Journal of Symbolic Computation 115 (2023) 248–265

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

An extended GCRD algorithm for parametric univariate polynomial matrices and application to parametric Smith form

Dingkang Wang [a,b], Hesong Wang [a,b], Jingjing Wei [a,b], Fanghui Xiao [c]

[a] *KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*
[b] *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China*
[c] *MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Hunan 410081, China*

ARTICLE INFO

Article history:
Available online 4 August 2022

Keywords:
Extended greatest common right divisor
Parametric univariate polynomial matrix
Comprehensive Gröbner system
Smith normal form

ABSTRACT

The first extended greatest common right divisor (GCRD) algorithm for parametric univariate polynomial matrices is presented. The starting point of this GCRD algorithm is the free property of submodules over univariate polynomial rings. We convert the computation of GCRDs to that of free basis for modules and prove that a free basis of the submodule generated by row vectors of input matrices forms just a GCRD of these matrices. The GCRD algorithm is obtained by computing a minimal Gröbner basis for the corresponding submodule since a minimal Gröbner basis of submodules is a free basis for univariate cases. While the key idea of extended algorithm is to construct a special module by adding the unit vectors which can record the representation coefficients. This method based on modules can be naturally generalized to the parametric case because of the comprehensive Gröbner systems for modules. As a consequence, we obtain an extended GCRD algorithm for parametric univariate polynomial matrices. More importantly, we apply the proposed extended GCD algorithm for univariate polynomials (as a special case of matrices) to the computation of Smith normal form, and give the first algorithm

E-mail addresses: dwang@mmrc.iss.ac.cn (D. Wang), wanghesong@amss.ac.cn (H. Wang), weijingjing18@mails.ucas.ac.cn (J. Wei), xiaofanghui@amss.ac.cn (F. Xiao).

https://doi.org/10.1016/j.jsc.2022.07.006

for reducing a univariate polynomial matrix with parameters to its Smith normal form.

1. Introduction

It is a basic problem in matrix theory to calculate common divisors or greatest common divisors (GCDs) of univariate polynomial matrices, which is widely used in linear system theory and dynamic system modeling (Beckermann and Labahn, 2000; Kailath, 1980; Rosenbrock, 1970). In contrast to common divisors of polynomials, multiplication of matrices is not commutative, so the left and right common divisors of a matrix are different. We focus on the greatest common right divisor (GCRD), and the results of the left common divisor (GCLD) can be obtained by similar generalization.

For non-parametric univariate matrices, the methods of solving matrix GCRDs are very mature (Hippe and Deutscher, 2009). The most common method is to merge matrices into a large matrix vertically, and then transform it into Hermite form or Popov form by row transformation. The top non-zero part of the matrix is one of GCRDs.

In addition, by Bezout identity for right coprime polynomial matrices (Kailath, 1980), GCRDs of matrices can be linearly represented by matrices with extend GCRDs. Wolovich (1974) based on the well-known extended Euclidean algorithm presented a method for solving the extended GCRD problem. Emre and Silverman (1976) gave some criteria for relatively prime polynomial matrices based on matrix fraction descriptions; Kung et al. (1976) proposed an efficient algorithm for calculating GCRDs by using the resultant matrix and Beckermann and Labahn (2000) used the interpolation algorithm to improve the calculation of extended GCRDs.

However, both the GCRD algorithm and the extended GCRD algorithm are only suitable for the case without parameters, and can not be simply extended to the case with parameters from non-parameters.

In this paper, we start from the perspective of modules and present an algorithm for computing the extended GCRD of parametric univariate polynomial matrices. We begin to present our key idea from the non-parametric case, then extend the method for computing the extended GCRD of univariate polynomial matrices to the parametric case. Unlike previous studies, we give a more strict definition of GCRD of matrices. We prove that the GCRD $\mathbf{D}$ of univariate polynomial matrices $\mathbf{M}_1, \ldots, \mathbf{M}_p$ can be obtained by computing the minimal Gröbner basis of the submodule generated by all row vectors $\{\mathbf{m}_1, \ldots, \mathbf{m}_s\}$ of these matrices. To get the representation coefficients (or multipliers) $\mathbf{U}_1, \ldots, \mathbf{U}_p$ for the GCRD expressed as a combination: $\mathbf{D} = \mathbf{U}_1\mathbf{M}_1 + \cdots + \mathbf{U}_p\mathbf{M}_p$, we construct a module generated by s row vectors $(\mathbf{m}_1, \mathbf{e}_1), \ldots, (\mathbf{m}_s, \mathbf{e}_s)$, where $\{\mathbf{e}_1, \ldots, \mathbf{e}_s\}$ is the standard basis for s-dimensional vector space, which can record the representation coefficient matrices. Under the special block order, one computes a minimal Gröbner basis of this module in which there exists some elements $(\mathbf{g}', u'_1, \ldots, u'_s)$ such that $\mathbf{g}'$ is nonzero. The matrix consisting of $\mathbf{g}'$ is exactly what we want. Most importantly, using comprehensive Gröbner systems for modules which presented by Nabeshima (2010) as the generalization of comprehensive Gröbner systems for polynomial rings studied by Weispfenning (1992), this method can be naturally extended to the parametric case. Meanwhile, we also get a free basis for the syzygy module of given polynomials $\mathbf{M}_1, \ldots, \mathbf{M}_p$ as a by-product.

In addition, our algorithm can also be applied to the computation of polynomial greatest common divisor (GCD), which is one of the most primitive computations in computer algebra with a wide range of applications that include simplifying rational expressions, partial fraction expansions, canonical transformations, mechanical geometry theorem proving, hybrid rational function approximation, and decoder implementation for error-correction (Geddes et al., 1992; Brent and Kung, 1984; Chou, 1988; Kai and Noda, 2000; Zippel, 1993). As we all know, the GCD computation for polynomials has been extensively studied and many algorithms have been constructed (Brown, 1971; Zippel, 1979; Gianni and Trager, 1985; Moses and Yun, 1973; Sasaki and Suzuki, 1992). As for parametric GCDs, there are also many researchers focusing on it and they have achieved some good results (Abramov and

Kvashenko, 1993; Ayad, 2010; Nagasaka, 2017; Kapur et al., 2018; Chen and Maza, 2012; Bächler et al., 2012). However, to our knowledge, there are two kinds of algorithms to compute the extended GCD for non-parametric univariate polynomials, but there is currently no algorithm for computing the extended parametric polynomial GCD.

In the rest of this paper, we will apply the proposed extended GCD algorithm (as a special case of matrices) to the computation of the Smith normal form together with transforming matrices. The reduction of univariate polynomial matrices to the Smith normal form is very useful in many areas of system theory (Rosenbrock, 1970; Brent and Kung, 1984; Barnett, 1971). A constructive proof of the uniqueness of the Smith form was given by Gantmacher (1959). This construction gives a basic algorithm for Smith form reduction and many other algorithms (Bradley, 1971; Pace and Barnett, 1974) based on this have been proposed with the view to improving efficiency. Moreover, Insua (2005) have presented a Gröbner basis based algorithm for the computation of Smith normal form of a matrix with entries in the univariate polynomial ring.

An essential step in the calculation of the Smith normal form is the calculation of the GCD and multipliers for each of its rows and columns. In order to get the GCD of each column (row), the algorithms in Bradley (1971); Pace and Barnett (1974) have to subtract multiples of the least degree polynomial in the corresponding column (row) of matrices, at any instant, from the others, until only one non-zero polynomial remains. The proposed extended GCD algorithm in this paper, however, can give the GCD and multipliers directly. What's more, our algorithm can be extended to the parametric case naturally, which is, to our knowledge, the first algorithm for computing the Smith normal form of polynomial matrices with parameters. Also, it's worth mentioning that Corless et al. (2017) presented an algorithm for computing the Jordan canonical form of a matrix in Frobenius (rational) canonical form where entries are polynomials with parameters.

This paper is an extension of Wang et al. (2020), and new contributions are as follows. 1) Unlike previous studies, we give a more strict definition of GCRD of matrices and convert the computation of GCRDs to that of free basis for modules. 2) Based on the construction of special modules related to matrices, we give a new method to compute the extended GCRD for univariate polynomial matrices. 3) The algorithm for computing the extended GCRDs of parameter univariate matrices is presented for the first time. The computation of polynomial GCD can be regarded as a special case of that of matrix GCRD, so the results on polynomials in (Wang et al., 2020) are corollaries of this paper.

The rest of the paper is organized as follows. In Section 2, we introduce some notations and definitions. The main results are presented in Section 3 and Section 4. In Section 3 we focus on the non-parametric case, discuss and give the method for computing GCRDs and extended GCRDs of univariate polynomial matrices. In Section 4 we extend the non-parametric results to the parametric case. Consequently the extended GCRD algorithm for parametric univariate polynomial matrices is presented. In Section 5, we apply the proposed algorithm to the computation of Smith normal form. We end with some concluding remarks in Section 6.

2. Preliminaries

In this section we will introduce some notations and definitions to prepare for the discussion of this article.

Let k be a field, L be an algebraically closed field containing k, $R = k[x]$ be the polynomial ring in the variable x (or $R = k[U][x]$ be the parametric polynomial ring with the parameters $U = \{u_1, \ldots, u_m\}$ and variable x), $R^{l\times r}$ be the set of $l \times r$ matrices with entries in R. Generally, we use the letters f, g, h for single polynomials (or elements of the ring $k[x]$), boldface letters $\mathbf{e}, \mathbf{f}, \mathbf{g}, \mathbf{h}$ for row vectors (that is, elements of the module $k[x]^s$), capital letters F, G for sets, and boldface capital letters $\mathbf{U}, \mathbf{V}$ for matrices. $\mathbf{g}^T$ and $\mathbf{U}^T$ indicate the transposition of $\mathbf{g}$ and $\mathbf{U}$, respectively.

First, we introduce the concept of the greatest common right divisor (GCRD) for a matrix. We will discuss GCRDs from the case of two matrices, and the case of more than two matrices is just a simple extension of it.

Given two matrices $\mathbf{0} \neq \mathbf{M}_1 \in R^{s_1\times r}$ and $\mathbf{M}_2 \in R^{s_2\times r}$ with the same number of columns, and $s = s_1 + s_2$.

Definition 1. The matrix $\mathbf{D} \in R^{t\times r}$ ($t \leq \min\{s, r\}$) is said to be a greatest common right divisor (GCRD) of $\mathbf{M}_1$ and $\mathbf{M}_2$ if the following conditions are satisfied.

1. $\mathbf{D}$ with full row rank is a common right divisor (CRD) of $\mathbf{M}_1$ and $\mathbf{M}_2$, i.e., there exist polynomial matrices $\mathbf{M}_1'$, $\mathbf{M}_2'$ such that
$$\mathbf{M}_1 = \mathbf{M}_1'\mathbf{D}, \quad \mathbf{M}_2 = \mathbf{M}_2'\mathbf{D}.$$
2. For any common right divisor $\mathbf{D}'$ of $\mathbf{M}_1$ and $\mathbf{M}_2$, there exists a polynomial matrix $\mathbf{S}$ such that
$$\mathbf{D} = \mathbf{S}\mathbf{D}'.$$

Obviously, $\text{rank}(\mathbf{D}) \leq \text{rank}(\mathbf{D}')$, so GCRD $\mathbf{D}$ has the minimal rank among CRDs. Further, the definition can be generalized to the case of more than two matrices.

Next, we review the concepts about modules. In practice, we frequently consider such a very important class of modules as follows.

Definition 2. Let $(\mathbf{m}_1, \ldots, \mathbf{m}_s)$ be an ordered s-tuple with $\mathbf{m}_i \in R^r$. The set of all $(a_1, \ldots, a_s) \in R^s$ such that $a_1\mathbf{m}_1 + \cdots + a_s\mathbf{m}_s = 0$ is an R-submodule of R^s, called the **syzygy module** of $(\mathbf{m}_1, \ldots, \mathbf{m}_s)$, and denoted by $\text{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_s)$.

Unlike vector spaces, modules need not have any generating set which is linearly independent. If a R-module have a module basis, that is, a generating set that is R-linearly independent, it is given a special name, **free module**.

For example, the R-module R^s is free. Let $\mathbf{e}_1 = (1, 0, \ldots, 0)$, $\mathbf{e}_2 = (0, 1, \ldots, 0)$, …, $\mathbf{e}_s = (0, 0, \ldots, 1)$, then $\{\mathbf{e}_1, \ldots, \mathbf{e}_s\}$ is a free basis of R^s. Since R is a principal ideal domain (PID), then any submodule of R^s is a free module.

Now we introduce Gröbner bases and comprehensive Gröbner systems for modules.

Let $\succ$ be a monomial order on $k[x]$, and $\succ_s$ be a module order by extending $\succ$ in a position over term (POT) fashion to $k[x]^s$ (that is, for $\alpha,\ \beta \in \mathbb{N}$, $x^\alpha\mathbf{e}_i \succ_s x^\beta\mathbf{e}_j$ if $i > j$, or $i = j$ and $x^\alpha \succ x^\beta$) or in a term over position (TOP) fashion to $k[x]^s$ (that is, for $\alpha,\ \beta \in \mathbb{N}$, $x^\alpha\mathbf{e}_i \succ_s x^\beta\mathbf{e}_j$ if $x^\alpha \succ x^\beta$ or $x^\alpha = x^\beta$ and $i > j$). For $f \in k[x], \mathbf{g} \in k[x]^s$, the leading term, leading coefficient, and leading monomial (a power product) of f and $\mathbf{g}$ with respect to $\succ$ and $\succ_s$ respectively are conveniently denoted by $\text{LT}(f)$, $\text{LC}(f)$, $\text{LM}(f)$, $\text{LT}(\mathbf{g})$, $\text{LC}(\mathbf{g})$, and $\text{LM}(\mathbf{g})$. We say $f \succ g$ if $\text{LM}(f) \succ \text{LM}(g)$, or if $\text{LM}(f) = \text{LM}(g)$ and $(f - \text{LT}(f)) \succ (g - \text{LT}(g))$, and similar to define $\mathbf{f} \succ \mathbf{g}$.

The definition of Gröbner bases for submodules is as follows.

Definition 3. Let $R = k[x]$ and M be a submodule of R^s, and let $\succ_s$ be a monomial order on $k[x]^s$.

1. We will denote by $\langle\text{LT}(M)\rangle$ the monomial submodule generated by the leading terms of all $\mathbf{g} \in M$ with respect to $\succ_s$.
2. A finite collection $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\} \subset M$ is called a **Gröbner basis** for M if $\langle\text{LT}(M)\rangle = \langle\text{LT}(\mathbf{g}_1), \ldots, \text{LT}(\mathbf{g}_t)\rangle$.

The following are about the definitions of minimal and reduced Gröbner bases for modules.

Definition 4. Let $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ be a Gröbner basis for $M \subset k[x]^s$ with respect to a monomial order $\succ_s$.

1. G is said to be **minimal**, if $\text{LM}(\mathbf{g}) \notin \langle\text{LM}(G\backslash \{\mathbf{g}\})\rangle$ for all $\mathbf{g} \in G$.
2. G is said to be **reduced**, if $\text{LC}(\mathbf{g}) = 1$ and no monomial of $\mathbf{g}$ lies in $\langle\text{LM}(G\backslash\{\mathbf{g}\})\rangle$.

Besides, we introduce some definitions for parametric univariate polynomials. For $\mathbf{g} \in k[U][x]^s$, $\text{LC}_x(\mathbf{g})$ denotes the leading coefficient of $\mathbf{g}$ with respect to the variable x under the order $\succ_s$.

A **specialization** of $k[U]$ is a homomorphism $\sigma : k[U] \to L$. In this paper, we only consider the specializations induced by the elements in L^m. That is, for $\alpha = (\alpha_1, \dots, \alpha_m) \in L^m$, the induced specialization σ_α is defined as

$$\sigma_\alpha : f \to f(\alpha),$$

where $f \in k[U]$. Every specialization $\sigma\colon k[U] \to L$ extends canonically to a specialization $\sigma\colon k[U][x]^s \to L[x]^s$ or $k[U][x]^{s\times r} \to L[x]^{s\times r}$ by applying σ coefficient-wise.

For an ideal $E \subset k[U]$, the variety defined by E in L^m is denoted by $\mathbb{V}(E) = \{\alpha \in L^m \mid f(\alpha) = 0$ for all $f \in E\}$. $A = \mathbb{V}(E) \setminus \mathbb{V}(N)$ is an algebraically constructible set, where E, N are ideals in $k[U]$.

For parametric systems, the definitions of comprehensive Gröbner systems and minimal comprehensive Gröbner systems for modules are given below.

Definition 5. Let F be a subset of $k[U][x]^s$, S be a subset of L^m, $G_1, \dots, G_l$ be subsets of $k[U][x]^s$, and $A_1, \dots, A_l$ be algebraically constructible subsets of L^m such that $S = \bigcup_{i=1}^{l} A_i$. A finite set $\mathcal{G} = \{(A_1, G_1), \dots, (A_l, G_l)\}$ is called a **comprehensive Gröbner system** (CGS) on S for F if $\sigma_\alpha(G_i)$ is a Gröbner basis of the submodule $\langle \sigma_\alpha(F)\rangle \subset L[x]^s$ with respect to $\succ_s$ for $\alpha \in A_i$ and $i = 1, \dots, l$. Each (A_i, G_i) is called a branch of $\mathcal{G}$. In particular, if $S = L^m$, then $\mathcal{G}$ is called a comprehensive Gröbner system for F.

Definition 6. A comprehensive Gröbner system $\mathcal{G} = \{(A_1, G_1), \dots, (A_l, G_l)\}$ on S for $M \subset k[U][x]^s$ is said to be **minimal** (**reduced**) under some monomial order $\succ_s$, if for each $i = 1, \dots, l$,

1. $A_i \neq \varnothing$, and furthermore, for each $i, j = 1, \dots, l$, $A_i \cap A_j = \emptyset$ whenever $i \neq j$, and
2. $\sigma_\alpha(G_i)$ is a minimal (reduced) Gröbner basis of $\langle \sigma_\alpha(F)\rangle \subset L[x]^m$ for $\alpha \in A_i$, and
3. for each $\mathbf{g} \in G_i \neq \{\mathbf{0}\}$, $\sigma_\alpha(\mathrm{LC}_x(\mathbf{g})) \neq 0$ for $\alpha \in A_i$.

Remark 7. For the computation of CGSs for modules, there exists an algorithm given by Nabeshima (2010) which is based on the results proposed by Suzuki and Sato (2006). Moreover, there exist various algorithms to compute the minimal CGS for polynomial rings; see (Kalkbrener, 1997; Montes, 2002; Suzuki and Sato, 2002, 2006; Nabeshima, 2007b,a) and so on. These algorithms can be extended to the case of modules. In this paper, we extend the KSW algorithm for computing CGSs over polynomial rings presented by Kapur et al. (2010, 2013) to the case of modules and then compute CGSs for modules since the KSW algorithm generates fewer branches and is the most efficient algorithm so far.

Finally, we introduce the GCRD systems for parametric univariate polynomial matrices.

Definition 8. Let $F = \{\mathbf{M}_1, \dots, \mathbf{M}_p\}$ with $\mathbf{M}_i \in k[U][x]^{s_i\times r}$, S be a subset of L^m and $\mathbf{D}_1, \dots, \mathbf{D}_l$ be parametric univariate polynomial matrices (where $\mathbf{D}_i \in k[U][x]^{t_i\times r}$), and $A_1, \dots, A_l$ be algebraically constructible subsets of L^m such that $S = \bigcup_{i=1}^{l} A_i$ and $A_i \cap A_j = \emptyset$ for $i \neq j$. A finite set $\mathcal{D} = \{(A_1, \mathbf{D}_1), \dots, (A_l, \mathbf{D}_l)\}$ is called a **GCRD system** on S for F if $\sigma_\alpha(\mathbf{D}_i)$ is a GCRD of $\sigma_\alpha(F)$ for $\alpha \in A_i$ and $i = 1, \dots, l$. Each $(A_i, \mathbf{D}_i)$ is regarded as a branch of $\mathcal{D}$. In particular, $\mathcal{D}$ is simply called a GCRD system for F if $S = L^m$.

3. GCRD and extended GCRD

In this section, we study GCRDs for matrices by means of the module.

3.1. GCRD for univariate polynomial matrices

Set matrix $\mathbf{M} = \begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{m}_1 \\ \vdots \\ \mathbf{m}_s \end{bmatrix}$, where $\mathbf{M}_1 \in R^{s_1 \times r}$, $\mathbf{M}_2 \in R^{s_2 \times r}$ and $s = s_1 + s_2$. Then consider the submodule $M_e \subset R^r$ generated by matrix row vectors $\mathbf{m}_i$, $i = 1, \ldots, s$. Obviously, M_e is a free module which has a free basis.

Theorem 9. *Let $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ be a free basis of M_e. Then the matrix $\mathbf{G} = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_t \end{bmatrix}$ is a GCRD of $\mathbf{M}_1$ and $\mathbf{M}_2$.*

Proof. Since $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ is a free basis of M_e, there exist $v_{ij} \in R$ such that $\mathbf{m}_i = \sum_{j=1}^{t} v_{ij} \mathbf{g}_j$ for $i = 1, \ldots, s$. Then $\begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \end{bmatrix} = \mathbf{VG} = \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \end{bmatrix} \mathbf{G}$, where $\mathbf{V} = (v_{ij})_{s \times t}, \mathbf{V}_1 \in R^{s_1 \times t}, \mathbf{V}_2 \in R^{s_2 \times t}$. That is, $\mathbf{M}_1 = \mathbf{V}_1 \mathbf{G}$ and $\mathbf{M}_2 = \mathbf{V}_2 \mathbf{G}$, which means $\mathbf{G}$ is a CRD of $\mathbf{M}_1$ and $\mathbf{M}_2$.

For every common right divisor $\mathbf{D}'$, $\begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{M}'_1 \\ \mathbf{M}'_2 \end{bmatrix} \mathbf{D}'$. Since M_e is generated by $\mathbf{m}_i$, there exist $u_{ji} \in R$ such that $\mathbf{g}_j = \sum_{i=1}^{s} u_{ji} \mathbf{m}_i$ for $j = 1, \ldots, t$. Then $\mathbf{G} = \mathbf{UM} = \mathbf{U} \begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \end{bmatrix} = \mathbf{U} \begin{bmatrix} \mathbf{M}'_1 \\ \mathbf{M}'_2 \end{bmatrix} \mathbf{D}'$, where $\mathbf{U} = (u_{ji})_{t \times s}$, so $\mathbf{G}$ is a GCRD of $\mathbf{M}_1$ and $\mathbf{M}_2$. □

Moreover, a minimal Gröbner basis under any module order is just a free basis for any submodule M_e of R^r.

Theorem 10. *Let $R = k[x]$ be a univariate polynomial ring and M_e be a submodule of R^r. If $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ is a minimal Gröbner basis for M_e under a module order $\succ_r$, then G is a free basis of M_e.*

Proof. We need to prove that the G is linearly independent over R.

Suppose that there exist $h_1, \ldots, h_t \in R$ which are not all zero such that $\sum_{i=1}^{t} h_i \mathbf{g}_i = 0$. Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r$ be the standard basis of R^r. Since G is a minimal basis, $\mathrm{LT}(\mathbf{g}_i)$ for all $i = 1, \ldots, t$ contain different standard basis vectors. That is, assume $\mathrm{LT}(\mathbf{g}_i) = c_i x^{\alpha} \mathbf{e}_i$ and $\mathrm{LT}(\mathbf{g}_j) = c_j x^{\beta} \mathbf{e}_j$, where $c_i, c_j \in k$, $i \neq j$. Thus $\mathrm{LT}(\sum_{i=1}^{t} h_i \mathbf{g}_i) = \max_i\{\mathrm{LT}(h_i \mathbf{g}_i)\} = \mathrm{LT}(h_j \mathbf{g}_j)$ for some j satisfying $h_j \neq 0$, which contradicts that $\mathrm{LT}(\sum_{i=1}^{t} h_i \mathbf{g}_i) = 0$. □

According to Theorems 9 and 10, one can obtain a GCRD of two univariate polynomial matrices by computing a minimal Gröbner basis of module generated by their row vectors. Furthermore, this approach can be easily extended to the case of more than two univariate polynomial matrices.

3.2. Extended GCRD for univariate polynomial matrices

Let $f_1, \ldots, f_s \in R$. Assume $d = \mathrm{GCD}(f_1, \ldots, f_s)$, then there are $a_1, \ldots, a_s \in R$ such that $a_1 f_1 + \cdots + a_s f_s = d$, and we call $a_1, \ldots, a_s$ **representation coefficients** for the GCD d as a R-linear combination of $f_1, \ldots, f_s$. In this paper we simply regard the GCD d together with the corresponding representation coefficients $a_1, \ldots, a_s$ as the extended GCD of $f_1, \ldots, f_s$. Similarly, we can extend this concept to the case of univariate polynomial matrices, i.e. extended GCRD. The idea is still stated from the case of two matrices to that of a finite number of matrices, then we have to solve the problem: how can we get $\mathbf{U}_1, \mathbf{U}_2$ and $\mathbf{G}$ simultaneously such that $\mathbf{U}_1 \mathbf{M}_1 + \mathbf{U}_2 \mathbf{M}_2 = \mathbf{G}$? Next, we share our approach.

Here we construct a submodule $M'_e \subset R^r \times R^s$(or equivalently, $R^r \oplus R^s$) generated by

$$\mathbf{m}'_i = \mathbf{m}_i \oplus \mathbf{e}_i = (\mathbf{m}_i, \mathbf{e}_i), \quad i = 1, \ldots, s,$$

where the unit vector set $\{\mathbf{e}_1, \dots, \mathbf{e}_s\}$ is the standard basis of R^s. According to the construction, $\mathbf{m}'_1, \dots, \mathbf{m}'_s$ are linearly independent over R, which is a free basis of M'_e. Thus, a minimal Gröbner basis G' of M'_e has s elements by Theorem 10.

Let $\{\epsilon_1, \epsilon_2, \dots, \epsilon_r\}$ be the standard basis of R^r. Let ϵ'_i and $\mathbf{e}'_j$ be the extensions of ϵ_i and $\mathbf{e}_j$ on R^{r+s} respectively, i.e., $\epsilon'_i = \epsilon_i \oplus \mathbf{0}_s$ and $\mathbf{e}'_j = \mathbf{0}_r \oplus \mathbf{e}_j$, then $\{\epsilon'_1, \dots, \epsilon'_r, \mathbf{e}'_1, \dots, \mathbf{e}'_s\}$ is the standard basis of R^{r+s}. Fix any monomial order on R^r being $\succ_r$ and any monomial order on R^s being $\succ_s$, then define a block order $\succ'$ on R^{r+s} with $\succ_r$ and $\succ_s$ satisfying:

(1) $x^\alpha \epsilon'_i \succ' x^\beta \mathbf{e}'_j$ for $1 \le i \le r$ and $1 \le j \le s$. (i.e., $\epsilon'_i \gg \mathbf{e}'_j$)

(2) $x^\alpha \epsilon'_i \succ' x^\beta \epsilon'_j$, if $x^\alpha \epsilon_i \succ_r x^\beta \epsilon_j$.

(3) $x^\alpha \mathbf{e}'_i \succ' x^\beta \mathbf{e}'_j$, if $x^\alpha \mathbf{e}_i \succ_s x^\beta \mathbf{e}_j$.

Now let's take a look at some of the properties of this module.

Proposition 11. *As above, given a block order $\succ'$ with $\succ_r$ and $\succ_s$ on R^{r+s}. Assume $G' = \{\mathbf{g}'_1, \dots, \mathbf{g}'_s\}$ is a minimal Gröbner basis for M'_e under the block order $\succ'$, and $\mathbf{g}'_i = (\mathbf{g}_i, u_{i1}, \dots, u_{is})$ with $\mathbf{0} \ne \mathbf{g}_i \in R^r$ for $1 \le i \le t$, $\mathbf{g}'_j = (\mathbf{0}_r, u_{j1}, \dots, u_{js})$ for $t+1 \le j \le s$. Let $\mathbf{u}_i = (u_{i1}, \dots, u_{is})$ for $1 \le i \le s$, then*

1. *If $(\mathbf{g}, u_1, \dots, u_s) \in M'_e$, then $\mathbf{g} = u_1 \mathbf{m}_1 + \cdots + u_s \mathbf{m}_s$ (i.e., $\mathbf{g}_i = [u_1 \ \cdots \ u_s]\mathbf{M}$).*
2. *$M'_e \cap (\{\mathbf{0}_r\} \times R^s) = \mathbf{0}_r \times \mathrm{Syz}(\mathbf{m}_1, \dots, \mathbf{m}_s)$.*
3. *The set $G = \{\mathbf{g} \in R^r \,|\, \mathbf{g} \ne \mathbf{0} \wedge \exists\, u_1, \dots, u_s \in R$ suchthat $(\mathbf{g}, u_1, \dots, u_s) \in G'\} = \{\mathbf{g}_1, \dots, \mathbf{g}_t\}$ is a minimal Gröbner basis for $M_e = \langle \mathbf{m}_1, \dots, \mathbf{m}_s \rangle$ with respect to $\succ_r$.*
4. *The set $G_0 = \{\mathbf{u}_{t+1}, \dots, \mathbf{u}_s\}$ defined by $\{\mathbf{0}_r\} \times G_0 = G' \cap (\{\mathbf{0}_r\} \times R^s)$ is a minimal Gröbner basis for $\mathrm{Syz}(\mathbf{m}_1, \dots, \mathbf{m}_s)$ with respect to $\succ_s$.*

Proof. By the construction of M'_e, 1 and 2 are obvious. For 3, it follows from Theorem 10 that G' is a free basis of M'_e. Based on the block order $\succ'$, $(\mathbf{g}_i, \mathbf{u}_i) \succ' (\mathbf{0}, \mathbf{u}_j)$ and $\mathrm{LT}((\mathbf{g}_i, \mathbf{u}_i)) = \mathrm{LT}((\mathbf{g}_i) \oplus \mathbf{0}_s$ for $\mathbf{0} \ne \mathbf{g}_i \in M_e, \mathbf{u}_i, \mathbf{u}_j \in R^s$, then $\mathrm{LT}(G) \times \{\mathbf{0}_s\} \subset \mathrm{LT}(G')$ and $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(M_e) \rangle$, which means G is a Gröbner basis for M_e. According to the definition of the block order: $x^\alpha \epsilon'_i \succ' x^\beta \epsilon'_j$ if and only if $x^\alpha \epsilon_i \succ_r x^\beta \epsilon_j$, $\mathrm{LT}(G)$ is a minimal Gröbner basis for M_e under $\succ_r$ since G' is a minimal Gröbner basis for M'_e under $\succ'$. As for 4, it's similar to 3. $(\mathbf{0}, \mathbf{u}_i) \succ' (\mathbf{0}, \mathbf{u}_j)$ if and only if $\mathbf{u}_i \succ_s \mathbf{u}_j$, so $\{\mathbf{u}_{t+1}, \dots, \mathbf{u}_s\}$ is a minimal Gröbner basis for $\mathrm{Syz}(\mathbf{m}_1, \dots, \mathbf{m}_s)$ with respect to the order $\succ_s$. □

Based on the above properties, we get the following results.

Theorem 12. *Assume $G' = \{\mathbf{g}'_1, \dots, \mathbf{g}'_s\}$ is a minimal Gröbner basis for M'_e under the block order $\succ'$, and $\mathbf{g}'_i = (\mathbf{g}_i, u_{i1}, \dots, u_{is})$ with $\mathbf{0} \ne \mathbf{g}_i \in R^r$ for $1 \le i \le t$, $\mathbf{g}'_j = (\mathbf{0}_r, u_{j1}, \dots, u_{js})$ for $t+1 \le j \le s$. Let $\mathbf{u}_i = (u_{i1}, \dots, u_{is})$ for $1 \le i \le s$, then*

1. *$\mathbf{G} = \left[\mathbf{g}_1^T \ \cdots \ \mathbf{g}_t^T\right]^T$ is a GCRD of $\mathbf{M}_1$ and $\mathbf{M}_2$.*
2. *$\mathbf{U}_1$ and $\mathbf{U}_2$ are the corresponding representation coefficient matrices for $\mathbf{G}$ as a combination of $\mathbf{M}_1$ and $\mathbf{M}_2$ (i.e., $\mathbf{U}_1\mathbf{M}_1 + \mathbf{U}_2\mathbf{M}_2 = \mathbf{G}$), where*

$$\mathbf{U}_1 = \begin{bmatrix} u_{11} & \cdots & u_{1s_1} \\ \vdots & \ddots & \vdots \\ u_{t1} & \cdots & u_{ts_1} \end{bmatrix}_{t \times s_1}, \quad \mathbf{U}_2 = \begin{bmatrix} u_{1(s_1+1)} & \cdots & u_{1s} \\ \vdots & \ddots & \vdots \\ u_{t(s_1+1)} & \cdots & u_{ts} \end{bmatrix}_{t \times s_2}$$

3. *$\mathbf{U} = (u_{ij})_{s \times s}$ is unimodular, that is, $\det(\mathbf{U}) \in k \setminus \{0\}$. Besides, let $\hat{\mathbf{G}} = \left[\mathbf{g}_1^T \ \cdots \ \mathbf{g}_s^T\right]^T$, where $\mathbf{g}_j = \mathbf{0}_r$ for $t+1 \le j \le s$, then $\mathbf{U}\mathbf{M} = \hat{\mathbf{G}}$.*

Proof. (1) According to Proposition 11, $G = \{\mathbf{g}_1, \dots, \mathbf{g}_t\}$ is a minimal Gröbner basis for M_e, then it is also a free basis, which implies that $\mathbf{G} = \left[\mathbf{g}_1^T \ \cdots \ \mathbf{g}_t^T\right]^T$ is a GCRD of $\mathbf{M}_1$ and $\mathbf{M}_2$.

(2) Let $\hat{\mathbf{G}} = \begin{bmatrix} \mathbf{g}_1^T & \cdots & \mathbf{g}_s^T \end{bmatrix}^T$, where $\mathbf{g}_j = \mathbf{0}_r$ for $t+1 \le j \le s$, then

$$\begin{bmatrix} \mathbf{g}_1' \\ \mathbf{g}_2' \\ \vdots \\ \mathbf{g}_s' \end{bmatrix} = \begin{bmatrix} \hat{\mathbf{G}} & \mathbf{U} \end{bmatrix} = \mathbf{U} \begin{bmatrix} \mathbf{M} & \mathbf{E}_s \end{bmatrix},$$

where $\mathbf{E}_s$ is the $s \times s$ identity matrix. So

$$\hat{\mathbf{G}} = \begin{bmatrix} \mathbf{G} \\ \mathbf{0} \end{bmatrix} = \mathbf{UM} = \begin{bmatrix} \mathbf{U_1} & \mathbf{U_2} \\ \mathbf{U_3} & \mathbf{U_4} \end{bmatrix} \begin{bmatrix} \mathbf{M_1} \\ \mathbf{M_2} \end{bmatrix}.$$

Then

$$\mathbf{G} = \mathbf{U}_1\mathbf{M}_1 + \mathbf{U}_2\mathbf{M}_2,$$

where $\mathbf{U}_1 \in R^{t \times s_1}, \mathbf{U_2} \in R^{t \times s_2}$.

(3) It's obvious that $\mathbf{UM} = \hat{\mathbf{G}}$. Since $G' = \{\mathbf{g}_1', \dots, \mathbf{g}_s'\}$ is the minimal Gröbner basis for M_e', hence these generators $\mathbf{m}_1', \dots, \mathbf{m}_s'$ of M_e' can be represented by $\mathbf{g}_1', \dots, \mathbf{g}_s'$. In other words, there exists matrix $\mathbf{V} \in k[x]^{s \times s}$ such that

$$\begin{bmatrix} \mathbf{M} & \mathbf{E}_s \end{bmatrix} = \mathbf{V} \begin{bmatrix} \mathbf{g}_1' \\ \vdots \\ \mathbf{g}_s' \end{bmatrix} = \mathbf{V} \begin{bmatrix} \mathbf{g}_1 & \mathbf{u}_1 \\ \vdots & \vdots \\ \mathbf{g}_s & \mathbf{u}_s \end{bmatrix} = \mathbf{V} \begin{bmatrix} \hat{\mathbf{G}} & \mathbf{U} \end{bmatrix}.$$

So $\mathbf{VU} = \mathbf{E}_s$. Thus $\mathbf{V}$ and $\mathbf{U}$ are unimodular. □

Based on the results of Theorem 12, we can design an algorithm to compute the GCRD of $\mathbf{M_1}$ and $\mathbf{M}_2$, and unimodular matrix $\mathbf{U}$, where the first t row submatrices $\mathbf{U}_1 \in R^{t \times s_1}, \mathbf{U_2} \in R^{t \times s_2}$ of $\mathbf{U}$ are the representation coefficient matrices. That is, we only need to construct the module M_e' by inputting polynomial matrices $\mathbf{M}_1, \mathbf{M_2}$ and then compute a minimal Gröbner basis for M_e' with respect to $\succ'$. Moreover, the computation of the extended GCRD for a finite number of matrices follows by it.

4. Extended GCRD systems for parametric univariate polynomial matrices

As stated in the introduction, there is currently no algorithm for computing extended GCRD of parametric univariate polynomial matrices. In this section, we are devoted to giving an extended GCRD algorithm for parametric univariate polynomial matrices.

Now we are ready to generalize the above method to the parametric case by means of the CGS for modules.

Given $\mathbf{M}_1, \dots, \mathbf{M}_p$ with $\mathbf{M}_i \in k[U][x]^{s_i \times r}$ and $s_1 + \dots + s_p = s$ for $1 \le i \le p$. Let $R = k[U][x]$, $M_e \subset R^r$ be the submodule generated by all row vectors $\mathbf{m}_j$ of $\mathbf{M}_i$ for all $i = 1, \dots, p$, $M_e' \subset R^r \times R^s$ be the submodule generated by $\mathbf{m}_j' = \mathbf{m}_j \oplus \mathbf{e}_j$ for $j = 1, \dots, s$. We get the following result.

Theorem 13. *Given a subset $S \subset L^m$. Let $\mathcal{G} = \left\{(A_i, G_i')\right\}_{i=1}^{l}$ be a minimal comprehensive Gröbner system of the module $M_e' \subset R^r \times R^s$ on S with respect to the block order $\succ'$. For each branch (A_i, G_i'), $|G_i'| = s$, where "$|\cdot|$" represents the number of elements in the set. And we have the following results.*

1. *Let $G_i = \{\mathbf{g} \in R^r | \, \mathbf{g} \neq \mathbf{0} \wedge \exists \, u_1, \dots, u_s \in R$ suchthat $(\mathbf{g}, u_1, \dots, u_s) \in G_i'\}$, then $\sigma_\alpha(G_i) \neq \emptyset$ is a minimal Gröbner basis of $\sigma_\alpha(M_e) = \langle \sigma_\alpha(\mathbf{m}_1), \dots, \sigma_\alpha(\mathbf{m}_s) \rangle$ with respect to $\succ_r$ for any $\alpha \in A_i$.*
2. *Let G_{0i} be a set defined by $\{\mathbf{0}_r\} \times G_{0i} = G_i' \cap (\{\mathbf{0}_r\} \times R^s)$, then $\sigma_\alpha(G_{0i})$ is a minimal Gröbner basis of* $\mathrm{Syz}(\sigma_\alpha(\mathbf{m}_1), \dots, \sigma_\alpha(\mathbf{m}_s))$ *with respect to $\succ_s$ for any $\alpha \in A_i$.*

Algorithm 1: Parametric extended GCRD algorithm.

```
Input  : $\mathbf{M}_1, \ldots, \mathbf{M}_p$ with $\mathbf{M}_i \in k[U][x]^{s_i \times r}$ and $s_1 + \cdots + s_p = s$ for $1 \le i \le p$, a constructible set $S \subset L^m$, and a block
         order $\succ'$.
Output: an extended GCRD system $\{(A_i, \mathbf{U}_i, \mathbf{G}_i)_{i=1}^{l}\}$, where $\sigma_\alpha(\mathbf{U}_i)$ is unimodular and
         $\mathrm{GCRD}(\sigma_\alpha(\mathbf{M}_1), \ldots, \sigma_\alpha(\mathbf{M}_p)) = \sigma_\alpha(\mathbf{G}_i)$ for any $\alpha \in A_i$.
begin
    compute a minimal CGS $\{(A_i, G_i')_{i=1}^{l}\}$ for the module $M_e' = \langle \mathbf{m}_1', \ldots, \mathbf{m}_s' \rangle$ w.r.t. $\succ'$;
    for i from 1 to l do
        $G_i' = \{(\mathbf{g}_1, \mathbf{u}_1), \ldots, (\mathbf{g}_{t_i}, \mathbf{u}_{t_i}), (\mathbf{0}, \mathbf{u}_{t_i+1}), \ldots, (\mathbf{0}, \mathbf{u}_s)\}$;
        $\mathbf{U}_i := (u_{\ell j})_{s \times s}$, where $\mathbf{u}_\ell = (u_{\ell 1}, u_{\ell 2}, \ldots, u_{\ell s})$ for $1 \le \ell, j \le s$;
        $\mathbf{G}_i := [\mathbf{g}_1^T \ \cdots \ \mathbf{g}_{t_i}^T]^T$;
    return $\{(A_i, \mathbf{U}_i, \mathbf{G}_i)\}_{i=1}^{l}$;
```

3. *Assume $G_i' = \{\mathbf{g}_1', \ldots, \mathbf{g}_s'\}$ and $\mathbf{g}_\ell' = (\mathbf{g}_\ell, u_{\ell 1}, \ldots, u_{\ell s})$ with $\mathbf{0} \neq \mathbf{g}_\ell \in R^r$ for $1 \le \ell \le t_i$, $\mathbf{g}_j' = (\mathbf{0}_r, u_{j1}, \ldots, u_{js})$ for $t_i + 1 \le j \le s$. Then $\sigma_\alpha(\mathbf{G}_i)$ is a GCRD of $\sigma_\alpha(\mathbf{M}_1), \ldots, \sigma_\alpha(\mathbf{M}_p)$ and $\sigma_\alpha(\mathbf{U}_{i1}), \ldots, \sigma_\alpha(\mathbf{U}_{ip})$ are the representation coefficient matrices for $\sigma_\alpha(\mathbf{G}_i)$ as a combination of $\sigma_\alpha(\mathbf{M}_1), \ldots, \sigma_\alpha(\mathbf{M}_p)$. Moreover, assume $\mathbf{U}_i = (u_{\ell j})_{s \times s}$, then $\sigma_\alpha(\mathbf{U}_i)\sigma_\alpha(\mathbf{M}) = \sigma_\alpha(\hat{\mathbf{G}}_i)$ and $\sigma_\alpha(\mathbf{U}_i)$ is unimodular for any $\alpha \in A_i$, where $\mathbf{U}_{i\nu} \in R^{t_i \times s_\nu}$ for $\nu = 1, \ldots, p$,*

$$\mathbf{G}_i = \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{t_i} \end{bmatrix}, \ \hat{\mathbf{G}}_i = \begin{bmatrix} \mathbf{G}_i \\ \mathbf{0} \end{bmatrix}_{s \times r}, \ \mathbf{U}_i = \begin{bmatrix} u_{11} & \cdots & u_{1s} \\ \vdots & \cdots & \vdots \\ u_{s1} & \cdots & u_{ss} \end{bmatrix} = \begin{bmatrix} \mathbf{U}_{i1} & \cdots & \mathbf{U}_{ip} \\ \mathbf{U}_{i1}' & \cdots & \mathbf{U}_{ip}' \end{bmatrix}, \ \mathbf{M} = \begin{bmatrix} \mathbf{M}_1 \\ \vdots \\ \mathbf{M}_p \end{bmatrix}.$$

Particularly, for the branch (A_i, G_i') with $G_i = \emptyset$, $\sigma_\alpha(\mathbf{G}_i) = \mathbf{0}$ and $\sigma_\alpha(\mathbf{U}_i) = \mathbf{E}_s$ for $\alpha \in A_i$. In this case, the corresponding syzygy module $\mathrm{Syz}(\sigma_\alpha(\mathbf{m}_1), \ldots, \sigma_\alpha(\mathbf{m}_s))$ *is* $k[x]^s$.

Proof. Since $\mathcal{G}$ is a minimal comprehensive Gröbner system, in each branch (A_i, G_i'), $\sigma_\alpha(G_i')$ is a minimal Gröbner basis of $\sigma_\alpha(M_e')$ for any $\alpha \in A_i$. Besides, there is no element in G_i' specializing to $\mathbf{0}$ because the leading coefficients of all elements in G_i' are non-zero under specialization. Thus, it is easy to derive the results from Theorem 10, Proposition 11 and Theorem 12. □

4.1. Algorithm

Based on Theorem 13, we are ready to give an algorithm to compute the extended GCRD system for parametric univariate polynomial matrices.

Theorem 14. *Algorithm 1 works correctly and terminates.*

Proof. The correctness of Algorithm 1 directly follows from Theorem 13, and the termination of Algorithm 1 fully depends on that of the algorithm for computing CGSs of the module M_e' which is obviously derived from the termination of the KSW algorithm as mentioned in Remark 7. □

Remark 15. For each $(A_i, \mathbf{U}_i, \mathbf{G}_i)$, the first t_i row submatrices $\mathbf{U}_{i1} \in R^{t_i \times s_1}, \mathbf{U}_{i2} \in R^{t_i \times s_2}, \ldots, \mathbf{U}_{ip} \in R^{t_i \times s_p}$ in $\mathbf{U}_i$ are the representation coefficient matrices of $\mathbf{G}_i$ under the specialization.

Here a simple example is presented to illustrate the steps in Algorithm 1.

Example 16. Let $\mathbf{M}_1, \mathbf{M}_2 \in \mathbb{C}[U][x]^{2 \times 2}$ be as follows:

$$\mathbf{M}_1 = \begin{bmatrix} (x-a) & 0 \\ 0 & x(x-b) \end{bmatrix} = \begin{bmatrix} \mathbf{m}_1 \\ \mathbf{m}_2 \end{bmatrix}, \quad \mathbf{M}_2 = \begin{bmatrix} x(x-b) & 0 \\ 0 & (x-a)^2 \end{bmatrix} = \begin{bmatrix} \mathbf{m}_3 \\ \mathbf{m}_4 \end{bmatrix}$$

where $U = \{a, b\}$ and $\succ$ is a lexicographic order with respect to $x \succ a \succ b$.

Table 1
A minimal CGS $\mathcal{G}$ for the module M_e'.

No.	A_i	G_i'
1	$\mathbb{C}^2 \backslash \mathbb{V}(a(a-b))$	G_1'
2	$\mathbb{V}(a) \backslash \mathbb{V}(b)$	G_2'
3	$\mathbb{V}(a-b) \backslash \mathbb{V}(ab)$	G_3'
4	$\mathbb{V}(a,b)$	G_4'

Table 2
The extended GCRD system of $\{\mathbf{M}_1, \mathbf{M}_2\}$.

No.	A_i	$[\mathbf{U}_{i1}, \mathbf{U}_{i2}]$	$\mathbf{D}_i$
1	$\mathbb{C}^2 \backslash \mathbb{V}(a(a-b))$	$[\mathbf{U}_{11}, \mathbf{U}_{12}]$	$\mathbf{D}_1$
2	$\mathbb{V}(a) \backslash \mathbb{V}(b)$	$[\mathbf{U}_{21}, \mathbf{U}_{22}]$	$\mathbf{D}_2$
3	$\mathbb{V}(a-b) \backslash \mathbb{V}(ab)$	$[\mathbf{U}_{31}, \mathbf{U}_{32}]$	$\mathbf{D}_3$
4	$\mathbb{V}(a,b)$	$[\mathbf{U}_{41}, \mathbf{U}_{42}]$	$\mathbf{D}_4$

Step 1: we compute a minimal CGS $\mathcal{G}$ for the module $M_e' = \langle \mathbf{m}_1 \oplus \mathbf{e}_1, \mathbf{m}_2 \oplus \mathbf{e}_2, \mathbf{m}_3 \oplus \mathbf{e}_3, \mathbf{m}_4 \oplus \mathbf{e}_4 \rangle \subset \mathbb{C}[a,b][x]^6$ with a block order $\succ'$ with $\succ_2$ and $\succ_4$ where $\succ_2$ is POT extension of $\succ$ on $\mathbb{C}[a,b][x]^2$ with standard basis $\epsilon_1 \succ_2 \epsilon_2$ and $\succ_4$ is POT extension of $\succ$ on $\mathbb{C}[a,b][x]^4$ with $\mathbf{e}_1 \succ_4 \mathbf{e}_2 \succ_4 \mathbf{e}_3 \succ_4 \mathbf{e}_4$ (Table 1).

$$\begin{aligned} G_1' =& \{(a^2-ab)\epsilon_1' + (-x-a+b)\mathbf{e}_1' + \mathbf{e}_3', \\ & (a^4-2a^3b+a^2b^2)\epsilon_2' + (3a^2-2ab-2ax+xb)\mathbf{e}_2' + (a^2-2ab+2ax+b^2-bx)\mathbf{e}_4', \\ & (-bx+x^2)\mathbf{e}_1' + (a-x)\mathbf{e}_3',\ (a^2-2ax+x^2)\mathbf{e}_2' + (bx-x^2)\mathbf{e}_4'\}; \\ G_2' =& \{x\epsilon_1' + \mathbf{e}_1',\ xb\epsilon_2' - \mathbf{e}_2' + \mathbf{e}_4',\ (x-b)\mathbf{e}_1' - \mathbf{e}_3',\ x\mathbf{e}_2' + (b-x)\mathbf{e}_4'\}; \\ G_3' =& \{(x-b)\epsilon_1' + \mathbf{e}_1',\ (-b^2+bx)\epsilon_2' + \mathbf{e}_2' - \mathbf{e}_4',\ x\mathbf{e}_1' - \mathbf{e}_3',\ (x-b)\mathbf{e}_2' - x\mathbf{e}_4'\}; \\ G_4' =& \{x\epsilon_1' + \mathbf{e}_1',\ x^2\epsilon_2' + \mathbf{e}_4', \mathbf{e}_1' - \mathbf{e}_3', \mathbf{e}_2' - \mathbf{e}_4'\}. \end{aligned}$$

Step 2: according to G_i' in the minimal CGS for module M_e', we obtain the following extended GCRD system of $\{\mathbf{M}_1, \mathbf{M}_2\}$. Where $\mathbf{U}_{i1}\mathbf{M}_1 + \mathbf{U}_{i2}\mathbf{M}_2 = \mathbf{G}_i = \mathbf{D}_i$ for $i = 1, 2, 3, 4$ (Table 2),

$$\begin{aligned} &\mathbf{U}_{11} = \begin{bmatrix} -a+b-x & 0 \\ 0 & u_{114} \end{bmatrix}, \quad \mathbf{U}_{12} = \begin{bmatrix} 1 & 0 \\ 0 & u_{124} \end{bmatrix}, \quad \mathbf{D}_1 = \begin{bmatrix} a^2-ab & 0 \\ 0 & a^4-2a^3b+a^2b^2 \end{bmatrix}, \\ &\mathbf{U}_{21} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathbf{U}_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{D}_2 = \begin{bmatrix} x & 0 \\ 0 & xb \end{bmatrix}, \\ &\mathbf{U}_{31} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{U}_{32} = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathbf{D}_3 = \begin{bmatrix} x-b & 0 \\ 0 & -b^2+bx \end{bmatrix}, \\ &\mathbf{U}_{41} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{U}_{42} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{D}_4 = \begin{bmatrix} x & 0 \\ 0 & x^2 \end{bmatrix}, \\ &u_{114} = 3a^2-2ab-2ax+bx, \\ &u_{124} = a^2-2ab+2ax+b^2-bx. \end{aligned}$$

In summary, parametric GCRDs are expressed as the combinations of $\mathbf{M}_1, \mathbf{M}_2$ as follows.

$$\begin{cases} \textit{if } a \neq b \textit{ and } b \neq 0, & \mathbf{U}_{11}\mathbf{M}_1 + \mathbf{U}_{12}\mathbf{M}_2 = \mathbf{D}_1; \\ \textit{if } a = 0 \textit{ and } b \neq 0, & \mathbf{U}_{21}\mathbf{M}_1 + \mathbf{U}_{22}\mathbf{M}_2 = \mathbf{D}_2; \\ \textit{if } a = b \textit{ and } ab \neq 0, & \mathbf{U}_{31}\mathbf{M}_1 + \mathbf{U}_{32}\mathbf{M}_2 = \mathbf{D}_3; \\ \textit{if } a = 0 \textit{ and } b = 0, & \mathbf{U}_{41}\mathbf{M}_1 + \mathbf{U}_{42}\mathbf{M}_2 = \mathbf{D}_4. \end{cases}$$

4.2. Extended GCD system for parametric univariate polynomials

Similar to GCRD systems for parametric univariate polynomial matrices, the definition of GCD systems for parametric univariate polynomials is as follows.

Definition 17. Let $F = \{f_1, \dots, f_s\}$ be a subset of $k[U][x]$, S be a subset of L^m and $d_1, \dots, d_l$ be parametric univariate polynomials in $k[U][x]$, and $A_1, \dots, A_l$ be algebraically constructible subsets of L^m such that $S = \bigcup_{i=1}^{l} A_i$ and $A_i \cap A_j = \emptyset$ for $i \neq j$. A finite set $\mathcal{D} = \{(A_1, d_1), \dots, (A_l, d_l)\}$ is called a **GCD system** on S for F if $\sigma_\alpha(d_i)$ is a GCD of $\sigma_\alpha(F) \subset L[x]$ for $\alpha \in A_i$ and $i = 1, \dots, l$. Moreover, for each $d_i \neq 0$, $\sigma_\alpha(\mathrm{LC}_x(d_i)) \neq 0$ for $\alpha \in A_i$. Each (A_i, d_i) is regarded as a branch of $\mathcal{D}$. In particular, $\mathcal{D}$ is simply called a GCD system for F if $S = L^m$.

Actually, GCDs (GCD systems) for non-parametric (parametric) univariate polynomials is a special case of GCRDs (GCRD systems) for non-parametric (parametric) univariate polynomial matrices, i.e., $r = s_i = t_j = 1$ for $1 \le i \le p, 1 \le j \le l$ in Definition 8. So the computing idea of (extended) GCRDs and GCRD systems by means of the module, as well as Gröbner basis and CGS for modules, is suitable for the polynomial case (1-dimensional case for modules).

Given $f_1, \dots, f_s \in k[x]$, then $M'_e = \langle (f_1, \mathbf{e}_1), \dots, (f_s, \mathbf{e}_s) \rangle$. The block order $\succ'$ can be adapted to $\succ_{s+1}$ which is a POT order on $k[x]^{s+1}$ by regarding f_i in the 0-th component with $\mathbf{e}'_0 \succ \mathbf{e}'_i$ for $1 \le i \le s$, where unit vector set $\{\mathbf{e}'_0, \mathbf{e}'_1, \dots, \mathbf{e}'_s\}$ is the standard basis of $k[x]^{s+1}$.

Consequently, we have the following corollaries (of Theorem 12 and Theorem 13).

Corollary 18. *Assume $G' = \{\mathbf{g}'_1, \dots, \mathbf{g}'_s\}$ is a minimal Gröbner basis for $M'_e \subset k[x]^{s+1}$ under the order $\succ_{s+1}$ with $\mathbf{e}'_0 \succ \mathbf{e}'_i$ for $1 \le i \le s$, and $\mathbf{g}'_1 = (d, u_{11}, \dots, u_{1s})$, $\mathbf{g}'_j = (0, u_{j1}, \dots, u_{js})$, $2 \le j \le s$. Then d is a GCD of $f_1, \dots, f_s$ and $u_{11}, \dots, u_{1s}$ are the corresponding representation coefficients for d as a $k[x]$-linear combination of $f_1, \dots, f_s$. Further, the matrix $\mathbf{U} = \left(u_{\ell j}\right)_{s \times s} \in k[x]^{s \times s}$ is unimodular, that is, $\det(\mathbf{U}) \in k \setminus \{0\}$, and $\mathbf{UF} = \mathbf{D}$, where*

$$\mathbf{U} = \begin{bmatrix} u_{11} & \cdots & u_{1s} \\ u_{21} & \cdots & u_{2s} \\ \vdots & \cdots & \vdots \\ u_{s1} & \cdots & u_{ss} \end{bmatrix}, \quad \mathbf{F} = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_s \end{bmatrix}, \quad \mathbf{D} = \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Naturally, we obtain an algorithm to compute the GCD of $f_1, \dots, f_s$ and unimodular matrix $\mathbf{U}$ by computing a minimal Gröbner basis for M'_e with respect to $\succ_{s+1}$, where the first row $u_{11}, \dots, u_{1s}$ of $\mathbf{U}$ are the representation coefficients.

Corollary 19. *Given $f_1, \dots, f_s \in k[U][x]$ and a subset $S \subset L^m$. Let $\mathcal{G} = \left\{(A_i, G'_i)\right\}_{i=1}^{l}$ be a minimal comprehensive Gröbner system of the module $M'_e = \langle f_1\mathbf{e}'_0 + \mathbf{e}'_1, \dots, f_s\mathbf{e}'_0 + \mathbf{e}'_s \rangle \subset k[U][x]^{s+1}$ on S with respect to an order $\succ_{s+1}$ with $\mathbf{e}'_0 \succ \mathbf{e}'_i$ for $1 \le i \le s$. For each branch (A'_i, G'_i), $|G'_i| = s$, and we have the following results.*

1. *Let $G_i = \{g \in k[U][x] |\ g \neq 0\ \wedge \exists\, h_1, \dots, h_s \in k[U][x]$ suchthat $(g, h_1, \dots, h_s) \in G'_i\}$, then $\sigma_\alpha(G_i)$ is a minimal Gröbner basis of the ideal $\langle \sigma_\alpha(f_1), \dots, \sigma_\alpha(f_s) \rangle$ with respect to $\succ$ on $k[x]$ for any $\alpha \in A_i$, and $|G_i| = 1$.*
2. *Let G_{0i} be a set defined by $\{0\} \times G_{0i} = G'_i \cap (\{0\} \times k[U][x]^s)$, then $\sigma_\alpha(G_{0i})$ is a minimal Gröbner basis of the syzygy module $\mathrm{Syz}(\sigma_\alpha(\mathrm{f}_1), \dots, \sigma_\alpha(\mathrm{f}_s))$ with respect to $\succ_s$ for any $\alpha \in A_i$, and $|G_{0i}| = s - 1$.*
3. *Assume $G'_i = \{\mathbf{g}'_1, \dots, \mathbf{g}'_s\}$ and $\mathbf{g}'_1 = (d_i, u_{11}, \dots, u_{1s})$, $\mathbf{g}'_j = (0, u_{j1}, \dots, u_{js})$ for $2 \le j \le s$. Then $\sigma_\alpha(d_i)$ is a GCD of $\sigma_\alpha(f_1), \dots, \sigma_\alpha(f_s)$ and $\sigma_\alpha(u_{11}), \dots, \sigma_\alpha(u_{1s})$ are the representation coefficients for $\sigma_\alpha(d_i)$ as a $k[x]$-linear combination of $\sigma_\alpha(f_1), \dots, \sigma_\alpha(f_s)$. Moreover, assume the matrix $\mathbf{U}_i = \left(u_{\ell j}\right)_{s \times s}$, then $\sigma_\alpha(\mathbf{U}_i)\sigma_\alpha(\mathbf{F}) = \sigma_\alpha(\mathbf{D}_i)$ and $\sigma_\alpha(\mathbf{U}_i)$ is unimodular for any $\alpha \in A_i$, where*

$$\mathbf{U} = \begin{bmatrix} u_{11} & \cdots & u_{1s} \\ u_{21} & \cdots & u_{2s} \\ \vdots & \cdots & \vdots \\ u_{s1} & \cdots & u_{ss} \end{bmatrix}, \quad \mathbf{F} = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_s \end{bmatrix}, \quad \mathbf{D}_i = \begin{bmatrix} d_i \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Particularly, for the branch (A_i, G_i') with $G_i = \emptyset$, $\sigma_\alpha(d_i) = 0$ and $\sigma_\alpha(\mathbf{U}_i) = \mathbf{E}_s$ for $\alpha \in A_i$. In this case, the corresponding syzygy module $\mathrm{Syz}(\sigma_\alpha(\mathrm{f}_1), \ldots, \sigma_\alpha(\mathrm{f}_s))$ *is* $k[x]^s$.

Remark 20. For polynomial cases, since $k[x]$ is a principal ideal domain (PID), a minimal Gröbner basis of any ideal on $k[x]$ has only one element. As a result, $|G_i| = s-1$, $|G_{0i}| = s-1$.

Similarly, Algorithm 1 is also suitable for computing an extended GCD system of parametric univariate polynomials. One inputs $f_1, \ldots, f_s \in k[U][x]$, a constructible set $S \subset L^m$, and a POT order $\succ_{s+1}$ with $\mathbf{e}_0' \succ \mathbf{e}_i', 1 \le i \le s$, then an extended GCD system $\{(A_i, \mathbf{U}_i, d_i)_{i=1}^l\}$ is output, where $\mathrm{GCD}(\sigma_\alpha(f_1), \ldots, \sigma_\alpha(f_s)) = \sigma_\alpha(d_i)$, $\sigma_\alpha(\mathbf{U}_i)$ is unimodular and the components of the first row vector in $\sigma_\alpha(\mathbf{U}_i)$ are the representation coefficients of $\sigma_\alpha(d_i)$ for any $\alpha \in A_i$.

5. Application to Smith normal form

5.1. Notations and definitions

In this subsection, we give some definitions and notations related to the Smith normal form. A matrix is called non-parametric (parametric) univariate polynomial matrix if its entries belong to $k[x]$ ($k[U][x]$).

Definition 21. Let $\mathbf{D}$ be an $s \times t$ matrix over $k[x]$ such that

1. all (i, j)-entries in $\mathbf{D}$ are zero for $i \neq j$, that is, $\mathbf{D}$ is a diagonal matrix;
2. each (i, i)-entry d_i in $\mathbf{D}$ is either monic or zero;
3. $d_i \mid d_{i+1}$ for $1 \le i < min\{s, t\}$.

Then $\mathbf{D}$ is said to be in Smith normal form.

In addition, we give the following theorem appearing in Norman (2012) which shows that any univariate polynomial matrix $\mathbf{B}$ can be reduced to its Smith normal form $S(\mathbf{B})$.

Theorem 22. *Let* $\mathbf{B}$ *be an* $s \times t$ *matrix over* $k[x]$*, then there is a sequence of elementary operations over* $k[x]$ *which changes* $\mathbf{B}$ *into* $S(\mathbf{B})$ *that is in Smith normal form, i.e., the Smith normal form of* $\mathbf{B}$*.*

That is, there exist unimodular matrices $\mathbf{U} \in k[x]^{s\times s}$, $\mathbf{V} \in k[x]^{t\times t}$ such that $\mathbf{UBV} = S(\mathbf{B})$.

5.2. The Smith normal form of parametric univariate polynomial matrix

For the non-parametric case, as stated in Theorem 22 any univariate polynomial matrix can be reduced to its Smith normal form under the elementary operations. As for the parametric case, corresponding to each algebraically constructible subset $A_i \subset L^m$, the parametric univariate polynomials matrix under the specialization σ_α can be reduced to its Smith normal form by elementary operations, i.e., there exist parametric unimodular matrices $\mathbf{U} \in k[U][x]^{s\times s}$, $\mathbf{V} \in k[U][x]^{t\times t}$ such that $\sigma_\alpha(\mathbf{U})\sigma_\alpha(\mathbf{B})\sigma_\alpha(\mathbf{V}) = S(\sigma_\alpha(\mathbf{B}))$ for $\alpha \in A_i$. Now we discuss how to reduce a univariate polynomials matrix to its Smith normal form.

In the above section, we have proposed an extended GCD algorithm which not only can output the GCD, but also gives a unimodular matrix $\mathbf{U}$. In particular, $\mathbf{U}[f_1, f_2, \ldots, f_s]^T = [d, 0, \ldots, 0]^T$, where

$f_1, \dots, f_s$ are given polynomials and d is the GCD of these polynomials. Then, we can apply the extended GCD algorithm to the calculation of the Smith normal form, and the actual practice is as follows.

Given $\mathbf{B} \in k[x]^{s\times t}$ (without loss of generality, assume $s \le t$), we first call the extended GCD algorithm on the first column of $\mathbf{B}$ and obtain the unimodular matrix $\mathbf{U} \in k[x]^{s\times s}$. Then $\mathbf{U}$ acts on $\mathbf{B}$, and the first column of $\mathbf{UB}$ are zeros except for the first element. Next, do the same operation for the first row of the $\mathbf{UB}$, we still get a unimodular matrix $\mathbf{V} \in k[x]^{t\times t}$ such that the first row in $\mathbf{UBV}$ are zeros except for the first element, but note that the first column of $\mathbf{UBV}$ are not necessarily zeros. So we repeatedly perform the above operation in order to get a matrix in which the first column and row are zeros except for the (1,1)-component. This is the first step. If all other elements in the new obtained matrix can be divisible by the (1,1)-element, then we only need to conduct the same step as the first step on the lower right submatrix of this matrix. Otherwise, we need an extra step to ensure the divisibility relation between (1,1)-element and other elements. Finally we will get the Smith normal form of $\mathbf{B}$. Most importantly, these can be naturally extended to the parametric case.

Here we will give the algorithm for the parametric case. Before discussing the algorithm, we would like to introduce some useful propositions which are related to the termination of the algorithm.

As known to all, currently the algorithms are all computing the minimal CGS. Here we show that the minimal CGS for modules over parametric univariate polynomial rings can always be reduced to the reduced CGS.

Proposition 23. *A minimal CGS $\mathcal{G} = \{(A_1, G_1), \dots, (A_l, G_l)\}$ for module $M \subset k[U][x]^s$ with respect to the POT order $\succ_s$ can be reduced to a reduced CGS.*

Proof. By Definition 6, we only need to prove that for each branch (A_v, G_v) of $\mathcal{G}$ where $v = 1, \dots, l$, the parametric minimal Gröbner basis G_v for M can be reduced to the parametric reduced Gröbner basis on A_v. For any $\mathbf{g_i}, \mathbf{g_j} \in G_v$, suppose that $\mathrm{LM}(\mathbf{g_i}) = g_1\mathbf{e}_i$ and $\mathrm{LM}(\mathbf{g_j}) = g\mathbf{e}_j$. Without loss of generality, one can assume $\mathbf{e}_i \succ \mathbf{e}_j$ and the j-th component of $\mathbf{g_i}$ is f, then the i-th component of $\mathbf{g_j}$ must be zero. If f is reduced with respect to g (i.e., no monomial of f is divisible by $\mathrm{LM}(g)$), there is nothing to do. Otherwise do pseudo division to f by g, then one get $hf = qg + r$ where h is the power of the leading coefficient of g with respect to the main variable x and $\sigma_\alpha(h) \neq 0$ for any $\alpha \in A_v$. Thus, $h\mathbf{g_i} - q\mathbf{g_j} = \bar{\mathbf{g}}_\mathbf{i}$ where $\bar{\mathbf{g}}_\mathbf{i}$ is reduced with respect to $\mathbf{g_j}$. We replace $\mathbf{g_i}$ with $\bar{\mathbf{g}}_\mathbf{i}$ and repeat the above process. Moreover, according to the definition of minimal CGS, $\sigma_\alpha(\mathrm{LC}_x(\mathbf{g})) \neq 0$ for any $\mathbf{g} \in G_v$ and $\alpha \in A_v$, then we can divide the coefficient such that $\sigma_\alpha(\mathrm{LC}_x(\mathbf{g})) = 1$. Thus, $\sigma_\alpha(G_v)$ is reduced. This proves the proposition. □

By the above proposition, we can get a new version of Algorithm 1 by computing a reduced CGS instead of a minimal CGS for M, denoted by Algorithm 1*.

Proposition 24. *Given $f_1, \dots, f_s \in k[U][x]$, a constructible set $S \subset L^m$ and a POT order $\succ_{s+1}$ with $\mathbf{e}'_0 \succ \mathbf{e}'_s \succ \cdots \succ \mathbf{e}'_1$. By Algorithm 1* we will get a reduced CGS $\{(A_i, G'_i)\}_{i=1}^l$ and an extended GCD system $\{(A_i, \mathbf{U}_i, d_i)\}_{i=1}^l$, where $G'_i = \{\mathbf{g}'_1, \dots, \mathbf{g}'_s\}$, $\mathbf{g}'_1 = (d_i, u_{11}, \dots, u_{1s})$, $\mathbf{g}'_j = (0, u_{j1}, \dots, u_{js})$ for $2 \le j \le s$. Then for any $\alpha \in A_i$, under the specialization σ_α, $\mathbf{u}_i = (u_{11}, \dots, u_{1s})$ is the minimal element in $M_i = \{(h_1, \dots, h_s) | h_1 f_1 + \cdots + h_s f_s = d_i\}$ with respect to $\succ_s$ being the restriction of $\succ_{s+1}$ on $k[x]^s$.*

Proof. Assume that under σ_α, $\mathbf{u}_i$ is not minimal, then there exists $\mathbf{u}'_i \in M_i$ and $\sigma_\alpha(\mathbf{u}_i) \succ_s \sigma_\alpha(\mathbf{u}'_i)$. By the definition of M_i, we have $\sigma_\alpha(\mathbf{u}_i - \mathbf{u}'_i) \in \mathrm{Syz}(\sigma_\alpha(f_1), \dots, \sigma_\alpha(f_s))$. Thus $\mathrm{LM}(\sigma_\alpha(\mathbf{u}_i)) = \mathrm{LM}(\sigma_\alpha(\mathbf{u}_i - \mathbf{u}'_i)) \in \mathrm{LM}(\mathrm{Syz}(\sigma_\alpha(f_1), \dots, \sigma_\alpha(f_s)))$. By Corollary 19, it implies that some term of $\sigma_\alpha(\mathbf{g}'_1)$ is divisible by one of $\mathrm{LM}(\sigma_\alpha(\mathbf{g}'_2)), \dots, \mathrm{LM}(\sigma_\alpha(\mathbf{g}'_s))$, which contradicts that $\sigma_\alpha(G'_i)$ is reduced. □

Now we give the algorithm for computing the Smith normal form of univariate polynomial matrices with parameters, and prove the termination of the algorithm.

In Algorithm 2, Reduce2Zero$(A_0, \mathbf{S}_0)$ stands for repeatedly calling Algorithm 1* on the first column and row of the matrix (matrices) for each algebraically constructible subset and the details is as

Algorithm 2: Parametric Smith normal form algorithm.

Input : $\mathbf{B} \in k[U][x]^{s\times t}$, a constructible set $A \subset L^m$, and a POT order $\succ_{s+1}$ with $\mathbf{e}'_0 \succ \mathbf{e}'_s \succ \cdots \succ \mathbf{e}'_1$.

Output: $\{[A_i, \mathbf{B}_i, \mathbf{U}_i, \mathbf{V}_i]\}_{i=1}^{l}$, where $\sigma_\alpha(\mathbf{U}_i)\sigma_\alpha(\mathbf{B})\sigma_\alpha(\mathbf{V}_i) = \sigma_\alpha(\mathbf{B}_i)$ and $\sigma_\alpha(\mathbf{B}_i)$ is in Smith normal form for any $\alpha \in A_i$.

```
begin
    $G := \{\}$;  $G_1 := \{[A, \mathbf{B}, \mathbf{E}_s, \mathbf{E}_t, \mathbf{B}]\}$;  $d := 0$;
    while $G_1$ is not empty do
        $[A_0, \mathbf{B}_0, \mathbf{U}_0, \mathbf{V}_0, \mathbf{S}_0]$:=$G_1[1]$;  $G_1 := G_1 \setminus \{G_1[1]\}$;
        $H_1 :=$ Reduce2Zero$(A_0, \mathbf{S}_0)$;
        for $[A_i, \mathbf{B}_i, \mathbf{U}_i, \mathbf{V}_i]$ in $H_1$ do
            $H_2 :=$ Divisible$(A_i, \mathbf{B}_i)$;
            for $[A_j, \mathbf{B}_j, \mathbf{U}_j, \mathbf{V}_j]$ in $H_2$ do
                $\mathbf{U}_1 :=$ diag$(\mathbf{E}_d, \mathbf{U}_j\mathbf{U}_i)$;
                $\mathbf{V}_1 :=$ diag$(\mathbf{E}_d, \mathbf{V}_i\mathbf{V}_j)$;
                $\mathbf{B}_1 := \mathbf{U}_1\mathbf{B}_0\mathbf{V}_1$; $\mathbf{U} := \mathbf{U}_1\mathbf{U}_0$; $\mathbf{V} := \mathbf{V}_0\mathbf{V}_1$;
                if $d = s - 1$ then
                    $G := G \cup \{[A_j, \mathbf{B}_1, \mathbf{U}, \mathbf{V}]\}$;
                else
                    $d := d + 1$;
                    $G_1 := G_1 \cup \{[A_j, \mathbf{B}_1, \mathbf{U}, \mathbf{V}, \text{SubMatrix}(\mathbf{B}_1, d)]\}$;
    return $G$;
```

Algorithm 3: Reduce2Zero.

Input : $\mathbf{B} \in k[U][x]^{s\times t}$, a constructible set $A \subset L^m$, and a POT order $\succ_{s+1}$ with $\mathbf{e}'_0 \succ \mathbf{e}'_s \succ \cdots \succ \mathbf{e}'_1$.

Output: $\{[A_i, \mathbf{B}_i, \mathbf{U}_i, \mathbf{V}_i]\}_{i=1}^{l}$, where $\sigma_\alpha(\mathbf{U}_i)\sigma_\alpha(\mathbf{B})\sigma_\alpha(\mathbf{V}_i) = \sigma_\alpha(\mathbf{B}_i)$ for any $\alpha \in A_i$ and the first column and row of $\mathbf{B}_i$ are zeros except for the (1,1)- element on A_i.

```
begin
    $G := \{\}$;  $G_1 := \{[A, \mathbf{B}, \mathbf{E}_s, \mathbf{E}_t]\}$;
    while $G_1$ is not empty do
        $[A_0, \mathbf{B}_0, \mathbf{U}_0, \mathbf{V}_0] := G_1[1]$;  $G_1 := G_1 \setminus \{G_1[1]\}$;
        $H_1 :=$ CEGCD$(A_0, \mathbf{B}_0)$;
        for $[A_i, \mathbf{U}_i, d_i]$ in $H_1$ do
            $\mathbf{B}_i := \mathbf{U}_i\mathbf{B}_0$;  $\mathbf{U}_i := \mathbf{U}_i\mathbf{U}_0$;
            $H_2 :=$ REGCD$(A_i, \mathbf{B}_i)$;
            for $[A_{i_j}, \mathbf{V}_{i_j}, d_{i_j}]$ in $H_2$ do
                $\mathbf{B}_{i_j} := \mathbf{B}_i\mathbf{V}_{i_j}^T$;  $\mathbf{V}_{i_j} := \mathbf{V}_0\mathbf{V}_{i_j}^T$;
                if IsZero$(A_{i_j}, \mathbf{B}_{i_j})$ then
                    $G := G \cup \{[A_{i_j}, \mathbf{B}_{i_j}, \mathbf{U}_i, \mathbf{V}_{i_j}]\}$;
                else
                    $G_1 := G_1 \cup \{[A_{i_j}, \mathbf{B}_{i_j}, \mathbf{U}_i, \mathbf{V}_{i_j}]\}$;
    return $G$;
```

follows. Divisible$(A_i, \mathbf{B}_i)$ is used to check whether all other elements in $\mathbf{B}_i$ can be divisible by (1,1)-element on A_i, if not, we need the extra step: adding the corresponding column in which the element which isn't divisible by (1,1)-element of $\mathbf{B}_i$ is to the first column of $\mathbf{B}_i$ and getting $\mathbf{B}'_i$, then performing Reduce2Zero$(A_i, \mathbf{B}'_i)$. SubMatrix$(\mathbf{B}_1, \mathrm{d})$ denotes the lower right submatrix of $\mathbf{B}_1$ which consists of the last $s - d$ rows and $t - d$ columns.

In Algorithm 3, CEGCD(A, $\mathbf{B}$) and REGCD$(A, \mathbf{B})$ stand for calling Algorithm 1* on the first column and row of matrix $\mathbf{B}$ on the constructible set A, respectively. IsZero$(A_{i_j}, \mathbf{B}_{i_j})$ is a subroutine to determine if the first column and row of $\mathbf{B}_{i_j}$ are zeros except for the (1,1)-element on algebraically constructible subset A_{i_j}.

Proposition 25. *Algorithm 2 terminates in finitely many steps.*

Table 3
Output of Reduce2Zero($A, \mathbf{B}$).

No.	A_i	$\mathbf{B}_i$	$\mathbf{U}_i$	$\mathbf{V}_i$
1	$\mathbb{C}\backslash\mathbb{V}(a)$	$\mathbf{B}_1$	$\mathbf{U}_1$	$\mathbf{V}_1$
2	$\mathbb{V}(a)\backslash\mathbb{V}(b)$	$\mathbf{B}_2$	$\mathbf{U}_2$	$\mathbf{V}_2$
3	$\mathbb{V}(a,b)$	$\mathbf{B}_3$	$\mathbf{U}_3$	$\mathbf{V}_3$

Proof. According to the design of the algorithm and above explain, we only need to prove that Algorithm 3 (Reduce2Zero($A, \mathbf{B}$)) terminates within finite steps. Since the original (1,1)-element of univariate polynomial matrix $\mathbf{B}$ has a definite degree and since the process of reducing the degree for the (1,1)-element cannot be continued indefinitely, after a finite number of loops the degree of (1,1)-element with respect to main variable x is stable and assume at the moment we get $\mathbf{B}_i$ of which the first column are zeros except for the (1,1)-element on A_i. Then $H_2 :=$ REGCD($\mathrm{A_i}, \mathbf{B_i}$), and we get a unimodular matrix $\mathbf{V}_{i_j}^T$ which can reduce the first row of $\mathbf{B}_i$ to be zeros on new algebraically constructible subset A_{i_j}. Since under the specialization, the degree of b_{11} (i.e., (1,1)-element of $\mathbf{B}_i$) is stable, b_{11} is the GCD of the first row elements of $\mathbf{B}_i$. We claim that $\mathbf{V}_{i_j}^T$ has the following form:

$$\mathbf{V}_{i_j}^T = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1t} \\ 0 & v_{11} & \dots & v_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & v_{t2} & \dots & v_{tt} \end{bmatrix}.$$

Otherwise, assume that for some $\alpha \in A_{i_j}$, there exists at least one $\sigma_\alpha(v_{l1}) \neq 0$, $2 \leq l \leq t$. Obviously, $\sigma_\alpha(\mathbf{v_1}) = (\sigma_\alpha(v_{11}), \dots, \sigma_\alpha(v_{t1}))^T \succ_t (\sigma_\alpha(v_{11}), 0, \dots, 0)$ under the POT order $\succ_t$ being the restriction of $\succ_{t+1}$ with $\mathbf{e}_0' \succ \mathbf{e}_t' \succ \cdots \succ \mathbf{e}_1'$ on $k[x]^t$, which contradicts that $\sigma_\alpha(\mathbf{v_1})$ should be minimal by Proposition 24.

Thus, $\mathbf{B}_{i_j} = \mathbf{B}_i \mathbf{V}_{i_j}^T$ satisfies that the first column and row are zeros except for the (1,1)-element on A_{i_j}. Consequently, Algorithm 3 terminates. □

We use a simple example to illustrate Algorithm 2.

Example 26. Given a matrix $B \in \mathbb{C}[a,b][x]^{3\times 2}$ and a constructible set $S = \mathbb{C}$ as follows:

$$\mathbf{B} = \begin{bmatrix} ax & x+1 \\ x^2 & bx \\ 0 & 1 \end{bmatrix}.$$

Step 1: perform the routine Reduce2Zero($A, \mathbf{B}$), that is, repeatedly call Algorithm 1* on the first column and row of the matrix, then we get the matrices in which the first column and row are zeros except for the (1,1)-component. Where $\mathbf{U}_i \mathbf{B} \mathbf{V}_i = \mathbf{B}_i$ for $i = 1, 2, 3$ (Table 3),

$$\mathbf{B}_1 = \begin{bmatrix} 1 & 0 \\ 0 & ax \\ 0 & ax^2(ab-x-1) \end{bmatrix}, \quad \mathbf{B}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & bx^2 \end{bmatrix}, \quad \mathbf{B}_3 = \begin{bmatrix} x^2 & 0 \\ 0 & x+1 \\ 0 & 1 \end{bmatrix},$$

$$\mathbf{U}_1 = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 1 \\ x^2-abx & a & 0 \end{bmatrix}, \quad \mathbf{U}_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -x-1 \\ 0 & -1 & bx \end{bmatrix}, \quad \mathbf{U}_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$\mathbf{V}_1 = \begin{bmatrix} -1/a & -x-1 \\ 1 & ax \end{bmatrix}, \quad \mathbf{V}_2 = \begin{bmatrix} 0 & -b \\ 1 & 0 \end{bmatrix}, \quad \mathbf{V}_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Step 2: perform the subroutine Divisible($A_i, \mathbf{B}_i$) to check if all elements in $\mathbf{B}_i$ are divisible by the (1,1)-element.

Table 4
Output of Divisible$(A_i, \mathbf{B}_i)$.

No.	A'_i	$\mathbf{B}'_i$	$\mathbf{U}'_i$	$\mathbf{V}'_i$
1	$\mathbb{C}\backslash\mathbb{V}(a)$	$\mathbf{B}'_1$	$\mathbf{U}'_1$	$\mathbf{V}'_1$
2	$\mathbb{V}(a)\backslash\mathbb{V}(b)$	$\mathbf{B}'_2$	$\mathbf{U}'_2$	$\mathbf{V}'_2$
3	$\mathbb{V}(a,b)$	$\mathbf{B}'_3$	$\mathbf{U}'_3$	$\mathbf{V}'_3$

Table 5
Output of SubMatrix$(\mathbf{B}'_i, 1)$.

No.	A''_i	$\mathbf{B}''_i$	$\mathbf{U}''_i$	$\mathbf{V}''_i$
1	$\mathbb{C}\backslash\mathbb{V}(a)$	$\mathbf{B}''_1$	$\mathbf{U}''_1$	$\mathbf{V}''_1$
2	$\mathbb{V}(a)\backslash\mathbb{V}(b)$	$\mathbf{B}''_2$	$\mathbf{U}''_2$	$\mathbf{V}''_2$
3	$\mathbb{V}(a,b)$	$\mathbf{B}''_3$	$\mathbf{U}''_3$	$\mathbf{V}''_3$

Table 6
Recover Smith normal forms.

No.	A'''_i	$\mathbf{B}'''_i$	$\mathbf{U}'''_i$	$\mathbf{V}'''_i$
1	$\mathbb{C}\backslash\mathbb{V}(a)$	$\mathbf{B}'''_1$	$\mathbf{U}'''_1$	$\mathbf{V}'''_1$
2	$\mathbb{V}(a)\backslash\mathbb{V}(b)$	$\mathbf{B}'''_2$	$\mathbf{U}'''_2$	$\mathbf{V}'''_2$
3	$\mathbb{V}(a,b)$	$\mathbf{B}'''_3$	$\mathbf{U}'''_3$	$\mathbf{V}'''_3$

Obviously, $\mathbf{B}_1$ and $\mathbf{B}_2$ satisfy the divisibility relation between the (1,1)-element and other elements, but $\mathbf{B}_3$ doesn't satisfy the divisibility relation. Where $\mathbf{A}'_i = \mathbf{A}_i,\ \mathbf{B}'_i = \mathbf{B}_i,\ \mathbf{U}'_i = \mathbf{U}_i,\ \mathbf{V}'_i = \mathbf{V}_i$ for $i = 1, 2$ (Table 4),

$$\mathbf{B}'_3 = \begin{bmatrix} 1 & 0 \\ 0 & -x^2 \\ 0 & -x^2 \end{bmatrix}, \quad \mathbf{U}'_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ -1 & -1 & x+1 \end{bmatrix}, \quad \mathbf{V}'_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Step 3: repeat the Step 1 and Step 2 on the lower right submatrices of $\mathbf{B}'_1$, $\mathbf{B}'_2$ and $\mathbf{B}'_3$. We obtain the following result (Table 5). Where

$$\mathbf{B}''_1 = \begin{bmatrix} x \\ 0 \end{bmatrix}, \quad \mathbf{B}''_2 = \begin{bmatrix} x^2 \\ 0 \end{bmatrix}, \quad \mathbf{B}''_3 = \begin{bmatrix} x^2 \\ 0 \end{bmatrix},$$

$$\mathbf{U}''_1 = \begin{bmatrix} 1 & 0 \\ x^2 + x - abx & 1 \end{bmatrix}, \quad \mathbf{U}''_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{U}''_3 = \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix},$$

$$\mathbf{V}''_1 = \begin{bmatrix} -1/a \end{bmatrix}, \quad \mathbf{V}''_2 = \begin{bmatrix} 1/b \end{bmatrix}, \quad \mathbf{V}''_3 = \begin{bmatrix} 1 \end{bmatrix}.$$

Step 4: recover the Smith normal forms (Table 6). Where

$$\mathbf{B}'''_1 = \begin{bmatrix} 1 & 0 \\ 0 & x \\ 0 & 0 \end{bmatrix}, \quad \mathbf{B}'''_2 = \begin{bmatrix} 1 & 0 \\ 0 & x^2 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{B}'''_3 = \begin{bmatrix} 1 & 0 \\ 0 & x^2 \\ 0 & 0 \end{bmatrix},$$

$$\mathbf{U}'''_1 = \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{U}''_1 \end{bmatrix} \mathbf{U}_1, \quad \mathbf{U}'''_2 = \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{U}''_2 \end{bmatrix} \mathbf{U}_2, \quad \mathbf{U}'''_3 = \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{U}''_3 \end{bmatrix} \mathbf{U}'_3,$$

$$\mathbf{V}'''_1 = \mathbf{V}_1 \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{V}''_1 \end{bmatrix}, \quad \mathbf{V}'''_2 = \mathbf{V}_2 \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{V}''_2 \end{bmatrix}, \quad \mathbf{V}'''_3 = \mathbf{V}'_3 \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{V}''_3 \end{bmatrix}.$$

6. Concluding remarks

An algorithm for computing extended GCRD systems of parametric univariate polynomial matrices has been proposed. We can see that this algorithm simultaneously gives the GCRD and the representation coefficient matrices (or multipliers) by computing the CGS of a constructed module, which adds the unit vectors to record the representation coefficients (as mentioned in Beckermann et al. (1999)). As for polynomial cases, it can be regarded as a special case of matrices, so we also have the extended GCD algorithm for parametric univariate polynomials. Meanwhile, this CGS for M'_e also gives a set of free bases for the parametric syzygy module of input polynomial matrices. It is worth noting that we get a stronger result: the unimodular matrix $\mathbf{U}$. Therefore, we can apply the proposed extended GCD algorithm for univariate polynomials to the computation of the Smith normal form and present the first algorithm for computing the Smith normal form of univariate polynomial matrices with parameters. In addition, the proposed algorithms have been implemented on the computer algebra system *Maple*, and the codes and examples are available on the web: http://www.mmrc.iss.ac.cn/~dwang/software.html.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was supported partially by the National Natural Science Foundation of China under Grant No. 12171469, the CAS Key Project QYZDJ-SSW-SYS022 and National Key Research and Development Project 2020YFA0712300.

References

Abramov, S., Kvashenko, K., 1993. On the greatest common divisor of polynomials which depend on a parameter. In: Proceedings of the 1993 ACM International Symposium on Symbolic and Algebraic Computation, pp. 152–156.

Ayad, A., 2010. Complexity of algorithms for computing greatest common divisors of parametric univariate polynomials. Int. J. Algebra 4 (4), 173–188.

Bächler, T., Gerdt, V., Lange-Hegermann, M., Robertz, D., 2012. Algorithmic Thomas decomposition of algebraic and differential systems. J. Symb. Comput. 47 (10), 1233–1266.

Barnett, S., 1971. Matrices in Control Theory: with Applications to Linear Programming. Van Nostrand Reinhold.

Beckermann, B., Labahn, G., 2000. Fraction-free computation of matrix rational interpolants and matrix GCDs. SIAM J. Matrix Anal. Appl. 22 (1), 114–144.

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

Bradley, G., 1971. Algorithms for Hermite and Smith normal matrices and linear Diophantine equations. Math. Comput. 25 (116), 897–907.

Brent, R.P., Kung, H.T., 1984. Systolic VLSI arrays for polynomial GCD computation. IEEE Trans. Comput. 100 (8), 731–736.

Brown, W., 1971. On Euclid's algorithm and the computation of polynomial greatest common divisors. J. ACM 18 (4), 478–504.

Chen, C., Maza, M., 2012. Algorithms for computing triangular decomposition of polynomial systems. J. Symb. Comput. 47 (6), 610–642.

Chou, S., 1988. Mechanical Geometry Theorem Proving, Vol. 41. Springer Science and Business Media.

Corless, R., Maza, M., Thornton, S., 2017. Jordan canonical form with parameters from Frobenius form with parameters. In: International Conference on Mathematical Aspects of Computer and Information Sciences, pp. 179–194.

Emre, E., Silverman, L., 1976. New criteria and system theoretic interpretations for relatively prime polynomial matrices. IEEE Trans. Autom. Control 22 (2), 239–242.

Gantmacher, F.R., 1959. The Theory of Matrices, Vol. 1. American Mathematical Society.

Geddes, K.O., Czapor, S.R., Labahn, G., 1992. Algorithms for Computer Algebra. Springer Science & Business Media.

Gianni, P., Trager, B., 1985. GCDs and factoring multivariate polynomials using Gröbner bases. In: European Conference on Computer Algebra. Springer, pp. 409–410.

Hippe, P., Deutscher, J., 2009. Polynomial Matrix Fraction Descriptions. Springer, London.

Insua, M., 2005. Varias perspectives sobre las bases de Gröbner: Forma normal de Smith, Algoritme de Berlekamp y álgebras de Leibniz. Ph.D. thesis. Universidade de Santiago de Compostela, Spain.

Kai, H., Noda, M.-T., 2000. Hybrid rational approximation and its applications. Reliab. Comput. 6, 429–438.

Kailath, T., 1980. Linear Systems, Vol. 156. Prentice-Hall, Englewood Cliffs, NJ.

Kalkbrener, M., 1997. On the stability of Gröbner bases under specializations. J. Symb. Comput. 24 (1), 51–58.

Kapur, D., Lu, D., Monagan, M., Sun, Y., Wang, D., 2018. An efficient algorithm for computing parametric multivariate polynomial GCD. In: Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation, pp. 239–246.

Kapur, D., Sun, Y., Wang, D., 2010. A new algorithm for computing comprehensive Gröbner systems. In: Proceedings of the 2010 ACM International Symposium on Symbolic and Algebraic Computation, pp. 29–36.

Kapur, D., Sun, Y., Wang, D., 2013. An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. J. Symb. Comput. 49, 27–44.

Kung, S., Kailath, T., Morf, M., 1976. A generalized resultant matrix for polynomial matrices. In: IEEE Conference on Decision and Control Including the 15th Symposium on Adaptive Processes, pp. 892–895.

Montes, A., 2002. A new algorithm for discussing Gröbner bases with parameters. J. Symb. Comput. 33 (2), 183–208.

Moses, J., Yun, D., 1973. The EZ GCD algorithm. In: Proceedings of the ACM Annual Conference. ACM, pp. 159–166.

Nabeshima, K., 2007a. PGB: a package for computing parametric Gröbner and related objects. ACM Commun. Comput. Algebra 41 (3), 104–105.

Nabeshima, K., 2007b. A speed-up of the algorithm for computing comprehensive Gröbner systems. In: Proceedings of the 2007 ACM International Symposium on Symbolic and Algebraic Computation, pp. 299–306.

Nabeshima, K., 2010. On the computation of parametric Gröbner bases for modules and syzygies. Jpn. J. Ind. Appl. Math. 27 (2), 217–238.

Nagasaka, K., 2017. Parametric greatest common divisors using comprehensive Gröbner systems. In: Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation, pp. 341–348.

Norman, C., 2012. Finitely Generated Abelian Groups and Similarity of Matrices over a Field. Springer Science & Business Media.

Pace, I., Barnett, S., 1974. Efficient algorithms for linear system calculations. I: Smith form and common divisor of polynomial matrices. Int. J. Syst. Sci., 403–411.

Rosenbrock, H., 1970. State-Space and Multivariable Theory. Nelson.

Sasaki, T., Suzuki, M., 1992. Three new algorithms for multivariate polynomial GCD. J. Symb. Comput. 13 (4), 395–411.

Suzuki, A., Sato, Y., 2002. An alternative approach to comprehensive Gröbner bases. J. Symb. Comput. 36 (3), 649–667.

Suzuki, A., Sato, Y., 2006. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In: Proceedings of the 2006 ACM International Symposium on Symbolic and Algebraic Computation, pp. 326–331.

Wang, D., Wang, H., Xiao, F., 2020. An extended GCD algorithm for parametric univariate polynomials and application to parametric Smith normal form. In: Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, pp. 442–449.

Weispfenning, V., 1992. Comprehensive Gröbner bases. J. Symb. Comput. 14 (1), 1–29.

Wolovich, W.A., 1974. Equivalence and invariants in linear multivariable systems. In: Joint Automatic Control Conference, vol. 12, pp. 177–185.

Zippel, R., 1979. Probabilistic algorithms for sparse polynomials. In: Proceedings of the EUROSAM'79. Springer-Verlag, pp. 216–226.

Zippel, R., 1993. Effective Polynomial Computation, Vol. 241. Springer Science and Business Media.