J Syst Sci Complex (2023) 36: 77–95

New Results on the Equivalence of Bivariate Polynomial Matrices*

ZHENG Xiaopeng · LU Dong · WANG Dingkang · XIAO Fanghui

DOI: 10.1007/s11424-023-1304-z
Received: 17 August 2021 / Revised: 16 October 2021

Abstract This paper investigates the equivalence problem of bivariate polynomial matrices. A necessary and sufficient condition for the equivalence of a square matrix with the determinant being some power of a univariate irreducible polynomial and its Smith form is proposed. Meanwhile, the authors present an algorithm that reduces this class of bivariate polynomial matrices to their Smith forms, and an example is given to illustrate the effectiveness of the algorithm. In addition, the authors generalize the main result to the non-square case.

Keywords Bivariate polynomial matrix, matrix equivalence, smith form.

1 Introduction

The equivalence of multivariate polynomial matrices is an important aspect in the theory of multidimensional systems with wide applications in areas of image processing, multidimensional signal analysis, iterative learning control systems, and so on (see [1, 2] and the references therein), as a multidimensional system is often represented by a multivariate polynomial matrix

ZHENG Xiaopeng
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China;*
School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049*, China.*
Email: zhengxiaopeng@amss.ac.cn.
LU Dong (Corresponding author)
School of Mathematics, Southwest Jiaotong University, Chengdu 610031*, China.* Email: donglu@amss.ac.cn.
WANG Dingkang
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China;*
School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049*, China.*
Email: dwang@mmrc.iss.ac.cn.
XIAO Fanghui
MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha 410081*, China.*
Email: xiaofanghui@hunnu.edu.cn.
*This research was supported by the National Natural Science Foundation of China under Grant Nos. 12171469, 12001030 and 12201210, the National Key Research and Development Program under Grant No. 2020YFA0712300, and the Fundamental Research Funds for the Central Universities under Grant No. 2682022CX048.
◇ *This paper was recommended for publication by Editor MOU Chenqi.*

by means of the polynomial approach to system theory. One motivation for transforming a multivariate polynomial matrix to its Smith form is to reduce a multidimensional system to an equivalent system containing fewer equations and unknowns.

For univariate polynomial matrices, the equivalence problem has been solved[3, 4]. As we all know, a univariate polynomial matrix is always equivalent to its Smith form since the univariate polynomial ring is a principal ideal domain with the Euclidean division property. For multivariate polynomial matrices with two or more variables, however, the equivalence problem is still open. There exist some results on the equivalence research of bivariate polynomial matrices (see, e.g., [5–9]). Meanwhile, for the case of more than two variables, the equivalence problem has only been investigated for some special cases (see, e.g., [10–12]).

Lin, et al.[13] generalized the result in [8] to the case with more than two variables and posed that the equivalence of polynomial matrices is closely related to a unimodular matrix completion. Furthermore, they showed that a square matrix F with $\det(F) = x_1 - f(x_2, \cdots, x_n)$ can be reduced to its Smith form. After that, Li, et al.[14] proved that a square matrix F with $\det(F) = (x_1 - f(x_2, \cdots, x_n))^t$ is equivalent to $\mathrm{diag}\{1, \cdots, 1, \det(F)\}$ if and only if the ideal generated by $\det(F)$ and all the minors of lower one order of F is a unit ideal. Recently, Li, et al.[15–17] and Lu, et al.[18] also presented some new results on the equivalence of several classes of multivariate polynomial matrices and obtained some criteria for these matrices to equivalent to their Smith forms, respectively. These criteria are easily checked by the existing Gröbner basis algorithm.

In this paper, we shall concentrate on the equivalence problem of bivariate polynomial matrices. Li, et al.[19] proved that a square matrix $F \in K[x, y]^{l\times l}$ with $\det(F)$ being an irreducible polynomial in $K[x]$ and its Smith form are equivalent. Inspired by the work in [19], we mainly investigate the Smith forms of a special type of polynomial matrices. That is, $F \in K[x, y]^{l\times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. We consider the problem that what is the necessary and sufficient condition for the equivalence of F and its Smith form. By establishing a homomorphic mapping from $K[x, y]$ to $R_p[y]$ and using elementary transformations in the Euclidean ring $R_p[y]$ to reduce a matrix in $R_p[y]^{l\times m}$ to an upper triangular matrix, by means of the Quillen-Suslin Theorem we obtain the desired results, where $R_p = K[x]/(p)$ is a field. Moreover, we present an algorithm for reducing this class of bivariate polynomial matrices to their Smith forms and extended this result to the non-square case.

The rest of the paper is organized as follows. We present preliminary knowledge and basic concepts for the equivalence of polynomial matrices, and two problems that we shall consider in Section 2. A necessary and sufficient condition for the equivalence of polynomial matrices and their Smith forms are showed in Section 3. An algorithm and an example are established to illustrate our results in Section 4. Section 5 is the extension of the main theorem to non-square case. The paper contains a summary of contributions and some remarks in Section 6.

2 Preliminaries

Let K be a field, L be the algebraic closed field containing K, $K[x,y]$ be the polynomial ring in the variables x and y over K, and $K[x,y]^{l\times m}$ be the set of $l\times m$ matrices with entries in $K[x,y]$. Throughout this paper, we for convenience use $\mathrm{diag}\{f_1,\cdots,f_l\}$ to denote the diagonal matrix in $K[x,y]^{l\times l}$ whose diagonal elements are $f_1,\cdots,f_l$, where $f_1,\cdots,f_l\in K[x,y]$.

Let $F\in K[x,y]^{l\times m}$. For any given $s+t$ positive integers arbitrarily with $1\le i_1<\cdots<i_s\le l$ and $1\le j_1<\cdots<j_t\le m$, let $F\begin{pmatrix} i_1\cdots i_s\\ j_1\cdots j_t\end{pmatrix}$ be an $s\times t$ matrix consisting of the i_1-th, $\cdots$, i_s-th rows and the j_1-th, $\cdots$, j_t-th columns of F. We use $\mathrm{rank}(F)$ to denote the rank of F, and $\det(F)$ to be the determinant of F if $l=m$. For each integer i with $1\le i\le \mathrm{rank}(F)$, let $I_i(F)$ be the ideal generated by all the $i\times i$ minors of F, and $d_i(F)$ be the greatest common divisor of all the $i\times i$ minors of F. Here, we make the convention that $d_0(F)\equiv 1$ and $d_i(F)\equiv 0$ for $i>\mathrm{rank}(F)$.

We first introduce a basic formula in matrix theory.

Lemma 2.1 (Binet-Cauchy Formula, [20]) *Let $F=G_1F_1$, where $G_1\in K[x,y]^{l\times k}$ and $F_1\in K[x,y]^{k\times m}$. Then an $r\times r$ $(1\le r\le \min\{l,k,m\})$ minor of F is*

$$\det\left(F\begin{pmatrix} i_1 & \cdots & i_r\\ j_1 & \cdots & j_r\end{pmatrix}\right)=\sum_{1\le s_1<\cdots<s_r\le k}\det\left(G_1\begin{pmatrix} i_1 & \cdots & i_r\\ s_1 & \cdots & s_r\end{pmatrix}\right)\cdot\det\left(F_1\begin{pmatrix} s_1 & \cdots & s_r\\ j_1 & \cdots & j_r\end{pmatrix}\right).$$

Then, we recall some important concepts and results from multidimensional systems theory.

Definition 2.2 ([21]) Let $F\in K[x,y]^{l\times m}$ be of normal full rank with $l\le m$, then F is said to be zero left prime (ZLP) if all the $l\times l$ minors of F generate $K[x,y]$.

Definition 2.3 Let $U\in K[x,y]^{l\times l}$, then U is said to be unimodular if $\det(U)$ is a unit in K.

In 1976, Quillen[22] and Suslin[23] solved a famous conjecture proposed by Serre[24] positively and independently, and established a relationship between a ZLP matrix and a unimodular matrix.

Theorem 2.4 (Quillen-Suslin Theorem) *Let $F\in K[x,y]^{l\times m}$ be a ZLP matrix with $l<m$, then a unimodular matrix $U\in K[x,y]^{m\times m}$ can be constructed such that F is its first l rows.*

There are many methods for the Quillen-Suslin Theorem, we refer to [25–27] for more details. In 2007, Fabiańska and Quadrat[28] first designed a Maple package QUILLENSUSLIN to implement the Quillen-Suslin Theorem.

Definition 2.5 ([29]) Let $F\in K[x,y]^{l\times m}$ with rank r, where $1\le r\le\min\{l,m\}$. For any given integer i with $1\le i\le r$, let $a_1,\cdots,a_\beta$ be all the $i\times i$ minors of F, where $\beta=\binom{l}{i}\binom{m}{i}$. Extracting $d_i(F)$ from $a_1,\cdots,a_\beta$ yields

$$a_j=d_i(F)\cdot b_j,\quad j=1,\cdots,\beta.$$

Then, $b_1,\cdots,b_\beta$ are called the $i\times i$ reduced minors of F. For convenience, we use $J_i(F)$ to denote the ideal in $K[x,y]$ generated by $b_1,\cdots,b_\beta$.

In 2001, Lin and Bose[30] proposed the Lin-Bose conjecture. After that, Pommaret[31], Wang and Feng[32] used the Quillen-Suslin Theorem to solve the Lin-Bose conjecture, independently. This result is as follows.

Lemma 2.6 *Let $F \in K[x,y]^{l\times m}$ with $l \le m$ and $\mathrm{rank}(F) = r$, all the $r\times r$ reduced minors of F generate $K[x,y]$, where $1 \le r \le l$. Then there exist $G_1 \in K[x,y]^{l\times r}$ and $F_1 \in K[x,y]^{r\times m}$ such that $F = G_1F_1$ with F_1 being a ZLP matrix.*

Now, we present the concept of matrix equivalence.

Definition 2.7 Let $F, Q \in K[x,y]^{l\times m}$, then F is said to be equivalent to Q if there are two unimodular matrices $U \in K[x,y]^{l\times l}$ and $V \in K[x,y]^{m\times m}$ such that $F = UQV$.

For convenience, F being equivalent to Q is denoted by $F \sim Q$. Given two polynomial matrices F_1 and F_2 with $F_1 \sim F_2$, we have the following result by the Binet-Cauchy Formula.

Lemma 2.8 *Let $F_1, F_2 \in K[x,y]^{l\times m}$ with $l \le m$. If $F_1 \sim F_2$, then $d_i(F_1) = d_i(F_2)$, $I_i(F_1) = I_i(F_2)$ and $J_i(F_1) = J_i(F_2)$, where $i = 1, \cdots, l$.*

In a univariate polynomial ring, there is the concept of Smith form for a univariate polynomial matrix. We can use the same method to define the Smith form for a bivariate polynomial matrix in $K[x,y]$.

Definition 2.9 Let $F \in K[x,y]^{l\times m}$ with rank r, and Φ_i be a polynomial defined as follows,

$$\Phi_i = \begin{cases} \dfrac{d_i(F)}{d_{i-1}(F)}, & 1 \le i \le r; \\ 0, & r < i \le \min\{l,m\}. \end{cases}$$

Moreover, Φ_i satisfies the divisibility property

$$\Phi_1 \mid \Phi_2 \mid \cdots \mid \Phi_r.$$

Then the Smith form of F is given by

$$S = \begin{pmatrix} \mathrm{diag}\{\Phi_1, \cdots, \Phi_r\} & 0_{r\times(m-r)} \\ 0_{(l-r)\times r} & 0_{(l-r)\times(m-r)} \end{pmatrix}.$$

In this paper, we focus on the following two problems.

Problem 2.10 Let $F \in K[x,y]^{l\times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. What is the necessary and sufficient condition for the equivalence of F and its Smith form?

Problem 2.11 Assume that F is equivalent to its Smith form S. Constructing an algorithm to compute two unimodular matrices $U, V \in K[x,y]^{l\times l}$ such that $F = USV$.

3 Necessary and Sufficient Condition

The main objective of this section is to solve Problem 2.10.

Let $F \in K[x,y]^{l\times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. We first analyze the specific form of Smith form of F.

It follows from $d_{i-1}(F) \mid d_i(F)$ and $d_i(F) \mid \det(F)$ that there are l integers $r_1, \cdots, r_l$ with $0 \le r_1 \le \cdots \le r_l \le t$ such that $d_i(F) = p^{r_i}$, where $i = 1, \cdots, l$. Let $s_1 = r_1$ and $s_j = r_j - r_{j-1}$, where $j = 2, \cdots, l$. By Definition 2.9, the Smith form of F is

$$S = \mathrm{diag}\{p^{s_1}, p^{s_2}, \cdots, p^{s_l}\},$$

where $s_1 \le s_2 \le \cdots \le s_l$.

Now, we give the main result in the paper.

Theorem 3.1 *Let $F \in K[x,y]^{l\times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. Then F is equivalent to its Smith form if and only if $J_i(F) = K[x,y]$ with $i = 1, \cdots, l$.*

The description of the main result is brief, but the proof is complicated. In order to understand the whole proof, we use a simple example to illustrate our idea.

Example 3.2 Let $F \in K[x,y]^{3\times 3}$ with $\det(F) = p^3$, where $p \in K[x]$ is an irreducible polynomial. Assume that the Smith form of F is $S = \mathrm{diag}\{1, p, p^2\}$.

The first thing we want to do is to prove that there exist two unimodular matrices $U, V \in K[x,y]^{3\times 3}$ such that $UFV = \mathrm{diag}\{1, p, p\} \cdot G$, where $G \in K[x,y]^{3\times 3}$.

Second, we want to propose a condition such that $U_1GV_1 = \mathrm{diag}\{1, 1, p\} \cdot G_1$, where $U_1, V_1 \in K[x,y]^{3\times 3}$ are two unimodular matrices, and $G_1 \in K[x,y]^{3\times 3}$. It is easy to verify that G_1 is also a unimodular matrix. Now, we have

$$F = U^{-1} \cdot \mathrm{diag}\{1, p, p\} \cdot U_1^{-1} \cdot \mathrm{diag}\{1, 1, p\} \cdot G_1 V_1^{-1} V^{-1}.$$

The third thing is to prove that $\mathrm{diag}\{1, p, p\} \cdot U_1^{-1} \cdot \mathrm{diag}\{1, 1, p\}$ is equivalent to $\mathrm{diag}\{1, p, p^2\}$ under the same condition.

Then, we can derive the conclusion: F is equivalent to S.

According to Example 3.2, we divide our proof into three steps. In the following, we explain them step by step.

Step 1 Let $R_p = K[x]/(p)$. Since p is irreducible, R_p is a field. We consider the following homomorphism

$$\begin{aligned} \phi : K[x,y] &\longrightarrow R_p[y] \\ \sum_{i=1}^{n} c_i y^i &\longrightarrow \sum_{i=1}^{n} \overline{c_i} y^i, \end{aligned}$$

where $c_1, \cdots, c_n$ are polynomials in $K[x]$. This homomorphism can extend canonically to the homomorphism $\phi : K[x,y]^{l\times l} \to R_p[y]^{l\times l}$ by applying ϕ entry-wise. Let $F \in K[x,y]^{l\times l}$, we use $\overline{F}$ to denote the polynomial matrix $\phi(F)$ in $R_p[y]^{l\times l}$.

Lemma 3.3 *Let $F \in K[x,y]^{l\times l}$ and $p \in K[x]$ be an irreducible polynomial. If* $\mathrm{rank}(\overline{F}) \le k$*, then there exist two unimodular matrices $U, V \in K[x,y]^{l\times l}$ such that*

$$UFV = \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\} \cdot G,$$

where $G \in K[x,y]^{l\times l}$.

Proof Note that $R_p[y]$ is an Euclidean ring. We can transform $\overline{F}$ to the following upper triangular matrix

$$\overline{F_1} = \begin{pmatrix} * & * & * & * & \cdots & * \\ & \ddots & \ddots & & & \vdots \\ & & & & & \\ & & * & * & \cdots & * \\ & & & & & \\ & & & & & \end{pmatrix}$$

only by using the first kind (interchanging the rows or columns) and third kind (adding multiple of one row or column to another) of elementary transformations in $R_p[y]$. Therefore, there exist a finite number of the first and third kinds of elementary matrices $\overline{U_1}, \cdots, \overline{U_s}, \overline{V_1}, \cdots, \overline{V_t} \in R_p[y]^{l\times l}$ such that

$$\overline{U_s} \cdots \overline{U_1} \cdot \overline{F} \cdot \overline{V_1} \cdots \overline{V_t} = \overline{F_1}. \tag{1}$$

For each entry of $\overline{U_i}$ and $\overline{V_i}$, we take the representation element whose degree with respect to x is less than $\deg_x(p)$. By this way, we have unimodular matrices $U_1, \cdots, U_s, V_1, \cdots, V_t \in K[x,y]^{l\times l}$ which satisfy Equation (1). Let $U = U_s \cdots U_1$ and $V = V_1 \cdots V_t$, then $\overline{U} \cdot \overline{F} \cdot \overline{V} = \overline{F_1}$. It follows from $\mathrm{rank}(\overline{F}) \le k$ that the last $l-k$ rows of $\overline{F_1}$ are zero vectors. This implies that all elements of the last $l-k$ rows of UFV are divisible by p. Consequently,

$$UFV = \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\} \cdot G$$

and the proof is completed. ∎

Based on Lemma 3.3, we have the following corollary.

Corollary 3.4 *Let $F \in K[x,y]^{l\times l}$ and $p \in K[x]$ be an irreducible polynomial. If $p \mid d_{k+1}(F)$, then there exist two unimodular matrices $U, V \in K[x,y]^{l\times l}$ such that*

$$UFV = \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\} \cdot G,$$

where $G \in K[x,y]^{l\times l}$.

Since $p \mid d_2(F)$ in Example 3.2, by Corollary 3.4 there exist two unimodular matrices $U, V \in K[x,y]^{3\times 3}$ such that $UFV = \mathrm{diag}\{1, p, p\} \cdot G$, where $G \in K[x,y]^{3\times 3}$. Then, we solve the first problem proposed in Example 3.2.

Step 2 According to Lemma 3.3, if we would propose a condition to prove $\operatorname{rank}(\overline{G}) = 2$, then we can solve the second problem raised in Example 3.2. Therefore, in this step we focus on the rank of $\overline{G}$.

In the following, we first present some useful lemmas.

Lemma 3.5 *Let $F \in K[x,y]^{l\times l}$ and $p \in K[x]$ (not necessarily irreducible). Assume that the Smith form of F is $\operatorname{diag}\{p^{s_1}, \cdots, p^{s_l}\}$ with $s_1 \le \cdots \le s_l$, and $J_i(F) = K[x,y]$ with $i = 1, \cdots, l$. If $F \sim \operatorname{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\} \cdot G$, then $d_i(G) = 1$ and $J_i(G) = K[x,y]$, where $G \in K[x,y]^{l\times l}$ and $i = 1, \cdots, k$.*

Proof Let $D = \operatorname{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\}$, then $d_i(D) = d_i(F) = p^{s_1+\cdots+s_i}$, where $i = 1, \cdots, k$. Let $A = DG$, then $F \sim A$. By Lemma 2.8, we have $d_j(F) = d_j(A)$ and $J_j(A) = K[x,y]$, where $j = 1, \cdots, l$. Hence, $d_i(D) = d_i(A)$ for $1 \le i \le k$. For any given integer i with $1 \le i \le k$ and an $i \times i$ minor h of A, according to the Cauchy-Binet Formula we get $h = \sum_{j=1}^{\beta} f_j g_j$, where f_j is an $i \times i$ minor of D and g_j is an $i \times i$ minor of G. Divide both sides of the above equation by $d_i(A)$, we obtain

$$\frac{h}{d_i(A)} = \sum_{j=1}^{\beta} \frac{f_j}{d_i(D)} g_j. \tag{2}$$

Obviously, the left side of Equation (2) is an $i \times i$ reduced minor of A. Moreover, $J_i(A) \subseteq I_i(G)$. It follows from $J_i(A) = K[x,y]$ that $I_i(G) = K[x,y]$. Therefore, $d_i(G) = 1$ and $J_i(G) = K[x,y]$, where $i = 1, \cdots, k$. ∎

Lemma 3.6 *Let $G \in K[x,y]^{l\times l}$ and $p \in K[x]$ be an irreducible polynomial. If there exist two subsets $\{i_1, \cdots, i_k\}$ and $\{j_1, \cdots, j_k\}$ of $\{1, \cdots, l\}$ such that $p \nmid \det\left(G\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}\right)$, and for any integer $i_{k+1} \in \{1, \cdots, l\} \setminus \{i_1, \cdots, i_k\}$ and any subset $\{q_1, \cdots, q_{k+1}\} \subset \{1, \cdots, l\}$ such that $p \mid \det\left(G\begin{pmatrix} i_1 & \cdots & i_k & i_{k+1} \\ q_1 & \cdots & q_k & q_{k+1} \end{pmatrix}\right)$, then $\operatorname{rank}(\overline{G}) = k$.*

Proof Let $\overline{G} = \left(\overline{\alpha}_1^{\mathrm{T}}, \cdots, \overline{\alpha}_l^{\mathrm{T}}\right)^{\mathrm{T}}$ and

$$h = \det\left(G\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}\right).$$

Since $p \nmid h$, we have $\overline{h} \ne \overline{0}$ in $R_p[y]$. It follows that $\overline{\alpha}_{i_1}, \cdots, \overline{\alpha}_{i_k}$ are $R_p[y]$-linearly independent, and $\operatorname{rank}(\overline{G}) \ge k$. As for any $i_{k+1} \in \{1, \cdots, l\} \setminus \{i_1, \cdots, i_k\}$ and $\{q_1, \cdots, q_{k+1}\} \subset \{1, \cdots, l\}$ such that

$$p \mid \det\left(G\begin{pmatrix} i_1 & \cdots & i_k & i_{k+1} \\ q_1 & \cdots & q_k & q_{k+1} \end{pmatrix}\right),$$

$\overline{\alpha}_{i_1}, \cdots, \overline{\alpha}_{i_k}, \overline{\alpha}_{i_{k+1}}$ are $R_p[y]$-linearly dependent. This implies that there are $h_{i_{k+1}1}, \cdots, h_{i_{k+1}k} \in R_p(y)$ such that

$$\overline{\alpha}_{i_{k+1}} = h_{i_{k+1}1}\overline{\alpha}_{i_1} + \cdots + h_{i_{k+1}k}\overline{\alpha}_{i_k}, \tag{3}$$

where $R_p(y)$ is the rational fraction field of $R_p[y]$. For any given subset $\{t_1, \cdots, t_k, t_{k+1}\}$ of $\{1, \cdots, l\}$, we next prove that $\overline{\alpha}_{t_1}, \cdots, \overline{\alpha}_{t_k}, \overline{\alpha}_{t_{k+1}}$ are $R_p[y]$-linearly dependent.

According to Equation (3), we have

$$\begin{pmatrix} \overline{\alpha}_{t_1} \\ \vdots \\ \overline{\alpha}_{t_k} \\ \overline{\alpha}_{t_{k+1}} \end{pmatrix} = \begin{pmatrix} h_{t_1 1} & \cdots & h_{t_1 k} \\ \vdots & \ddots & \vdots \\ h_{t_k 1} & \cdots & h_{t_k k} \\ h_{t_{k+1} 1} & \cdots & h_{t_{k+1} k} \end{pmatrix} \begin{pmatrix} \overline{\alpha}_{i_1} \\ \vdots \\ \overline{\alpha}_{i_k} \end{pmatrix}, \tag{4}$$

where $h_{t_r n} \in R_p(y)$, $1 \le r \le k+1$ and $1 \le n \le k$. For convenience, we write Equation (4) as $A = HB$, where $H \in R_p(y)^{(k+1)\times k}$. Obviously, $\operatorname{rank}(H) \le k$ in $R_p(y)$. Then there exists a nonzero vector $\overline{w} \in R_p(y)^{1\times(k+1)}$ such that $\overline{w}H = \overline{0}$. Combining this equation and $A = HB$, we have $\overline{w}A = \overline{0}$. Assume that $\overline{w} = (w_1, \cdots, w_k, w_{k+1})$, where $w_1, \cdots, w_k, w_{k+1} \in R_p(y)$. Multiplying both sides of the equation $\overline{w}A = \overline{0}$ by the least common multiple of the denominators of $w_1, \cdots, w_k, w_{k+1}$, we obtain $w'_1\overline{\alpha}_{t_1} + \cdots + w'_k\overline{\alpha}_{t_k} + w'_{k+1}\overline{\alpha}_{t_{k+1}} = \overline{0}$, where $w'_1, \cdots, w'_k, w'_{k+1} \in R_p[y]$ and are not all zeros.

As a consequence, $\operatorname{rank}(\overline{G}) = k$. ∎

Now, we propose the most important result in this step.

Lemma 3.7 *Let $F \in K[x,y]^{l\times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. Assume that the Smith form of F is $\operatorname{diag}\{p^{s_1}, \cdots, p^{s_l}\}$ with $s_1 \le \cdots \le s_l$. If $F \sim \operatorname{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\} \cdot G$ and $s_k \le s < s_{k+1}$, then $\operatorname{rank}(\overline{G}) = k$, where $G \in K[x,y]^{l\times l}$.*

Proof According to Lemma 3.5, we have $d_k(G) = 1$. Then, there exists a $k \times k$ minor h of G such that $p \nmid h$. This implies that $\operatorname{rank}(\overline{G}) \ge k$. Next, we prove that $\operatorname{rank}(\overline{G}) = k$. Let

$$A = \operatorname{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\} \cdot G,$$

then $F \sim A$. In the following, we consider three cases.

1) $s_1 = \cdots = s_k = s$. Then for all subsets $\{i_1, \cdots, i_k, i_{k+1}\}$ and $\{j_1, \cdots, j_k, j_{k+1}\}$ of $\{1, \cdots, l\}$ we have

$$\det\left(A\begin{pmatrix} i_1 & \cdots & i_k & i_{k+1} \\ j_1 & \cdots & j_k & j_{k+1} \end{pmatrix}\right) = p^{(k+1)s} \cdot \det\left(G\begin{pmatrix} i_1 & \cdots & i_k & i_{k+1} \\ j_1 & \cdots & j_k & j_{k+1} \end{pmatrix}\right).$$

By $F \sim A$ and Lemma 2.8, we get $d_{k+1}(A) = d_{k+1}(F) = p^{ks+s_{k+1}}$. As $s_{k+1} > s$ and $d_{k+1}(A)$ is a divisor of any $(k+1)\times(k+1)$ minor of A, we have

$$p \mid \det\left(G\begin{pmatrix} i_1 & \cdots & i_k & i_{k+1} \\ j_1 & \cdots & j_k & j_{k+1} \end{pmatrix}\right).$$

It follows that $p \mid d_{k+1}(G)$. Hence, $\operatorname{rank}(\overline{G}) = k$.

2) There exists an integer m with $m < k$ such that $s_1 \le \cdots \le s_m < s_{m+1} = \cdots = s_k = s$.

Let

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1l} \\ \vdots & \ddots & \vdots \\ \\ g_{l1} & \cdots & g_{ll} \end{pmatrix},$$

then

$$A = \begin{pmatrix} p^{s_1} g_{11} & \cdots & p^{s_1} g_{1k} & \cdots & p^{s_1} g_{1l} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \\ p^{s_m} g_{m1} & \cdots & p^{s_m} g_{mk} & \cdots & p^{s_m} g_{ml} \\ p^{s} g_{m+1,1} & \cdots & p^{s} g_{m+1,k} & \cdots & p^{s} g_{m+1,l} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \\ p^{s} g_{l1} & \cdots & p^{s} g_{lk} & \cdots & p^{s} g_{ll} \end{pmatrix}. \tag{5}$$

Let $e = \sum_{i=1}^{m} s_i$, then

$$\det\left(A\begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_k \\ j_1 & \cdots & j_m & j_{m+1} & \cdots & j_k \end{pmatrix}\right) = p^{e+(k-m)s} \cdot \det\left(G\begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_k \\ j_1 & \cdots & j_m & j_{m+1} & \cdots & j_k \end{pmatrix}\right).$$

We assert that there exist two sets $\{i_{m+1}, \cdots, i_k\} \subset \{m+1, \cdots, l\}$ and $\{j_1, \cdots, j_k\} \subset \{1, \cdots, l\}$ such that

$$p \nmid \det\left(G\begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_k \\ j_1 & \cdots & j_m & j_{m+1} & \cdots & j_k \end{pmatrix}\right).$$

If the assertion would not hold, then we have

$$p^{e+(k-m)s+1} \mid \det\left(A\begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_k \\ j_1 & \cdots & j_m & j_{m+1} & \cdots & j_k \end{pmatrix}\right)$$

for all $\{i_{m+1}, \cdots, i_k\} \subset \{m+1, \cdots, l\}$ and $\{j_1, \cdots, j_k\} \subset \{1, \cdots, l\}$. From Equation (5), it is easy to check that any other $k \times k$ minor of A is also divisible by $p^{e+(k-m)s+1}$. This contradicts the fact that $d_k(A) = p^{e+(k-m)s}$.

For any given $i_{k+1} \in \{m+1, \cdots, l\} \setminus \{i_{m+1}, \cdots, i_k\}$ and $\{q_1, \cdots, q_{k+1}\} \subset \{1, \cdots, l\}$, we have

$$\det\left(A\begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_{k+1} \\ q_1 & \cdots & q_m & q_{m+1} & \cdots & q_{k+1} \end{pmatrix}\right) = p^{e+(k-m+1)s} \cdot \det\left(G\begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_{k+1} \\ q_1 & \cdots & q_m & q_{m+1} & \cdots & q_{k+1} \end{pmatrix}\right).$$

Since $d_{k+1}(A) = p^{e+(k-m)s+s_{k+1}}$ and $s_{k+1} > s$, we get

$$p \,|\, \det\left(G \begin{pmatrix} 1 & \cdots & m & i_{m+1} & \cdots & i_{k+1} \\ q_1 & \cdots & q_m & q_{m+1} & \cdots & q_{k+1} \end{pmatrix} \right).$$

Based on Lemma 3.6, we obtain $\mathrm{rank}(\overline{G}) = k$.

3) $s_1 \leq \cdots \leq s_k < s$. We can use the same method to prove that $\mathrm{rank}(\overline{G}) = k$.

Therefore, $\mathrm{rank}(\overline{G}) = k$ and the proof is completed. ∎

Remark 3.8 Combining Lemma 3.3 and Lemma 3.7, there exist two unimodular matrices $U_1, V_1 \in K[x,y]^{l\times l}$ such that

$$U_1 G V_1 = \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\} \cdot G_1,$$

where $G_1 \in K[x,y]^{l\times l}$.

By Remark 3.8, we solve the second problem proposed in Example 3.2.

Step 3 In this step, we will prove that

$$\mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\} \cdot U \cdot \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\}$$

is equivalent to $\mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^{s+1}, \cdots, p^{s+1}\}$ under the condition which proposed in Lemma 3.10, where $U \in K[x,y]^{l\times l}$ is a unimodular matrix.

First, we propose a lemma.

Lemma 3.9 *Let $F \in K[x,y]^{l\times l}$ and $p \in K[x]$ (not necessarily irreducible). Assume that the Smith form of F is $\mathrm{diag}\{p^{s_1}, \cdots, p^{s_l}\}$ with $s_1 \leq \cdots \leq s_l$, and $J_i(F) = K[x,y]$ with $i = 1, \cdots, l$. Let*

$$B = \mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\} \cdot U \cdot \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\},$$

where $U \in K[x,y]^{l\times l}$ (not necessarily unimodular). If $F \sim BG$, then $d_i(B) = p^{s_1+\cdots+s_i}$ and $J_i(B) = K[x,y]$, where $G \in K[x,y]^{l\times l}$ and $i = 1, \cdots, k$.

The proof of Lemma 3.9 is basically the same as that of Lemma 3.5, except that we focus on B. Hence, the proof is omitted here.

Now, we solve the problem proposed in this step.

Lemma 3.10 *Let*

$$B = \mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^s, \cdots, p^s\} \cdot U \cdot \mathrm{diag}\{\underbrace{1,\cdots,1}_{k}, p, \cdots, p\},$$

where $s_1 \leq \cdots \leq s_k \leq s$, $p \in K[x]$ is an irreducible polynomial and $U \in K[x,y]^{l\times l}$ is a unimodular matrix. If $d_i(B) = p^{s_1+\cdots+s_i}$ and $J_i(B) = K[x,y]$ with $i = 1, \cdots, k$, then

$$B \sim \mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^{s+1}, \cdots, p^{s+1}\}.$$

Proof We consider the following three cases.

1) If $s_1 = \cdots = s_k = s$, then the conclusion is obvious.

2) There exists an integer m with $m < k$ such that $s_1 \le \cdots \le s_m < s_{m+1} = \cdots = s_k = s$. Let $U = \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix}$, where $U_1 \in K[x,y]^{m\times k}$, $U_2 \in K[x,y]^{m\times(l-k)}$, $U_3 \in K[x,y]^{(l-m)\times k}$ and $U_4 \in K[x,y]^{(l-m)\times(l-k)}$. Let $a_1,\cdots,a_\beta$ be all the $m\times m$ minors of (U_1,U_2). Since U is a unimodular matrix, $a_1,\cdots,a_\beta$ have no common zeros in L^2. By the computation, all the $m\times m$ minors of (U_1,pU_2) are

$$a_1,\cdots,a_{\beta_0},pa_{\beta_1},\cdots,p^2a_{\beta_2},\cdots,p^3a_{\beta_3},\cdots,p^ta_\beta,$$

where $t=\min\{m,l-k\}$. We claim that (U_1,pU_2) is a ZLP matrix. Otherwise, $a_1,\cdots,a_{\beta_0},p$ have common zeros. We compute all the $m\times m$ reduced minors of B, and these reduced minors can be classified into two types: The $m\times m$ reduced minors of $\mathrm{diag}\{p^{s_1},\cdots,p^{s_m}\}\cdot U_1$, and other $m\times m$ reduced minors. Since $d_m(B)=p^{s_1+\cdots+s_m}$, the $m\times m$ reduced minors of $\mathrm{diag}\{p^{s_1},\cdots,p^{s_m}\}\cdot U_1$ are exactly $a_1,\cdots,a_{\beta_0}$, and other $m\times m$ reduced minors are divisible by p. Therefore, all the $m\times m$ reduced minors of B have common zeros, which contradicts to $J_m(B)=K[x,y]$.

According to the Quillen-Suslin Theorem, there exists a unimodular matrix $P\in K[x,y]^{l\times l}$ such that

$$(U_1,pU_2)P=(E_m,0_{m\times(l-m)}),$$

where E_m is the $m\times m$ identity matrix. Hence,

$$BP=\begin{pmatrix} p^{s_1} & & & & & \\ & \ddots & & & & \\ & & p^{s_m} & & & \\ p^sv_{m+1,1} & \cdots & p^sv_{m+1,m} & p^sv_{m+1,m+1} & \cdots & p^sv_{m+1,l} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ p^sv_{l,1} & \cdots & p^sv_{l,m} & p^sv_{l,m+1} & \cdots & p^sv_{l,l} \end{pmatrix},$$

where

$$(U_3,pU_4)P=\begin{pmatrix} v_{m+1,1} & \cdots & v_{m+1,l} \\ \vdots & \ddots & \vdots \\ v_{l,1} & \cdots & v_{l,l} \end{pmatrix}.$$

If $v_{i,j}$ is divisible by p for all i with $m+1\le i\le l$ and j with $k+1\le j\le l$, we get

$$BP=Q\cdot\mathrm{diag}\{p^{s_1},\cdots,p^{s_m},\underbrace{p^s,\cdots,p^s}_{k-m},p^{s+1},\cdots,p^{s+1}\}.$$

It is easy to compute that $\det(Q) \in K \setminus \{0\}$. Therefore, we have

$$B \sim \mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^{s+1}, \cdots, p^{s+1}\}.$$

Otherwise, by elementary transformations we have

$$B \sim C = \begin{pmatrix} p^{s_1} & & & \\ & \ddots & & \\ & & p^{s_m} & \\ & & & p^s V \end{pmatrix},$$

where

$$V = \begin{pmatrix} v_{m+1,m+1} & \cdots & v_{m+1,l} \\ \vdots & \ddots & \vdots \\ v_{l,m+1} & \cdots & v_{l,l} \end{pmatrix}.$$

In the following, we prove that there are two unimodular matrices $P_1, Q_1 \in K[x, y]^{(l-m)\times(l-m)}$ such that

$$V = P_1 \begin{pmatrix} E_{k-m} & \\ & pE_{l-k} \end{pmatrix} G Q_1, \tag{6}$$

where $G \in K[x, y]^{(l-m)\times(l-m)}$. It suffices to prove that $\mathrm{rank}(\overline{V}) \le k - m$.

Let $e = \sum_{i=1}^{m} s_i + (k - m + 1)s + 1$. Since $p^e \mid d_{k+1}(B)$ and $B \sim C$, we have $p^e \mid d_{k+1}(C)$. Let V' be an arbitrary $(k - m + 1) \times (k - m + 1)$ submatrix of V, then

$$C' = \begin{pmatrix} p^{s_1} & & & \\ & \ddots & & \\ & & p^{s_m} & \\ & & & p^s V' \end{pmatrix}$$

is a $(k+1) \times (k+1)$ submatrix of C. Therefore, $p^e \mid \det(C')$ implies that $p \mid \det(V')$. It follows that $p \mid d_{k-m+1}(V)$. Then, $\mathrm{rank}(\overline{V}) \le k - m$. Based on Lemma 3.3, Equation (6) holds. Through some simple elementary transformations, we have

$$C \sim \mathrm{diag}\{p^{s_1}, \cdots, p^{s_m}, \underbrace{p^s, \cdots, p^s}_{k-m}, p^{s+1}, \cdots, p^{s+1}\} \cdot \begin{pmatrix} E_m & \\ & G \end{pmatrix}.$$

By computing the determinant of $\begin{pmatrix} E_m & \\ & G \end{pmatrix}$ we find that it is a unimodular matrix. Therefore,

$$B \sim C \sim \mathrm{diag}\{p^{s_1}, \cdots, p^{s_k}, p^{s+1}, \cdots, p^{s+1}\}.$$

3) If $s_1 \leq \cdots \leq s_k < s$, then we obtain the same conclusion by the above method.

Therefore, the proof is completed. ▮

Based on Lemma 3.10, we solve the third problem proposed in Example 3.2.

Proof of the Main Theorem

With all the above results, we now prove Theorem 3.1.

Proof Necessity. Assume that $F \sim S = \mathrm{diag}\{p^{s_1}, \cdots, p^{s_l}\}$. By Lemma 2.8, it is easy to compute that $J_i(F) = J_i(S) = K[x, y]$, where $i = 1, \cdots, l$.

Sufficiency. Since $d_1(F) = p^{s_1}$, we have $F = \mathrm{diag}\{p^{s_1}, \cdots, p^{s_1}\} \cdot G_1$. If $s_2 = s_1$, then $F = \mathrm{diag}\{p^{s_1}, p^{s_2}, \cdots, p^{s_2}\} \cdot G_2$, where $G_2 = G_1$. If $s_2 > s_1$, then by Lemma 3.7 and Remark 3.8 we have $G_1 = U_{21} \cdot \mathrm{diag}\{1, p, \cdots, p\} \cdot G_{21} V_{21}$, where $U_{21}, V_{21} \in K[x, y]^{l \times l}$ are two unimodular matrices, and $G_{21} \in K[x, y]^{l \times l}$. Then, we get

$$F \sim \mathrm{diag}\{p^{s_1}, p^{s_1}, \cdots, p^{s_1}\} \cdot U_{21} \cdot \mathrm{diag}\{1, p, \cdots, p\} \cdot G_{21}.$$

According to Lemmas 3.9 and 3.10, there exist two unimodular matrices $U'_{21}, V'_{21} \in K[x, y]^{l \times l}$ such that

$$\mathrm{diag}\{p^{s_1}, p^{s_1}, \cdots, p^{s_1}\} \cdot U_{21} \cdot \mathrm{diag}\{1, p, \cdots, p\} = U'_{21} \cdot \mathrm{diag}\{p^{s_1}, p^{s_1+1}, \cdots, p^{s_1+1}\} \cdot V'_{21}.$$

Let $G'_{21} = V'_{21} G_{21}$, then $F \sim \mathrm{diag}\{p^{s_1}, p^{s_1+1}, \cdots, p^{s_1+1}\} G'_{21}$. Repeat this process for $s_2 - s_1$ times, we obtain

$$F \sim \mathrm{diag}\{p^{s_1}, p^{s_2}, \cdots, p^{s_2}\} \cdot G_2.$$

We can use the same method to get $F \sim \mathrm{diag}\{p^{s_1}, p^{s_2}, \cdots, p^{s_l}\} \cdot G_l$. It is easy to check that G_l is a unimodular matrix. Therefore, we have

$$F \sim \mathrm{diag}\{p^{s_1}, p^{s_2}, \cdots, p^{s_l}\},$$

and the proof is completed. ▮

4 Algorithm and Illustrative Example

In this section, we first propose an algorithm to solve Problem 2.11, and then use an example to show the effectiveness of the algorithm.

According to the proof of Theorem 3.1, we can construct the following algorithm to compute the Smith form of $F \in K[x, y]^{l \times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. We have implemented the algorithm on Maple with K of characteristic zero. For interested readers, more examples can be generated by the codes at: http://www.mmrc.iss.ac.cn/ dwang/software.html.

Theorem 4.1 *Algorithm* 1 *outputs as specified within a finite number of steps.*

Proof The correctness and termination follow directly from Theorem 3.1. ▮

We now use an example to illustrate the calculation process of Algorithm 1.

Algorithm 1: Smith Form(F)

Input: $F \in K[x,y]^{l\times l}$ with $\det(F) = p^t$, where $p \in K[x]$ is irreducible.

Output: $S, U, V \in K[x,y]^{l\times l}$, where S is the Smith form of F, and U, V are two unimodular matrices such that $F = USV$.

Compute $d_i(F)$ and $J_i(F)$, where $i = 1, \cdots, l$;

if *there exists some integer* i *with* $1 \le i \le l$ *such that* $J_i(F) \ne K[x,y]$ **then**

  return F is not equivalent to its Smith form.

$S := \mathrm{diag}\{p^{s_1}, p^{s_2}, \cdots, p^{s_l}\}$;

Extract p^{s_1} from each row of F and obtain a matrix G which satisfies $F = \mathrm{diag}\{p^{s_1}, \cdots, p^{s_1}\} \cdot G$;

Let U, V be two identity matrices;

for i *from* 2 *to* l **do**

  if $s_i \ne s_{i-1}$ **then**

    for j *from* 1 *to* $s_i - s_{i-1}$ **do**

      compute a matrix G' and two unimodular matrices U', V' such that $G = U' \cdot \mathrm{diag}\{\underbrace{1, \cdots, 1}_{i-1}, p, \cdots, p\} \cdot G' \cdot V'$;

      compute a matrix G'' and two unimodular matrices U'', V'' such that $\mathrm{diag}\{p^{s_1}, \cdots, p^{s_{i-1}}, p^{s_{i-1}+j-1}, \cdots, p^{s_{i-1}+j-1}\} \cdot U' \cdot \mathrm{diag}\{\underbrace{1, \cdots, 1}_{i-1}, p, \cdots, p\} = U'' \cdot \mathrm{diag}\{p^{s_1}, \cdots, p^{s_{i-1}}, p^{s_{i-1}+j}, \cdots, p^{s_{i-1}+j}\} \cdot V''$;

      $G := V'' \cdot G'$, $U := U \cdot U''$ and $V := V' \cdot V$;

$V := G \cdot V$;

return S, U, V.

Example 4.2 Let

$$F = \begin{pmatrix} -y^2 + 1 + (x-y-1)(x^2+1)^2 y & x - y - 1 & -y + (x-y-1)(x^2+1)^2 \\ x(x+1)(-y^2+1) + y(x^2+1)^2 & -(x+1)(xy+x+1) & x^4 - x^2y + 2x^2 - xy + 1 \\ x(y^2-1) & x(y-x+1) + x^2 + 1 & xy \end{pmatrix}$$

be a bivariate polynomial matrix in $\mathbb{Q}[x,y]^{3\times 3}$, where $\mathbb{Q}$ is the rational number field.

It is easy to compute that $d_1(F) = 1$, $d_2(F) = x^2 + 1$, $d_3(F) = (x^2+1)^3$. Then, the Smith form of F is

$$S = \mathrm{diag}\{1, x^2 + 1, (x^2+1)^2\}.$$

We compute the reduced Gröbner basis $\mathcal{G}_i$ of all the $i \times i$ reduced minors of F and obtain $\mathcal{G}_i = \{1\}$, where $i = 1, 2, 3$. Based on Theorem 3.1, F is equivalent to S. In the following, we compute two unimuodular matrices $U, V \in \mathbb{Q}[x,y]^{3\times 3}$ such that $F = USV$.

Let $p = x^2+1$. As $p \mid d_2(F)$, we have $\mathrm{rank}(\overline{F}) \le 1$. By Lemma 3.3, there are two unimodular matrices

$$U_1 = \begin{pmatrix} 1 & 0 & 0 \\ -x+1 & 1 & 0 \\ x & 0 & 1 \end{pmatrix} \quad \text{and} \quad V_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

such that $U_1 F V_1 = \mathrm{diag}\{1, p, p\} \cdot G_1$, where

$$G_1 = \begin{pmatrix} x-y-1 & G_1[1,2] & G_1[1,3] \\ -y-2 & G_1[2,2] & G_1[2,3] \\ 1 & xy(x^2+1)(x-y-1) & x(x^2+1)(x-y-1) \end{pmatrix}$$

with $G_1[1,2] = -y^2+1+(x-y-1)(x^2+1)^2 y$, $G_1[1,3] = -y+(x-y-1)(x^2+1)^2$, $G_1[2,2] = -x^4y+x^3y^2+2x^3y-x^2y^2-x^2y+xy^2+2xy-2y^2+1$ and $G_1[2,3] = -x^4+x^3y+2x^3-x^2y-x^2+xy+2x-2y$. It follows from Lemma 3.7 that $\mathrm{rank}(\overline{G}) = 2$. Using Lemma 3.3 again, there exist two unimodular matrices

$$U_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & y+2 \\ 1 & -1 & -x-1 \end{pmatrix} \quad \text{and} \quad V_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

such that $U_2 G_1 V_2 = \mathrm{diag}\{1, 1, p\} \cdot G_2$, where

$$G_2 = \begin{pmatrix} 1 & x(x^2+1)(x-y-1) & xy(x^2+1)(x-y-1) \\ 0 & G_2[2,2] & G_2[2,3] \\ 0 & -1 & -y \end{pmatrix}$$

with $G_2[2,2] = x^4y-x^3y^2+x^4-2x^3y-xy^2+x^2-2xy-2y$ and $G_2[2,3] = -x^4+x^3y+2x^3-x^2y-x^2+xy+2x-2y$. Since $\det(G_2) = 1$, we have that G_2 is a unimodular matrix. So,

$$F = U_1^{-1} \cdot \mathrm{diag}\{1, p, p\} \cdot U_2^{-1} \cdot \mathrm{diag}\{1, 1, p\} \cdot G_2 V_2^{-1} V_1^{-1}.$$

Let

$$B = \mathrm{diag}\{1, p, p\} \cdot U_2^{-1} \cdot \mathrm{diag}\{1, 1, p\} = \begin{pmatrix} x-y-1 & 1 & x^2+1 \\ (x^2+1)(-y-2) & x^2+1 & 0 \\ x^2+1 & 0 & 0 \end{pmatrix}.$$

It is easy to see that the first row of $U_2^{-1} \cdot \mathrm{diag}\{1, 1, p\}$ is a ZLP vector. Then, we can construct a unimodular matrix

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -x+y+1 & -x^2-1 \\ 0 & 0 & 1 \end{pmatrix}$$

such that

$$BP = \begin{pmatrix} 1 & 0 & 0 \\ x^2+1 & -(x+1)(x^2+1) & -(x^2+1)^2 \\ 0 & x^2+1 & 0 \end{pmatrix}.$$

Since the last column of BP is divisible by p^2, we obtain

$$BP = U_3 \cdot \mathrm{diag}\{1, p, p^2\} = \begin{pmatrix} 1 & 0 & 0 \\ x^2+1 & -(x+1) & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p^2 \end{pmatrix},$$

where U_3 is a unimodular matrix. Let $U = U_1^{-1}U_3$ and $V = P^{-1}G_2V_2^{-1}V_1^{-1}$, then

$$F = USV.$$

5 Non-Square Case

In this section, we extend Theorem 3.1 to the case of non-square matrices.

Corollary 5.1 *Let $F \in K[x,y]^{l\times m}$ with $l < m$ and $d_l(F) = p^t$, where $p \in K[x]$ is an irreducible polynomial and t is a positive integer. Then F is equivalent to its Smith form if and only if $J_i(F) = K[x,y]$ with $i = 1, \cdots, l$.*

Proof The Smith form of F is $S = (\mathrm{diag}\{p^{s_1}, \cdots, p^{s_l}\}, 0_{l\times(m-l)})$.

Necessity. Assume that $F \sim S$. By Lemma 2.8, it is easy to verify that $J_i(F) = J_i(S) = K[x,y]$, where $i = 1, \cdots, l$.

Sufficiency. Since $J_l(F) = K[x,y]$, by Lemma 2.6 there exist $G_1 \in K[x,y]^{l\times l}$ and $F_1 \in K[x,y]^{l\times m}$ such that $F = G_1F_1$ with F_1 being a ZLP matrix. According to the Quillen-Suslin Theorem, there is a unimodular matrix $P \in K[x,y]^{m\times m}$ such that $F_1P = (E_l, 0_{l\times(m-l)})$. Multiplying both sides of the equation $F = G_1F_1$ by P, we obtain $FP = (G_1, 0_{l\times(m-l)})$. As P is a unimodular matrix, we have $F \sim (G_1, 0_{l\times(m-l)})$. Using Lemma 2.8, $d_i(G_1) = d_i(F)$ and $J_i(G_1) = J_i(F) = K[x,y]$, where $i = 1, \cdots, l$. According to Theorem 3.1, there are two unimodular matrices $U, V \in K[x,y]^{l\times l}$ such that $G_1 = U \cdot \mathrm{diag}\{p^{s_1}, \cdots, p^{s_l}\} \cdot V$. Therefore,

$$F = US \begin{pmatrix} V & \\ & E_{m-l} \end{pmatrix} P^{-1}.$$

The proof is completed. ∎

Remark 5.2 Li, et al.[19] also considered the non-square case. They proved that F and

$$(\mathrm{diag}\{\underbrace{1,\cdots,1}_{l-1},p^t\},0_{l\times(m-l)})$$

are equivalent if and only if the $(l-1)\times(l-1)$ minors of F generate the unit ideal $K[x,y]$. It is easy to check that this result is a special case of Corollary 5.1.

Corollary 5.3 *Let $F\in K[x,y]^{l\times m}$ with rank r, where $1\le r\le l<m$. Assume that $d_r(F)=p^t$, where $p\in K[x]$ is an irreducible polynomial and t is a positive integer. Then F is equivalent to its Smith form if and only if $J_i(F)=K[x,y]$ with $i=1,\cdots,r$.*

The proof of Corollary 5.3 is the same as that of Corollary 5.1, and is omitted here.

6 Conclusions

A necessary and sufficient condition for the equivalence of a bivariate polynomial matrix and its Smith form has been proposed. We establish a homomorphic mapping from $K[x,y]$ to $R_p[y]$, where $p\in K[x]$ is an irreducible polynomial and $R_p=K[x]/(p)$ is a field. Then we can use elementary transformations in the Euclidean ring $R_p[y]$ to reduce a matrix in $R_p[y]^{l\times m}$ to an upper triangular matrix. This implies that we can extract p from some rows of a matrix in $K[x,y]^{l\times m}$ after multiplying by some unimodular matrices in $K[x,y]^{l\times m}$. The Quillen-Suslin Theorem plays an important role in the proof of Theorem 3.1, which helps us eliminate the influence of a unimodular matrix and obtain the Smith form of a bivariate polynomial matrix.

In this paper we solve the equivalence problem of a special bivariate polynomial matrix and its Smith form, but the following problem arises naturally. If $F\in K[x_1,\cdots,x_n]^{l\times l}$ and $\det(F)=p^t$, where $p\in K[x_1]$ is an irreducible polynomial, is F equivalent to its Smith form? Although $K[x_1]/(p)$ is a field, $K[x_1]/(p)[x_2,\cdots,x_n]$ is just a quotient ring and no longer has the Euclidean division property. This shows that we cannot directly extend the research method of Theorem 3.1 to the n-dimensional case. The authors in [29, 33, 34] studied algebraic invariants of multidimensional (n-D) systems and used them to transform multivariate polynomial matrices to some simpler but equivalent forms. We expect that the method will provide us with new ideas for solving the above problem and obtain the desired result.

References

[1] Bose N K, *Applied Multidimensional Systems Theory*, Van Nostrand Reinhold, New York, 1982.

[2] Bose N K, Buchberger B, and Guiver J, *Multidimensional Systems Theory and Applications*, Dordrecht, Kluwer, The Netherlands, 2003.

[3] Kailath T, *Linear Systems*, Englewood Cliffs, NJ: Prentice Hall, 1980.

[4] Rosenbrock H H, *State Space and Multivariable Theory*, Nelson-Wiley, New Work, London, 1970.

[5] Morf M, Levy B, and Kung S, New results in 2-D systems theory: Part I, *Proceeding of the IEEE*, 1977, **65**: 861–872.

[6] Frost M and Storey C, Equivalence of a matrix over $R[s,z]$ with its Smith form, *International Journal of Control*, 1978, **28**(5): 665–671.

[7] Lee E and Zak S, Smith forms over $R[z_1,z_2]$, *IEEE Transactions on Automatic Control*, 1983, **28**(1): 115–118.

[8] Frost M and Boudellioua M, Some further results concerning matrices with elements in a polynomial ring, *International Journal of Control*, 1986, **43**(5): 1543–1555.

[9] Pugh A C, McInerney S J, and El-Nabrawy E M O, Equivalence and reduction of 2-D systems, *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2005, **52**(5): 271–275.

[10] Cluzeau T and Quadrat A, Factoring and decomposing a class of linear functional systems, *Linear Algebra and Its Applications*, 2008, **428**: 324–381.

[11] Boudellioua M S and Quadrat A, Serre's reduction of linear function systems, *Mathematics in Computer Science*, 2010, **4**(2–3): 289–312.

[12] Cluzeau T and Quadrat A, A new insight into Serre's reduction problem, *Linear Algebra and its Applications*, 2015, **483**: 40–100.

[13] Lin Z, Boudellioua M S, and Xu L, On the equivalence and factorization of multivariate polynomial matrices, *Proceeding of ISCAS*, Greece, 2006, 4911–4914.

[14] Li D, Liu J, and Zheng L, On the equivalence of multivariate polynomial matrices, *Multidimensional Systems and Signal Processing*, 2017, **28**(1): 225–235.

[15] Li D and Liang R, Serre's reduction and the Smith forms of multivariate polynomial matrices, *Mathematical Problems in Engineering*, 2020, 1–13, DOI: 10.1155/2020/5430842.

[16] Li D, Liu J, and Chu D, The Smith form of a multivariate polynomial matrix over an arbitrary coefficient field, *Linear and Multilinear Algebra*, 2022, **70**(2): 366–379.

[17] Li D, Liu J, and Zheng L, On serre reduction of multidimensional systems, *Mathematical Problems in Engineering*, 2020, 1–8, DOI: 10.1155/2020/7435237.

[18] Lu D, Wang D, and Xiao F, Further results on the factorization and equivalence for multivariate polynomial matrices, *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, 2020, 328–335.

[19] Li D, Liang R, and Liu J, Some further results on the Smith form of bivariate polynomial matrices, *Journal of System Science and Mathematical Science* (*Chinese Series*), 2019, **39**(12): 1983–1997.

[20] Strang G, *Linear Algebra and Its Applications*, Academic Press, Cambridge, Massachusetts, 2010.

[21] Youla D and Gnavi G, Notes on n-dimensional system theory, *IEEE Transactions on Circuits and Systems*, 1979, **26**(2): 105–111.

[22] Quillen D, Projective modules over polynomial rings, *Inventiones Mathematicae*, 1976, **36**(1): 167–171.

[23] Suslin A A, Projective modules over polynomial rings are free, *Soviet Mathematics Doklady*, 1976, **17**: 1160–1164.

[24] Serre J P, Faisceaux algébriques cohérents, *Annals of Mathematics*, 1955, **61**(2): 197–278.

[25] Logar A and Sturmfels B, Algorithms for the Quillen-Suslin theorem, *Journal of Algebra*, 1992, **145**(1): 231–239.

[26] Park H, A computational theory of laurent polynomial rings and multidimensional FIR systems, Doctoral Dissertation, University of California at Berkeley, USA, 1995.

[27] Youla D and Pickel P, The Quillen-Suslin theorem and the structure of n-dimensional elementary

polynomial matrices, *IEEE Transactions on Circuits and Systems*, 1984, **31**(6): 513–518.

[28] Fabiańska A and Quadrat A, Applications of the Quillen-Suslin theorem to multidimensional systems theory, Eds. by Park H, Regensburger G, *Gröbner Bases in Control Theory and Signal Processing*, Radon Series on Computational and Applied Mathematics, Walter de Gruyter, 2007, **3**: 23–106.

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

[30] Lin Z and Bose N, A generalization of serre's conjecture and some related issues, *Linear Algebra and Its Applications*, 2001, **338**: 125–138.

[31] Pommaret J F, Solving bose conjecture on linear multidimensional systems, *Proceedings of European Control Conference, IEEE*, Porto, Portugal, 2001, 1653–1655.

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

[33] Pugh A C, McInerney S J, and El-Nabrawy E M O, Zero structures of n-D systems, *International Journal of Control*, 2005, **78**(4): 277–285.

[34] Li L, Li X, and Lin Z, Stability and stabilisation of linear multidimensional discrete systems in the frequency domain, *International Journal of Control*, 2013, **86**(11): 1969–1989.