots, z_n)$ such that $H_0F(f, z_2, \ldots, z_n) = 0_{r_0\times m}$, where the reduced minors of H_0 generate $\mathbf{R}$. Next, we get a ZLP matrix H by factorizing H_0. Proceeding as the construction of H_0 in Lemma 3.1, it is easy to calculate H_0. Therefore, this subsection focuses on how to obtain H by factorizing H_0. In order to propose our new algorithm for constructing H, we need to introduce two new symbols for simplicity of presentation and two important lemmas for proving our main result.

Let $\mathrm{Syz}_R(F)$ denote the right syzygy module of F consisting of linear relations over $\mathbf{R}$ among the column vectors of F: $\mathrm{Syz}_R(F) = \{\vec{q} \in \mathbf{R}^{m\times 1} \mid F\vec{q} = 0_{l\times 1}\}$. Similarly, let $\mathrm{Syz}_L(F)$ denote the left syzygy module of F, i.e., $\mathrm{Syz}_L(F) = \{\vec{p} \in \mathbf{R}^{1\times l} \mid \vec{p}F = 0_{1\times m}\}$.

Lemma 4.1. *Let $P \in \mathbf{R}^{r_0\times l}$ be of full row rank. If $P = GP_1$ for some $G \in \mathbf{R}^{r_0\times r_0}$ and $P_1 \in \mathbf{R}^{r_0\times l}$, then $\mathrm{Syz}_R(P) = \mathrm{Syz}_R(P_1)$.*

This is a very powerful lemma, and the proof can be found in [13]. The following lemma is an important consequence from Quillen-Suslin theorem.

Lemma 4.2. *Let $W \in \mathbf{R}^{s\times l}$ be a ZLP matrix with $s < l$. Then $\mathrm{Syz}_R(W)$ is a free module of rank $(l-s)$ over $\mathbf{R}$.*

Proof. According to Quillen-Suslin theorem, it follows that a $l\times l$ unimodular matrix U can be constructed such that W is its first s rows. This implies that there is an invertible matrix $V \in \mathbf{R}^{l\times l}$ satisfying $UV = I_{l\times l}$. Let $B \in \mathbf{R}^{l\times s}$ consist of the first s columns of V, then $WB = I_{s\times s}$.

Considering an $\mathbf{R}$-module homomorphism ϕ: $\mathbf{R}^{l\times 1} \to \mathbf{R}^{s\times 1}$ with $\phi(\vec{q}) = W\vec{q}$ for all $\vec{q} \in \mathbf{R}^{l\times 1}$. Obviously, ϕ is a surjective, as $\phi(B\vec{p}) = WB\vec{p} = \vec{p}$ for all $\vec{p} \in \mathbf{R}^{s\times 1}$. We can construct the following short exact sequence: $0 \to \mathrm{Ker}(\phi) \to \mathbf{R}^{l\times 1} \xrightarrow{\phi} \mathbf{R}^{s\times 1} \to 0$. If we can prove this sequence is split, then the lemma follows immediately. We define another $\mathbf{R}$-module homomorphism φ: $\mathbf{R}^{s\times 1} \to \mathbf{R}^{l\times 1}$ by $\varphi(\vec{p}) = B\vec{p}$ for all $\vec{p} \in \mathbf{R}^{s\times 1}$. Then $\phi \cdot \varphi = 1_{\mathbf{R}^{s\times 1}}$ implies that the above sequence is split. Therefore, $\mathbf{R}^{l\times 1} = \mathbf{R}^{s\times 1} \oplus \mathrm{Ker}(\phi)$. In view of $\mathrm{Syz}_R(W) = \mathrm{Ker}(\phi)$, we get that $\mathrm{Syz}_R(W)$ is a free module of rank $(l-s)$ over $\mathbf{R}$. □

Now we prove the main result for calculating H.

Theorem 4.3. *Let $H_0 \in \mathbf{R}^{r_0\times l}$ be of full row rank, and the reduced minors of H_0 generate $\mathbf{R}$. If $W \in \mathbf{R}^{l\times(l-r_0)}$ is composed of a basis in $\mathrm{Syz}_R(H_0)$, then W is a ZLP matrix. Moreover, let $H \in \mathbf{R}^{r_0\times l}$ consist of a basis in $\mathrm{Syz}_L(W)$, then H_0 has a matrix factorization $H_0 = GH$ such that $G \in \mathbf{R}^{r_0\times r_0}$ and H is a ZLP matrix.*

Proof. By Lemma 2.9, we have $H_0 = G_1H_1$, where $G_1 \in \mathbf{R}^{r_0\times r_0}$ and $H_1 \in \mathbf{R}^{r_0\times l}$ is a ZLP matrix. Then Lemma 4.1 easily implies that $\mathrm{Syz}_R(H_0) = \mathrm{Syz}_R(H_1)$. According to Lemma 4.2, it follows that $\mathrm{Syz}_R(H_0)$ is a free module of rank $(l-r_0)$ over $\mathbf{R}$.

For simplicity, we may take $\vec{w}_1(\mathbf{z}), \ldots, \vec{w}_{l-r_0}(\mathbf{z})$ as a basis of $\mathrm{Syz}_R(H_0)$, where $\vec{w}_i(\mathbf{z}) \in \mathbf{R}^{l\times 1}$ and $1 \le i \le l - r_0$. Let $W = [\vec{w}_1(\mathbf{z}), \ldots, \vec{w}_{l-r_0}(\mathbf{z})]$, then $H_0W = 0_{r_0\times(l-r_0)}$. By Lemma 2.7, the reduced minors of W generate $\mathbf{R}$. We claim that W is a ZLP matrix. If otherwise, then there exist matrices $G_2 \in \mathbf{R}^{(l-r_0)\times(l-r_0)}$ and $W_1 \in \mathbf{R}^{l\times(l-r_0)}$ such that

$$W = W_1G_2, \tag{3}$$

where $\det(G_2) = d_{l-r_0}(W) \in \mathbf{R} \setminus k$ and W_1 is a ZLP matrix. Since $H_0W = 0_{r_0\times(l-r_0)}$ and $\det(G_2) \neq 0$, it can easily be verified that $H_0W_1 = 0_{r_0\times(l-r_0)}$. Consequently, every column vector of W_1 is in $\mathrm{Syz}_R(H_0)$, and there exists a matrix $G_3 \in \mathbf{R}^{(l-r_0)\times(l-r_0)}$ such that

$$W_1 = WG_3. \tag{4}$$

By substituting Eq.(3) into Eq.(4), we obtain

$$I_{(l-r_0)\times(l-r_0)} = G_2G_3. \tag{5}$$

It follows from Eq.(5) that G_2 and G_3 are unimodular matrices, which leads to a contradiction.

Notice that $\mathrm{Syz}_L(W)$ is a free module of rank r_0 over $\mathbf{R}$, there exists a basis $\vec{h}_1(\mathbf{z}), \ldots, \vec{h}_{r_0}(\mathbf{z})$ of $\mathrm{Syz}_L(W)$, where $\vec{h}_j(\mathbf{z}) \in \mathbf{R}^{1\times l}$ and $1 \leq j \leq r_0$. Let $H \in \mathbf{R}^{r_0\times l}$ consist of these row vectors, then H is a ZLP matrix. As $H_0 \in \mathrm{Syz}_L(W)$, there exists a matrix $G \in \mathbf{R}^{r_0\times r_0}$ such that $H_0 = GH$. □

Remark 2. *In Theorem 4.3, we need to compute a basis of a free module over $k[\mathbf{z}]$. Fabiańska and Quadrat in [24] proposed a general algorithm for computing bases of a free module by using some kind of heuristic, and first gave a Maple package QUILLENSUSLIN [27] which performs basis computation of free modules over $k[\mathbf{z}]$ with rational and integer coefficients. When k is another field such as a finite field, our strategies are that we first compute a standard basis of a free module, next use a criterion which is proposed in [10] (see Corollary 3.1.12, page 154) to reduce redundant elements from the standard basis, then we get a minimal standard basis. If the number of elements of the minimal standard basis is equal to that of a basis, then we obtain a basis of a free module; otherwise, further research needs to be done.*

For simplicity, we call a matrix consisting of a basis of $\mathrm{Syz}_R(H_0)$ (or $\mathrm{Syz}_L(W)$) as a **generating matrix**. According to Theorem 4.3, we get the following algorithm:

Algorithm 2: ZLP algorithm

```
Input  : $H_0 \in \mathbf{R}^{r_0\times l}$, has a ZLP matrix factorization.
Output : two generating matrices $W \in \mathbf{R}^{l\times(l-r_0)}$ and
         $H \in \mathbf{R}^{r_0\times l}$.
begin
    1. calculate a generating matrix $W$ of $\mathrm{Syz}_R(H_0)$;
    2. compute $d_{r_0}(H_0)$ of $H_0$;
    if $d_{r_0}(H_0)$ is a nonzero constant then
        let $H = H_0$;
    else
        compute a generating matrix $H$ of $\mathrm{Syz}_L(W)$;
    return $W$ and $H$.
```

Remark 3. *The Maple package QUILLENSUSLIN has implemented the Lin-Bose's conjecture and basis computation, but with the increase in the size of multivariate polynomial matrices, we cannot get a ZLP matrix or a basis of a free module in a considerable amount of time. Therefore, we implement the* **ZLP** *algorithm over $k[\mathbf{z}]$ with coefficients in a finite field for avoiding the phenomenon of coefficient expansion in the computation process.*

We randomly generate a number of different order matrices with all reduced minors generating the unit ideal $\mathbf{R}$, and all the polynomials in the matrices are taken from the polynomial ring $\mathbf{R} = \mathbf{F}_{32003}[z_1, z_2, z_3]$, where $\mathbf{F}_{32003}$ is a finite field. We implement the **ZLP** algorithm on the computer algebra system *Singular*, and compare our algorithm with the algorithm in [31]. All the timings in the following table are the average for computing 10 randomly generated examples running on a computer with Intel Core i7-4790 CPU(3.60GHz) and 4GB memories, operated by Windows 7.

Table 1: Timings (msec)

Order	New algorithm	Old algorithm
$(3,8)$	11	23
$(4,8)$	16	85
$(5,10)$	35	239
$(5,11)$	42	430
$(5,12)$	87	618
$(5,13)$	135	892
$(6,12)$	138	2000
$(7,12)$	207	4636
$(8,12)$	529	6957
$(9,12)$	2041	13338
$(10,13)$	3897	17979
$(11,14)$	7269	49437

As indicated in Table 1, we find that our algorithm is faster than the algorithm in [31]. This is because Wang and Kwong need to calculate a basis of the syzygy of a matrix with size $l\times(r_0+l)$, but we decompose the method of computing a basis of the syzygy of a large matrix into the method of computing two bases of the syzygies of two small matrices with size $r_0 \times l$ and $(l - r_0) \times l$.

We also test ten more examples. The numbers of columns of the matrices in the examples are fixed on 15, and the numbers of the rows are from 2 to 11. The following figure shows that our algorithm is more efficient when the number of rows becomes larger.

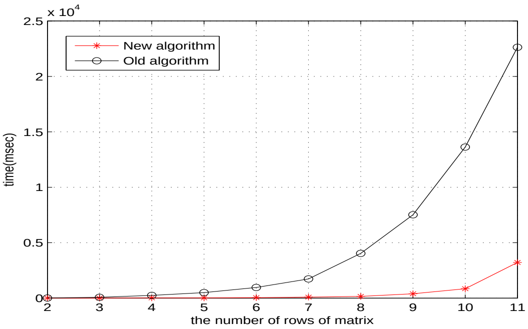

Figure 1: The timings between two algorithms.

4.2 Constructing a Unimodular Matrix

In this subsection, we first give a detailed algorithm for constructing a unimodular matrix by combining the **ZLP** algorithm, then we prove the correctness of our algorithm.

Algorithm 3: Unimodular algorithm

```
Input : an $r_0 \times l$ ZLP matrix $H$ and an $l \times (l - r_0)$
        ZLP matrix $W$ which satisfy $HW = 0$.
Output: an $l \times l$ unimodular matrix $V$.
begin
    1. calculate a matrix $B \in \mathbf{R}^{l \times r_0}$, such that
       $HB = I_{r_0 \times r_0}$;
    return $V = [B, W]$, is a unimodular matrix.
```

THEOREM 4.4. *Let $H \in \mathbf{R}^{r_0 \times l}$ be a ZLP matrix, then we can obtain a unimodular matrix $V \in \mathbf{R}^{l \times l}$ by using the* **unimodular** *algorithm, and H is the first r_0 rows of V^{-1}.*

PROOF. The theorem will be proved if we show the column vectors of V can span a free module $\mathbf{R}^{l \times 1}$. Denote the submodule generated by the columns of B and W by $\rho(B)$ and $\rho(W)$, respectively. First, we consider the following short exact sequence: $0 \to \mathrm{Ker}(\sigma) \to \mathbf{R}^{l \times 1} \xrightarrow{\sigma} \mathbf{R}^{r_0 \times 1} \to 0$, where σ: $\mathbf{R}^{l \times 1} \to \mathbf{R}^{r_0 \times 1}$ is an $\mathbf{R}$-module homomorphism with $\sigma(\vec{q}) = H\vec{q}$ for all $\vec{q} \in \mathbf{R}^{l \times 1}$. Due to the fact H is a ZLP matrix and W is a generating matrix of $\mathrm{Syz}_{\mathbf{R}}(H)$, it follows that $\mathbf{R}^{l \times 1} = \mathbf{R}^{r_0 \times 1} \oplus \rho(W)$.

Second, we define another $\mathbf{R}$-module homomorphism π: $\mathbf{R}^{r_0 \times 1} \to \mathbf{R}^{l \times 1}$ by $\pi(\vec{p}) = B\vec{p}$ for any $\vec{p} \in \mathbf{R}^{r_0 \times 1}$. It is not difficult to verify that π is injective since B is a full column rank matrix. This implies that $\rho(B)$ spans the submodule $\mathrm{Im}(\pi)$. Noting that $\mathbf{R}^{r_0 \times 1} \cong \mathrm{Im}(\pi)$, we have $\mathbf{R}^{l \times 1} \cong \rho(B) \oplus \rho(W)$. Consequently, V is a unimodular matrix.

Let $U \in \mathbf{R}^{l \times l}$ be the invertible matrix of V, then $H = HVU = H[B, W]U = [I_{r_0 \times r_0}, 0_{r_0 \times (l - r_0)}]U$. Therefore, H is the first r_0 rows of V^{-1}. □

It follows from the **Unimodular** algorithm that the **ZLP** algorithm provides two pieces of information for constructing a unimodular matrix: a ZLP matrix H and a generating matrix W of $\mathrm{Syz}_{\mathbf{R}}(H)$.

With the help of the **ZLP** algorithm and the **Unimodular** algorithm, we can now factorize F w.r.t. $d^{r_0}(\mathbf{z})$ by using the **MF** algorithm. This implies that Problem 2 is solved.

5 IMPLEMENTATION AND EXAMPLE

We implement our algorithms presented in this paper on the computer algebra system *Singular*. The codes and a simple example are available on the web:

http://www.mmrc.iss.ac.cn/~dwang/software.html

We first discuss our implementation in Section 5.1. Then a simple example is presented to illustrate how our algorithms factorize a multivariate polynomial matrix in section 5.2.

5.1 Implementation

We implement all algorithms on *Singular* for the following reasons:

(1) In the **MF** algorithm, we need to construct a ring homomorphism: $k[\mathbf{z}] \to k[\mathbf{z}]/d(\mathbf{z})$. We can use the command "map" to set up arbitrary ring maps.

(2) In the **Unimodular** algorithm, we need to compute a matrix B such that $HB = I_{r_0 \times r_0}$. This problem is equivalent to a lifting homomorphism problem in [4] (see Problem 4.1, page 129). The *Singular* command "lift" can help us quickly obtain B.

5.2 A Simple Example

Consider the matrix $F(z_1, z_2, z_3) =$

$$\begin{bmatrix} z_2^2-2z_1z_2+z_1-4z_2+4 & z_1z_2-z_1^2-z_2-z_1+2 & z_1 \\ z_1^2-z_1z_2-z_1z_3+3z_1-3z_2-3z_3 & z_1-z_2+2 & z_2+z_3-z_1 \\ z_1^2-z_2^2+z_1z_2-z_1z_3+z_1+z_2-3z_3-7 & z_1^2-z_1z_2+2z_1 & z_2+z_3-2z_1+1 \end{bmatrix}^{\mathbf{T}}$$

with $\det(F) = (z_1 - z_2 + 2)^3$. Let $f(z_2, z_3) = z_2 - 2$ and $d(\mathbf{z}) = z_1 - f(z_2, z_3)$. We will factorize F according to the **MF** algorithm.

Step 1. We need to find r_0 such that $d(\mathbf{z})$ and all $(l - r_0) \times (l - r_0)$ minors of F generate $\mathbf{R}$ and $d(\mathbf{z}) \mid d_{l-r_0+1}(F)$. Since $d(\mathbf{z})$ is a common divisor of all 2×2 minors of F, it follows that $d(\mathbf{z})$ and all 2×2 minors of F do not generate $\mathbf{R}$. This implies that F cannot be factorized w.r.t. $d(\mathbf{z})$ by using Lemma 2.10. Note that the Gröbner basis of the ideal generated by $\{z_1, z_2 + z_3 - 2z_1 + 1, z_1 - z_2 + 2, z_2 - z_1 + z_3\}$ is $\mathbf{R}$, which implies all 1×1 minors of F and $d(\mathbf{z})$ generate $\mathbf{R}$. Thus $r_0 = 2$, and we can use the **MF** algorithm to factorize F w.r.t. $d^{r_0}(\mathbf{z})$.

Step 2. We construct a 2×3 ZLP matrix $H(z_2, z_3)$ such that $HF(f, z_2, z_3) = 0_{2\times3}$. Substituting $f(z_2, z_3)$ for z_1 in F, we have $F(f, z_2, z_3) =$

$$\begin{bmatrix} -(z_2+1)(z_2-2) & -(z_2+1)(z_3+2) & -(z_2+1)(z_3-z_2+5) \\ 0 & 0 & 0 \\ z_2-2 & z_3+2 & z_3-z_2+5 \end{bmatrix}.$$

It is not difficult to compute two $\mathbf{R}$-linear independent row vectors of $\mathrm{Syz}_L(F(f, z_2, z_3))$, they are $\vec{q}_1 = [1, 0, z_2 + 1]$, $\vec{q}_2 = [0, 1, 0]$. Let $H(z_2, z_3) = [\vec{q}_1^{\mathbf{T}}, \vec{q}_2^{\mathbf{T}}]^{\mathbf{T}}$. It follows from all 2×2 minors of H generating $\mathbf{R}$ that H is a ZLP matrix. Thus H satisfies the above requirements.

Step 3. we can construct a 3×3 unimodular matrix $U(z_2, z_3)$ such that $H(z_2, z_3)$ is its first 2 rows. Using the **ZLP** algorithm, we can get a generating matrix of $\mathrm{Syz}_{\mathbf{R}}(H)$: $W = [-z_2 - 1, 0, 1]^{\mathbf{T}}$. According to the **Unimodular** algorithm, we obtain $B = \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right]^{\mathbf{T}}$ by calculating the equation $HB = I_{2\times2}$. Let $V = [B, W]$, then $U = V^{-1}$.

Step 4. Extracting $d(\mathbf{z})$ from the first 2 rows of UF, we get $UF = \Lambda_1 F_1$, where $\Lambda_1 = \mathrm{diag}(d(\mathbf{z}), d(\mathbf{z}), 1)$ and $F_1 =$

$$\begin{bmatrix} 2-z_2 & z_1-z_2-z_3 & z_1-z_3-3 \\ 1-z_1 & 1 & z_1 \\ z_1 & z_2+z_3-z_1 & z_2+z_3-2z_1+1 \end{bmatrix}.$$

Step 5. Recall the **MF** algorithm to factorize F_1 w.r.t. $d(\mathbf{z})$. Since $d(\mathbf{z})$ and all 2×2 minors of F_1 generate $\mathbf{R}$, we can construct a ZLP vector $w(z_2, z_3) = [1, 0, 1]$ such that $wF_1(f, z_2, z_3) = 0_{1\times3}$. Consequently, there exists a 3×3

unimodular matrix $U_1(z_2, z_3) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ such that $U_1 F_1 = \Lambda_2 F_2$, where $\Lambda_2 = \mathrm{diag}(d(\mathbf{z}), 1, 1)$ and $F_2 =$

$$\begin{bmatrix} 1 & 0 & -1 \\ 1-z_1 & 1 & z_1 \\ z_1 & z_2-z_1+z_3 & z_2-2z_1+z_3+1 \end{bmatrix}.$$

Combining **Step 4** and **Step 5**, we conclude that the factorization of F w.r.t. $d^3(\mathbf{z})$ is

$$\begin{bmatrix} d^2(\mathbf{z}) & 0 & -z_1-3 \\ 0 & d(\mathbf{z}) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 1-z_1 & 1 & z_1 \\ z_1 & z_2-z_1+z_3 & z_2-2z_1+z_3+1 \end{bmatrix}.$$

6 CONCLUSIONS

We have studied the problems of multivariate polynomial matrix factorization following the ideas from [16, 17]. First, the matrix factorization theorem and the main algorithm are presented in this paper such that the application range of the method proposed in [16, 17] has been greatly extended. Second, the **ZLP** algorithm is more efficient than the previous algorithm in [31]. Moreover, this new sub-algorithm provides more information for constructing a unimodular matrix, which is impossible for the previous algorithm. A point that should be stressed is that the idea of the **ZLP** algorithm can be applied to many other places, such as solving the null-space basis of a high-order univariate polynomial matrix.

Although we have considered $d(\mathbf{z}) = z_1 - f(z_2, \ldots, z_n)$, it would be interesting to investigate the factorizations of polynomial matrices w.r.t. different forms of $d(\mathbf{z})$. We hope that the results of this paper will motivate new progress in this important research topic.

ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China (Grant No. 11371356), and the Chinese Universities Scientific Fund (Grant No. 2017QC061). The authors would like to thank professor J. Liu for helpful discussions and anonymous referees for detailed suggestions on the paper which have made it more readable.

REFERENCES

[1] N. K. Bose. 1995. *Multidimensional Systems Theory and Applications.* Springer Netherlands.

[2] C. Charoenlarpnopparut and N. K. Bose. 1999. Multidimensional FIR filter bank design using Grobner bases. *IEEE Transactions on Circuits and Systems II Analog and Digital Signal Processing* 46, 12 (1999), 1475–1486.

[3] Thomas Cluzeau and Alban Quadrat. 2015. A new insight into Serre's reduction problem. *Linear Algebra and Its Applications* 483 (2015), 40–100.

[4] Wolfram Decker and Christoph Lossen. 2006. *Computing in Algebraic Geometry.* Algorithms and Computation in Mathematics, Vol. 16. Springer Berlin Heidelberg.

[5] David Eisenbud. 1995. *Commutative Algebra: With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics, Vol. 150. Springer-Verlag.

[6] Ettore Fornasini and Maria Elena Valcher. 1997. n-D Polynomial Matrices with Applications to Multidimensional Signal Analysis. *Multidimensional Systems and Signal Processing* 8, 4 (1997), 387–408.

[7] J. Guiver and N. Bose. 1982. Polynomial matrix primitive factorization over arbitrary coefficient field and related results. *IEEE Transactions on Circuits and Systems* 29, 10 (1982), 649–657.

[8] Thomas Kailath. 1980. *Linear systems.* Vol. 156. Prentice-Hall Englewood Cliffs, NJ.

[9] Sigurd Kleon and Ulrich Oberst. 1999. Transfer Operators and State Spaces for Discrete Multidimensional Linear Systems. *Acta Applicandae Mathematicae* 57, 1 (1999), 1–82.

[10] Martin Kreuzer and Lorenzo Robbiano. 2000. *Computational Commutative Algebra 1.* Springer Berlin.

[11] Zhiping Lin. 1988. On matrix fraction descriptions of multivariable linear n-D systems. *IEEE Transactions on Circuits and Systems* 35, 10 (1988), 1317–1322.

[12] Zhiping Lin. 1999. Notes on n-D Polynomial Matrix Factorizations. *Multidimensional Systems and Signal Processing* 10, 4 (1999), 379–393.

[13] Zhiping Lin. 1999. On syzygy modules for polynomial matrices. *Linear Algebra and Its Applications* 298, 1-3 (1999), 73–86.

[14] Zhiping Lin. 2001. Further Results on n-D Polynomial Matrix Factorizations. *Multidimensional Systems and Signal Processing* 12, 2 (2001), 199–208.

[15] Zhiping Lin and N. K. Bose. 2001. A generalization of Serre's conjecture and some related issues. *Linear Algebra and Its Applications* 338, 1 (2001), 125–138.

[16] Zhiping Lin, Jiang Qian Ying, and Li Xu. 2001. Factorizations for n-D polynomial matrices. *Circuits, Systems, and Signal Processing* 20, 6 (2001), 601–618.

[17] J. Liu, D. Li, and M. Wang. 2011. On General Factorizations for n-D Polynomial Matrices. *Circuits Systems and Signal Processing* 30, 3 (2011), 553–566.

[18] J. Liu, D. Li, and L. Zheng. 2014. The Lin-Bose Problem. *Circuits and Systems II Express Briefs IEEE Transactions on* 61, 1 (2014), 41–43.

[19] J. Liu and M. Wang. 2010. Notes on factor prime factorizations for n-D polynomial matrices. *Multidimensional Systems and Signal Processing* 21, 1 (2010), 87–97.

[20] Jinwang Liu and Mingsheng Wang. 2015. Further remarks on multivariate polynomial matrix factorizations. *Linear Algebra and Its Applications* 465, 465 (2015), 204–213.

[21] Alessandro Logar and Bernd Sturmfels. 1992. Algorithms for the Quillen-Suslin theorem. *Journal of Algebra* 145, 1 (1992), 231–239.

[22] M. Morf, B. C. Levy, and Sun Yuan Kung. 1977. New results in 2-D systems theory, part I: 2-D polynomial matrices, factorization, and coprimeness. *Proc. IEEE* 65, 6 (1977), 861–872.

[23] HyungJu Park. 1995. *A computational theory of Laurent polynomial rings and multidimensional FIR systems.* Ph.D. Dissertation. UNIVERSITY of CALIFORNIA at BERKELEY.

[24] Hyungju Park and Georg Regensburger. 23-106, 2007. *Gröbner Bases in Control Theory and Signal Processing.* Radon Series on Computational and Applied Mathematics, Vol. 3. De Gruyter.

[25] J. F Pommaret. 2001. Solving Bose conjecture on linear multidimensional systems. In *Control Conference (ECC), 2001 European.* IEEE, Porto, Portugal, 1653–1655.

[26] Daniel Quillen. 1976. Projective modules over polynomial rings. *Inventiones mathematicae* 36, 1 (1976), 167–171.

[27] Package QuillenSuslin. 2007. A Maple implementation of a constructive version of the Quillen-Suslin Theorem. https://wwwb.math.rwth-aachen.de/QuillenSuslin/. (2007).

[28] A. A. Suslin. 1976. Projective modules over polynomial rings. *Inventiones Mathematicae* 36, 1 (1976), 167–171.

[29] M. Wang. 2007. On factor prime factorization for n-D polynomial matrices. *IEEE Transactions on Circuits and Systems* 54, 6 (2007), 1398–1405.

[30] M. Wang and D. Feng. 2004. On Lin-Bose problem. *Linear Algebra and Its Applications* 390, 1 (2004), 279–285.

[31] M. Wang and C. P. Kwong. 2005. On multivariate polynomial matrix factorization problems. *Mathematics of Control, Signals, and Systems* 17, 4 (2005), 297–311.

[32] D. Youla and G. Gnavi. 1979. Notes on n-dimensional System Theory. *IEEE Transactions on Circuits and Systems* 26, 2 (1979), 105–111.