An Algorithm for Computing Greatest Common Right Divisors of Parametric Ore Polynomials

Xiuquan Ding[a,b], Dingkang Wang[a,b], Fanghui Xiao[c] and Xiaopeng Zheng[a,b]
[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, Changsha 410081, China
dingxiuquan@amss.ac.cn,dwang@mmrc.iss.ac.cn,xiaofanghui@hunnu.edu.cn,zhengxiaopeng@amss.ac.cn

ABSTRACT

A new algorithm for computing the parametric greatest common right divisor (GCRD) of a set of parametric Ore polynomials is presented in this paper. The algorithm is based on Gröbner bases for modules. Inspired by the resultant theory in Ore polynomial rings, the Sylvester matrix is defined for a set of Ore polynomials. In the case of non-parametric polynomials, the GCRD of Ore polynomials can be obtained by computing the row echelon form of the Sylvester matrix. For the parametric case, the parametric Sylvester matrix is also defined in the paper. Based on this, under the assumption that the specializations commute with the conjugate operator and derivation in the Ore polynomial ring, the parametric GCRD of parametric Ore polynomials can be obtained by computing the Gröbner basis for the module generated by rows of the parametric Sylvester matrix. As a consequence, the algorithm for computing the parametric GCRD is presented in detail and has been implemented in the computer algebra system Singular.

CCS CONCEPTS

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

KEYWORDS

Parametric Ore polynomial, Sylvester matrix, Gröbner bases for modules.

ACM Reference Format:
Xiuquan Ding[a,b], Dingkang Wang[a,b], Fanghui Xiao[c] and Xiaopeng Zheng[a,b]. 2024. An Algorithm for Computing Greatest Common Right Divisors of Parametric Ore Polynomials. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '24), July 16–19, 2024, Raleigh, NC, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3666000.3669694

1 INTRODUCTION

Ore polynomials, introduced by Ore in [23], establish a general mathematical setting to describe linear operational polynomials, including linear differential, difference, and q-difference polynomials [7, 24]. Algorithms related to Ore polynomial rings have been implemented in many computer algebra systems such as Maple [2], Sage [16] and Singular. Recently, Ore polynomials over a finite field have been found to have a lot of applications in coding theory [5, 6], cryptography [4, 30], and so on. Furthermore, the development of basic Ore polynomial algorithms is an active research area in computer algebra[8–11, 25].

The greatest common right divisor (GCRD) of Ore polynomials is a basic object in the theory of Ore polynomial rings. A modular algorithm for computing the GCRD of Ore polynomials was proposed by Li and Nemes [18]. In some cases, the coefficients of Ore polynomials may depend on certain parameters. To deal with this, Glotov presented an algorithm in 1998 that can compute the GCRD of two parametric Ore polynomials [12]. This algorithm is based on the subresultant theory proposed by Li in [17].

In a usual (commutative) polynomial ring, the GCD for polynomials whose coefficients depend on some parameters is called parametric GCD. This topic has been thoroughly researched and several works have been published on it, including [1, 3, 13, 14, 22, 27]. Among them, the algorithms in [14, 22, 27] are based on comprehensive Gröbner systems and many effective algorithms for computing comprehensive Gröbner systems in the commutative polynomial ring can be found in [15, 20, 21, 26, 28]. However, in Ore polynomial rings, the coefficients, parameters, and the variable may not be commutative. Therefore, when utilizing the method mentioned in [14, 22, 27], it becomes necessary to take into account non-commutative Gröbner bases. Yet in fact the computation of non-commutative Gröbner bases is less efficient compared with the commutative Gröbner bases because there are many improved methods to accelerate in the commutative case. Hence, we attempt to use the commutative Gröbner bases to compute the parametric GCRD of Ore polynomials instead of non-commutative Gröbner bases.

In this paper, we introduce a new algorithm called the parametric GCRD algorithm. Under the assumption that any considered specialization commutes with the conjugate operator and derivation in the Ore polynomial ring, this algorithm directly calculates the Gröbner basis of a specific module and obtains the parametric GCRD of a set of Ore polynomials.

This paper is organized as follows. In Section 2, we provide background about the Ore polynomial rings, GCRD, and parametric GCRD for Ore polynomials. In Section 3, we present the definition of Sylvester matrix for several Ore polynomials and utilize it to compute the GCRD of several non-parametric Ore polynomials. In Section 4, we define the Sylvester matrix for the parametric case and present the main theorem in the paper, which states that the parametric GCRD can be obtained by computing the Gröbner basis

ISSAC '24, July 16–19, 2024, Raleigh, NC, USA

ACM ISBN 979-8-4007-0696-7/24/07
https://doi.org/10.1145/3666000.3669694

of the module generated by the rows of the parametric Sylvester matrix. In Section 5, the algorithm is presented specifically, and an illustrative example and the implementation of the algorithm on some polynomials is given. Finally, we conclude this paper.

2 PRELIMINARIES

This section consists of two parts: Section 2.1 provides an overview of Ore polynomial rings and introduces the associated notation, while Section 2.2 introduces the definitions of specialization and parametric GCRD. For more details about Ore polynomial rings can refer to [7, 23, 24].

2.1 (Univariate) Ore polynomials

Let R be a commutative domain and let σ be an injective endomorphism of R, which is called a *conjugate operator* by Ore. A *derivation* with respect to σ is any mapping $\delta\colon R \to R$ satisfying the following conditions for any $a, b \in R$:

$$\delta(a+b) = \delta(a) + \delta(b), \qquad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b. \tag{1}$$

Definition 2.1 ([23]). An Ore polynomial ring $R[x;\sigma,\delta]$ over R given by σ and δ is the polynomial ring in x over R with the usual addition of polynomials and multiplication given by the rule

$$xa = \sigma(a)x + \delta(a) \quad \text{for any } a \in R.$$

The elements in the ring $R[x;\sigma,\delta]$ are called *Ore polynomials* or *skew polynomials*.

Example 2.2. Several examples about Ore polynomial rings are provided below:

(1) **(Polynomial ring over a field)** Let $R = k$ be a field and let $\sigma = \mathrm{id}$ and $\delta = 0$.
(2) **(Field with positive characteristic)** Let $R = \mathbb{F}_q$ be a finite field with characteristic p. The endomorphism σ is defined as the map $a \mapsto a^{p^r}$, and $\delta = 0$.
(3) **(Differential operators)** Let $R = \mathbb{C}(t)$ and let $\sigma = \mathrm{id}$ and $\delta = \frac{d}{dt}$ be the standard derivation.

For further examples, please refer to [2].

In Definition 2.1, we define an Ore polynomial ring over a commutative domain. In particular, when $R = k$ is a field, the right Euclidean algorithm can be applied to two polynomials in $k[x;\sigma,\delta]$. Consider $a, b \in k[x;\sigma,\delta]\backslash\{0\}$. By applying the right division algorithm, we can express a as

$$a = qb + r, \quad q, r \in k[x;\sigma,\delta], \quad \deg r < \deg b;$$

where r and q are the *right remainder* and the *right quotient* of a divided by b, respectively.

For $a, d \in k[x;\sigma,\delta]$, we say that d is a right factor of a if there exists $b \in k[x;\sigma,\delta]$ such that $a = bd$. A common right factor of $f_1, \ldots, f_\ell$, with the highest degree, is called a *Greatest Common Right Divisor (GCRD)* of $f_1, \ldots, f_\ell$, denoted by $\mathrm{gcrd}(f_1, \ldots, f_\ell)$.

2.2 Parametric GCRD for Ore polynomials

Let $\mathcal{R} = k[x;\sigma,\delta]$ be an Ore polynomial ring, where k is a field. Consider two polynomials $f_1(u_1, \ldots, u_s, x)$ and $f_2(u_1, \ldots, u_s, x)$ with parameters $u_1, \ldots, u_s$ and the variable x. For any point $(a_1, \ldots, a_s) \in k^s$, we can define two polynomials in $k[x]$ by evaluation as follows:

$$f_{\vec{a}}(x) = f(a_1, \ldots, a_s, x), \qquad g_{\vec{a}}(x) = g(a_1, \ldots, a_s, x).$$

It is clear that for a given point $(a_1, \ldots, a_s) \in k^s$, determining the greatest common right divisor of $f_{\vec{a}}(x)$ and $g_{\vec{a}}(x)$ is straightforward. Now the problem is how to precompute an expression $d(u_1, \ldots, u_s, x)$ without precise knowledge of $(a_1, \ldots, a_s)$ and then conveniently compute the greatest common right divisor of $f_{\vec{a}}(x)$ and $g_{\vec{a}}(x)$ by evaluating $d(u_1, \ldots, u_s, x)$ with u_i replaced by a_i when the exact values of $(a_1, \ldots, a_s)$ are known.

To more rigorously describe the problem under consideration, we need to first introduce some definitions.

Definition 2.3 (Specialization). Let $R = k[u_1, \ldots, u_s]$. A specialization of R is a homomorphism $\phi_{\vec{a}}\colon R \to k$ induced by the element $\vec{a} = (a_1, \ldots, a_s) \in k^s$. That is, for any $h \in R$, $\phi_{\vec{a}}(h)$ is defined by

$$\phi_{\vec{a}}\colon h(u_1, \ldots, u_s) \mapsto h(a_1, \ldots, a_s).$$

Every specialization $\phi_{\vec{a}}\colon R \to k$ is extended canonically to a specialization $\phi_{\vec{a}}\colon R[x] \to k[x]$ by applying $\phi_{\vec{a}}$ coefficient-wise, i.e.,

$$\phi_{\vec{a}}\colon \sum_{i=0}^{l} h_i(u_1, \ldots, u_s)x^i \mapsto \sum_{i=0}^{l} h_i(a_1, \ldots, a_s)x^i.$$

For a matrix $M = (f_{ij}) \in R[x]^{\ell\times n}$, we define $\phi_{\vec{a}}(M)$ by $(\phi_{\vec{a}}(f_{ij}))$.

We denote $k[u_1, \ldots, u_s]$ by $k[U]$. For an ideal $I \subset k[U]$, denote by $\mathbb{V}_L(I)$ the set $\{(a_1, \ldots, a_s) \in L^s\colon h(a_1, \ldots, a_s) = 0, h \in I\}$, where L is a subset of k. Then we define the parametric greatest common right divisors as follows:

Definition 2.4 (Parametric GCRD). Let $\mathcal{R} = k[x;\sigma,\delta]$ be an Ore polynomial ring, and let L be a subset of k. The *parametric greatest common right divisors* (PGCRD) of $F = \{f_1, \ldots, f_\ell\} \subset k[U, x]$ with respect to L is a set $\{(E_1, N_1, d_1), \ldots, (E_t, N_t, d_t)\}$, satisfying

(a) $E_i, N_i \subset k[U]$, and $d_i \in k[U, x]$, with $i = 1, \ldots, t$.
(b) $\bigcup_{i=1}^{t} \mathbb{V}_L(E_i) \setminus \mathbb{V}_L(N_i) = L^s$.
(c) $\phi_{\vec{a}}(d_i)$ is a GCRD of $\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell) \in \mathcal{R}$ for $\vec{a} \in \mathbb{V}_L(E_i) \setminus \mathbb{V}_L(N_i)$ (up to a non-zero constant in L). Moreover, for each $d_i \neq 0$, $\phi_{\vec{a}}(\mathrm{lc}_x(d_i)) \neq 0$ for $\vec{a} \in \mathbb{V}_L(E_i) \setminus \mathbb{V}_L(N_i)$.

where $\mathrm{lc}_x(d_i)$ is the leading coefficient of d_i with respect to x.

To compute the parametric GCRD, we need to construct a new Ore polynomial ring, which is called *parametric Ore polynomial ring*.

Definition 2.5. Let $\mathcal{R} = k[x;\sigma,\delta]$ be an Ore polynomial ring, and let L be a subset of k. An Ore polynomial ring $\mathcal{R}' = k[U][x;\sigma',\delta']$ is called the parametric Ore polynomial ring associated with $\mathcal{R}$ and L if for any $\vec{a} \in L^s$, the specialization

$$\phi_{\vec{a}}\colon k[U] \to k, \qquad h(u_1, \ldots, u_s) \mapsto h(a_1, \ldots, a_s)$$

satisfies $\sigma(\phi_{\vec{a}}(h)) = \phi_{\vec{a}}(\sigma'(h))$ and $\delta(\phi_{\vec{a}}(h)) = \phi_{\vec{a}}(\delta'(h))$.

In this paper, we will prove that for any Ore polynomial ring $\mathcal{R}$ and any subset L of k, if the parametric Ore polynomial ring associated with $\mathcal{R}$ and L exists, then we can construct the parametric GCRD by computing the Gröbner basis of a specific module.

Remark 2.6. *In [12], Glotov only considered the case of one parameter, that is $U = \{u_1\}$. Moreover, k and L were chosen to be $K(t)$ and K, respectively, where K is a field. In this paper, we consider a more general case.*

In the following we present two examples of parametric GCRD:

Example 2.7. Let $\mathbb{F}_2$ be a finite field with cardinality 2 and $\overline{\mathbb{F}_2}$ the algebraic closure of $\mathbb{F}_2$. Consider the Ore polynomial ring

$$\mathcal{R} = \overline{\mathbb{F}_2}[x; \sigma, 0], \text{ where } \sigma\colon \overline{\mathbb{F}_2} \to \overline{\mathbb{F}_2}, \qquad a \mapsto a^2.$$

Let $f_1 = x^2 + u_1x + 1$, $f_2 = u_2x^2 + x$, $f_3 = x^2 + u_3x + 1 \in \overline{\mathbb{F}_2}[U, x]$. Then the parametric GCRD of f_1, f_2, f_3 with respect to $\overline{\mathbb{F}_2}$ is

$$\{(\{u_1 + u_3, u_2^2u_3^2 + u_2^3 + 1\}, \{1\}, x + u_2u_3^3 + u_2^2u_3 + u_3^2 + u_2),$$
$$(\{0\}, \{u_1 + u_3, u_2^2u_3^2 + u_2^3 + 1\}, 1)\}.$$

That is, assume $\vec{a} = (a_1, a_2, a_3) \in \overline{\mathbb{F}_2}^3$ and $\phi_{\vec{a}}\colon \overline{\mathbb{F}_2}[U] \to \overline{\mathbb{F}_2}$ is a specialization induced by $\vec{a}$, then

(1) If $a_1 + a_3 = 0$ and $a_2^2a_3^2 + a_2^3 + 1 = 0$, then

$$\operatorname{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = x + a_2a_3^3 + a_2^2a_3 + a_3^2 + a_2.$$

(2) If $a_1 + a_3 \neq 0$ or $a_2^2a_3^2 + a_2^3 + 1 \neq 0$, then

$$\operatorname{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = 1.$$

Remark 2.8. *In Example 2.7, we has computed the parametric GCRD of f_1, f_2, f_3 with $k = L = \overline{\mathbb{F}_2}$. To extend the analysis to the case where $k = L = \mathbb{F}_q$ with $q = 2^s$ for some integer s, it suffices to include the additional equations $a_i^q = 1$ for $i = 1, 2, 3$ among the equality constraints in the final outcome.*

Example 2.9. Let $\mathcal{R} = \mathbb{C}(t)[x; \mathrm{id}, \frac{d}{dt}]$, and let $f_1 = u_1x^2 + tx + 1$, $f_2 = x^2 + u_2tx + (u_1t^2 + 1)$, $f_3 = x^2 + (t + u_1)x + (t + u_1) \in \mathbb{C}(t)[U, x]$. Then the parametric GCRD of f_1, f_2, f_3 associated with $\mathbb{C}$ is

$$\{(\{u_1 - 1, u_2 - 2\}, \{1\}, x + t), (\{0\}, \{u_1 - 1, u_2 - 2\}, 1)\}.$$

That is, assume $\vec{a} = (a_1, a_2) \in \mathbb{C}^2$ and $\phi_{\vec{a}}\colon \mathbb{C}(t)[U] \to \mathbb{C}(t)$ is a specialization induced by $\vec{a}$, then

(1) If $a_1 - 1 = 0$ and $a_2 - 2 = 0$, then

$$\operatorname{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = x + t.$$

(2) If $a_1 - 1 \neq 0$ or $a_2 - 2 \neq 0$, then

$$\operatorname{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = 1.$$

Remark 2.10. *In Example 2.7, the parametric Ore polynomial ring associated with $\mathcal{R}$ and $\overline{\mathbb{F}_2}$ is $\mathcal{R}' = \overline{\mathbb{F}_2}[U][x; \sigma', 0]$, where*

$$\sigma'\colon \overline{\mathbb{F}_2}[U] \to \overline{\mathbb{F}_2}[U], \qquad h(u_1, u_2, u_3) \mapsto h(u_1, u_2, u_3)^2.$$

It is easy to check that for any $(a_1, a_2, a_3) \in \overline{\mathbb{F}_2}$, we have

$$\sigma(\phi_{\vec{a}}(h)) = \sigma(h(a_1, a_2, a_3)) = h(a_1, a_2, a_3)^2$$

and

$$\phi_{\vec{a}}(\sigma'(h)) = \phi_{\vec{a}}(h(u_1, u_2, u_3)^2) = h(a_1, a_2, a_3)^2.$$

Hence, $\sigma(\phi_{\vec{a}}(h)) = \phi_{\vec{a}}(\sigma'(h))$. It is clear that $\delta(\phi_{\vec{a}}(h)) = \phi_{\vec{a}}(\delta'(h))$. Therefore, $\mathcal{R}'$ is the parametric Ore polynomial ring associated with $\mathcal{R}$ and $\overline{\mathbb{F}_2}$. In Example 2.9, it is easy to check $\mathcal{R}' = \mathbb{C}(t)[U][x; \mathrm{id}, \frac{\partial}{\partial t}]$ is the parametric Ore polynomial ring associated with $\mathcal{R}$ and $\mathbb{C}$.

Remark 2.11. *In Example 2.9, if we consider $L = \mathbb{C}(t)$, then $\mathcal{R}' = \mathbb{C}(t)[U][x; \mathrm{id}, \frac{\partial}{\partial t}]$ is not the parametric Ore polynomial ring associated with $\mathcal{R}$ and L. For example, if $(a_1, a_2) = (t, 0) \in L^2$, and $h = u_1 \in \mathbb{C}(t)[U]$, then*

$$\sigma(\phi_{\vec{a}}(h)) = \sigma(t) = 1,$$

but $\phi_{\vec{a}}(\sigma'(h)) = \phi_{\vec{a}}(0) = 0$. Hence, $\sigma(\phi_{\vec{a}}(h)) \neq \phi_{\vec{a}}(\sigma'(h))$.

3 COMPUTING THE GCRD FOR NON-PARAMETRIC ORE POLYNOMIALS

In this section, we will present the definition of the Sylvester matrix for several Ore polynomials and utilize it to compute the GCRD of non-parametric Ore polynomials.

Consider the Ore polynomial ring $\mathcal{R} = k[x; \sigma, \delta]$ over a field k. Let $n \in \mathbb{N}$ be a fixed integer and $\mathcal{R}_{<n}$ the subset of $\mathcal{R}$ with degrees less than n. A k-isomorphism is given by

$$v_n\colon \mathcal{R}_{<n} \to k^n, \quad \sum_{i=0}^{n-1} a_ix^i \mapsto (a_{n-1}, \ldots, a_0).$$

For $f_1, \ldots, f_\ell \in \mathcal{R}_{<n}$, define

$$\operatorname{mat}_n(f_1, \ldots, f_\ell) = \begin{pmatrix} v_n(f_1) \\ \vdots \\ v_n(f_\ell) \end{pmatrix}.$$

Definition 3.1 ([17]). Let $f_1, f_2 \in \mathcal{R}$ be two Ore polynomials. The *Sylvester matrix* of f_1 and f_2 is defined as

$$\operatorname{Syl}(f_1, f_2) = \operatorname{mat}_n(x^{m_2-1}f_1, \ldots, xf_1, f_1, x^{m_1-1}f_2, \ldots, xf_2, f_2),$$

where $m_1 = \deg f_1$, $m_2 = \deg f_2$, and $n = m_1 + m_2$.

Li and Nemes presented the following proposition in [18].

Proposition 3.2. *Let $f_1, f_2 \in \mathcal{R}$. Then the Sylvester matrix of f and g can be transformed into G through elementary row transformations, where G satisfies the following conditions:*

(1) $G = \begin{pmatrix} I_r & C \\ O & O \end{pmatrix}$ *and $C \in k^{r\times(n-r)}$, where I_r is the $r \times r$ identity matrix.*
(2) *Suppose the last non-zero row of G is*

$$\vec{w}_r = (0, \ldots, 0, 1, c_{r,r+1}, \ldots, c_{r,n}),$$

then $\operatorname{gcrd}(f_1, f_2) = x^{n-r} + c_{r,r+1}x^{n-r-1} + \cdots + c_{r,n}$.

In the following, we extend Proposition 3.2 from two polynomials to a set of polynomials. Denote by $[m]$ the set $\{0, 1, \ldots, m-1\}$.

Definition 3.3. Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}$ be a set of Ore polynomials, and let $p \in F$. The Sylvester matrix of F with respect to p is defined as

$$\operatorname{Syl}(F; p) = \operatorname{mat}_n(x^ip, x^jf\colon f \in F \setminus \{p\},\ i \in [m], j \in [\deg(p)]),$$

where $m = \max\{\deg(f)\colon f \in F \setminus \{p\}\}$ and $n = m + \deg(p)$.

Theorem 3.4. *Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}$, and let $p \in F$. Then the Sylvester matrix $\operatorname{Syl}(F; p)$ can be transformed into G through elementary row transformations, where G satisfies the following conditions:*

(1) $G = \begin{pmatrix} I_r & C \\ O & O \end{pmatrix}$ *and $C \in k^{r\times(n-r)}$, where I_r is the $r \times r$ identity matrix.*

(2) *Suppose the last non-zero row of G is*

$$\vec{w}_r = (0, \ldots, 0, 1, c_{r,r+1}, \ldots, c_{r,n}),$$

then $\operatorname{gcrd}(f_1, \ldots, f_\ell) = x^{n-r} + c_{r,r+1}x^{n-r-1} + \cdots + c_{r,n}$.

Proof. We prove it by induction on ℓ. The theorem is true for $\ell = 2$ according to Proposition 3.2. We assume that the theorem is true for $\ell - 1$. For ℓ, without loss of generality, we suppose $p = f_1$ and $\deg(f_2) \geq \deg(f_3) \geq \cdots \geq \deg(f_\ell)$. Then

$$\operatorname{Syl}(F; p) = \operatorname{mat}_n(x^i p, x^j f : i \in [m], f \in F \setminus \{p\}, j \in [\deg(p)]).$$

Let $F' = \{f_1, \ldots, f_{\ell-1}\}$. Then $\operatorname{Syl}(F; p)$ consists of the rows of $\operatorname{Syl}(F'; p)$ and $v_n(x^j f_\ell)$ with $j \in [\deg(p)]$. Denote the GCRD of $f_1, \ldots, f_{\ell-1}$ by g'. By the induction hypothesis, the reduced row echelon form of $\operatorname{Syl}(F'; p)$ is as follows:

$$G' = \begin{pmatrix} I_{r'} & C' \\ O & O \end{pmatrix},\ C' \in k^{r' \times (n-r')}, \tag{2}$$

where $r' = n - \deg(g')$. Moreover, the last non-zero row of G corresponds to g'. Suppose that $\vec{w}_1, \ldots, \vec{w}_{r'}$ are the first r' rows of G' and M' is the module generated by the rows of $\operatorname{Syl}(F'; p)$ over k. For any $v_n(x^i g')$ with $i \in [\deg(f_\ell)]$, we can verify that $v_n(x^i g') \in M'$: Since $n \geq \deg(f_\ell) + \deg(g')$, then $v_n(x^i g')$ can be defined. Reduce $v_n(x^i g')$ by $\vec{w}_1, \ldots, \vec{w}_\ell$ and obtain a new vector $\vec{w} \in M$ that corresponds to a polynomial w with degree less than g'. However, w belongs to the left ideal generated by $f_1, \ldots, f_{\ell-1}$, which is equal to the left ideal generated by g'. Hence, $w = 0$, which implies that $v_n(x^i g') \in M'$.

Suppose that $g = \operatorname{gcrd}(g', f_\ell)$, which is also equal to the GCRD of $f_1, \ldots, f_\ell$. Let M be the module generated by the rows of $\operatorname{Syl}(F; p)$ over k, then $v_n(x^i g') \in M' \subset M$ for any $i \in [\deg(f_\ell)]$. Moreover, each $v_n(x^j f_\ell)$, $j \in [\deg(g')]$, also belongs to M. Therefore, by Proposition 3.2 we have $v_n(g) \in M$ and there exists

$$\vec{w}'_k = (0, \cdots, 0, \underbrace{0, \ldots, 0}_{k-1}, \overbrace{1, c'_{k,k+1}, \ldots, c'_{k,n}}^{\deg g' + \deg f_\ell}) \in M, \tag{3}$$

where $k = 1, \ldots, \deg g' + \deg f_\ell - \deg g$. By (2) and (3), there exists

$$\vec{w}_i = (\overbrace{0, \cdots, 0}^{i-1}, 1, c_{i,i+1}, \ldots, c_{1,n}) \in M, i = 1, \ldots, n - \deg g.$$

where $\vec{w}_1, \ldots, \vec{w}_{r'}$ are the first r' rows of G', and $\vec{w}_{r'+t} = \vec{w}'_{t+\deg f_\ell}$ for $t = 1, \ldots, \deg(g') - \deg(g)$. Thus, $\operatorname{rank}(\operatorname{Syl}(F; p)) \geq n - \deg g$. If $\operatorname{rank}(\operatorname{Syl}(F; p)) > n - \deg g$, we get a non-zero vector $\vec{w} \in M$, with $\deg(v_n^{-1}(\vec{w})) < \deg(g)$. However, it is impossible since $v_n^{-1}(\vec{w})$ belongs to the left ideal generated by $f_1, \ldots, f_\ell$, which is equal to the left ideal generated by g. Therefore,

$$\operatorname{rank}(\operatorname{Syl}(F; p)) = n - \deg(g).$$

In addition, since $\vec{w}_i \in M$, $i = 1, \ldots, n - \deg g$, then the reduced row echelon form of $\operatorname{Syl}(F; p)$ is as follows:

$$G = \begin{pmatrix} I_r & C \\ O & O \end{pmatrix},\ C \in k^{r \times (n-r)}, r = n - \deg(g).$$

Suppose the last non-zero row of G is

$$\vec{w}_r = (0, \ldots, 0, 1, c_{r,r+1}, \ldots, c_{r,n}),$$

and let $\tilde{g} = x^{n-r} + c_{r,r+1}x^{n-r-1} + \cdots + c_{r,n}$. By the definition of $\operatorname{Syl}(F; p)$, $\tilde{g}$ belongs to the left ideal generated by $f_1, \ldots, f_\ell$, which is equal to the left ideal generated by g. Furthermore, $\tilde{g}$ is with the same degree as g. So

$$g = \tilde{g} = x^{n-r} + c_{r,r+1}x^{n-r-1} + \cdots + c_{r,n},$$

completing the induction. □

Remark 3.5. *For the polynomial ring, a similar result is proved in [29], and Theorem 3.4 is a generalization of Theorem 2.4.4. in [29].*

Here a simple example is presented to illustrate Theorem 3.4.

Example 3.6. Let $\mathcal{R} = \mathbb{C}(t)[x; \mathrm{id}, \frac{d}{dt}]$, where $xt = tx + 1$. Let $f_1 = x^2 + (t+1)x + (t+1)$, $f_2 = x^3 + 2tx^2 + (t^2+2)x + t$, $f_3 = x^2 + 2tx + (t^2+1) \in \mathcal{R}$, $F = \{f_1, f_2, f_3\}$. Choosing $p = f_1$, then

$$\operatorname{Syl}(F; p) = \begin{pmatrix} 1 & t+1 & t+3 & 2 & 0 \\ 0 & 1 & t+1 & t+2 & 1 \\ 0 & 0 & 1 & t+1 & t+1 \\ 1 & 2t & t^2+4 & 3t & 1 \\ 0 & 1 & 2t & t^2+2 & t \\ 0 & 1 & 2t & t^2+3 & 2t \\ 0 & 0 & 1 & 2t & t^2+1 \end{pmatrix}.$$

By computing, the reduced row echelon form of $\operatorname{Syl}(F; p)$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -t^4+6t^2-3 \\ 0 & 1 & 0 & 0 & t^3-3t \\ 0 & 0 & 1 & 0 & -t^2+1 \\ 0 & 0 & 0 & 1 & t \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then $\operatorname{gcrd}(f_1, f_2, f_3) = x + t$.

4 PARAMETRIC GCRD FOR PARAMETRIC ORE POLYNOMIALS

Let $\mathcal{R} = k[x; \sigma, \delta]$. Suppose that $L \subset k$ and $U = \{u_1, \ldots, u_s\}$. Let $\mathcal{R}' = k[U][x; \sigma', \delta']$ be the parametric Ore polynomial ring associated with $\mathcal{R}$ and L.

4.1 Parametric Sylvester matrix

In this subsection we will define the parametric Sylvester matrix that is compatible with the Sylvester matrix defined above.

Let $\mathcal{R}'_{<n}$ be the subset of $\mathcal{R}'$ consisting of polynomials with x-degree less than n. We define a R'-isomorphism

$$v_n : \mathcal{R}' \to k[U]^n, \qquad \sum_{i=0}^{n-1} c_i(U)x^i \mapsto (c_{n-1}(U), \ldots, c_0(U)).$$

For convenience, $v_n(f)$ is denoted by $\vec{f}$ if there is no confusion about n in context.

For $f_1, \ldots, f_\ell \in \mathcal{R}'_{<n}$, define

$$\operatorname{mat}_n(f_1, \ldots, f_\ell) = \begin{pmatrix} \vec{f}_1 \\ \vdots \\ \vec{f}_\ell \end{pmatrix}.$$

Remark 4.1. *Let $\phi_{\vec{a}} : k[U] \to k$ be a specialization induced by the element $\vec{a}$ in L^s. It can be extended to a specialization $\phi_{\vec{a}} : k[U]^n \to k^n$ by applying $\phi_{\vec{a}}$ entry-wise. It is easy to check that*

(1) *$\phi_{\vec{a}}(c \cdot \vec{f}) = \phi_{\vec{a}}(c) \cdot \phi_{\vec{a}}(\vec{f})$ for $c \in k[U]$, $\vec{f} \in k[U]^n$;*
(2) *$\phi_{\vec{a}}(\vec{f}_1 + \vec{f}_2) = \phi_{\vec{a}}(\vec{f}_1) + \phi_{\vec{a}}(\vec{f}_2)$ for $\vec{f}_1, \vec{f}_2 \in k[U]^n$;*
(3) *$v_n(\phi_{\vec{a}}(f)) = \phi_{\vec{a}}(v_n(f))$ for $f \in k[U]$.*

Lemma 4.2. *Let $\mathcal{R}'$ be the parametric Ore polynomial ring associated with $\mathcal{R}$ and L, and let $\phi_{\vec{a}}\colon k[U] \to k$ be a specialization induced by $\vec{a} \in L^s$. Then*

(1) *$\phi_{\vec{a}}(xf) = x\phi_{\vec{a}}(f)$ for any polynomial $f \in \mathcal{R}'$.*
(2) *$\phi_{\vec{a}}(hf) = \phi_{\vec{a}}(h)\phi_{\vec{a}}(f)$ for any polynomials $h, f \in \mathcal{R}'$.*
(3) *For any $m < n - \deg(f)$, we have*

$$\phi_{\vec{a}}\left(\mathrm{mat}_n(f, xf, \ldots, x^m f)\right) = \mathrm{mat}_n(\phi_{\vec{a}}(f), x\phi_{\vec{a}}(f), \ldots, x^m\phi_{\vec{a}}(f)).$$

Proof. (1) For any $f = \sum_{i=0}^{n-1} c_i x^i \in \mathcal{R}'$, we have

$$\begin{aligned}\phi_{\vec{a}}(x \cdot f) &= \phi_{\vec{a}}\left(\sum_{i=0}^{n-1} x c_i x^i\right)\\ &= \phi_{\vec{a}}\left(\sum_{i=0}^{n-1} (\sigma'(c_i)x + \delta'(c_i))x^i\right)\\ &= \sum_{i=0}^{n-1} (\phi_{\vec{a}}(\sigma'(c_i))x + \phi_{\vec{a}}(\delta'(c_i)))x^i\\ &= \sum_{i=0}^{n-1} (\sigma(\phi_{\vec{a}}(c_i))x + \delta(\phi_{\vec{a}}(c_i)))x^i = x\phi_{\vec{a}}(f)\end{aligned}$$

(2) For any $h = \sum_{i=0}^{s} c_i x^i$, we have

$$\begin{aligned}\phi_{\vec{a}}(hf) &= \phi_{\vec{a}}\left(\sum_{i=0}^{s} c_i (x^i \cdot f)\right)\\ &= \sum_{i=0}^{s} \phi_{\vec{a}}(c_i)\phi_{\vec{a}}(x^i \cdot f)\\ &= \sum_{i=0}^{s} \phi_{\vec{a}}(c_i)x^i\phi_{\vec{a}}(f) = \phi_{\vec{a}}(h)\phi_{\vec{a}}(f).\end{aligned}$$

(3) It is easy to check that

$$\begin{aligned}\mathrm{mat}_n(\phi_{\vec{a}}(f),, \ldots, x^m\phi_{\vec{a}}(f)) &= \begin{pmatrix} v_n(\phi_{\vec{a}}(f)) \\ \vdots \\ v_n(x^m\phi_{\vec{a}}(f)) \end{pmatrix} = \begin{pmatrix} v_n(\phi_{\vec{a}}(f)) \\ \vdots \\ v_n(\phi_{\vec{a}}(x^m f)) \end{pmatrix}\\ &= \phi_{\vec{a}}\left(\mathrm{mat}_n(f, xf, \ldots, x^m f)\right),\end{aligned}$$

where the last equation can be verified by Remark 4.1.(3). □

In the following, we introduce the parametric Sylvester matrix for polynomials in $\mathcal{R}'$. For any $f \in \mathcal{R}'$, the leading coefficient of f with respect to x is denoted by $\mathrm{lc}_x(f)$.

Definition 4.3. Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}'$ and $p \in F$. The *parametric Sylvester matrix of F with respect to p* is defined as

$$\mathrm{PSyl}(F; p) = \mathrm{mat}_n(x^i p, x^j f\colon f \in F \setminus \{p\}, i \in [m],\ j \in [\deg_x(p)]),$$

where $m = \max\{\deg_x(f)\colon f \in F \setminus \{p\}\}$ and $n = m + \deg_x(p)$.

Based on the definition of parametric Sylvester matrices, the following two propositions can be obtained.

Proposition 4.4. *Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}'$ and $p \in F$. Let $\phi_{\vec{a}}$ be the specialization induced by $\vec{a} \in L^s$. If $\phi_{\vec{a}}(\mathrm{lc}_x(f)) \neq 0$ for all $f \in F$, then*

$$\phi_{\vec{a}}(\mathrm{PSyl}(F; p)) = \mathrm{Syl}(\phi_{\vec{a}}(F); \phi_{\vec{a}}(p)),$$

where $\phi_{\vec{a}}(F) = \{\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell)\}$.

Proof. It can be verified by the definitions and Lemma 4.2 directly. □

Proposition 4.5. *Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}'$ and $p \in F$. Let $\phi_{\vec{a}}$ be the specialization induced by $\vec{a} \in L^s$, with $\phi_{\vec{a}}(\mathrm{lc}_x(p)) \neq 0$. Then*

$$\phi_{\vec{a}}(\mathrm{PSyl}(F; p)) = \begin{pmatrix} A & B \\ \mathbf{0} & \mathrm{Syl}(\phi_{\vec{a}}(F); \phi_{\vec{a}}(p)) \end{pmatrix},$$

with $(A, B) = \mathrm{mat}_n(x^i p\colon i = m', \ldots, m-1) \in L^{(m-m')\times n}$, where $m = \max\{\deg_x(f)\colon f \in F \setminus \{p\}\}$ and $m' = \max\{\deg(\phi_{\vec{a}}(f))\colon f \in F \setminus \{p\}\}$.

Proof. It can be verified directly by the definition of parametric Sylvester matrix and Lemma 4.2. □

An illustrative example is presented as follows.

Example 4.6. Let $\mathcal{R} = \overline{\mathbb{F}_2}[x; \sigma, 0]$, where $\sigma(c) = c^2$ for $c \in \overline{\mathbb{F}_2}$, and let $L = \overline{\mathbb{F}_2}$. Then $\mathcal{R}' = \overline{\mathbb{F}_2}[u_1, u_2][x; \sigma', 0]$ is the parametric Ore polynomial ring associate with $\mathcal{R}$ and L, where $\sigma'(c(u_1, u_2)) = c(u_1, u_2)^2$. Let $f_1 = x^2 + u_1 x + 1$, $f_2 = u_1 x^3 + u_2 x + 1$, $f_3 = u_1 x^2 + u_2 \in R'$ and $F = \{f_1, f_2, f_3\}$. By Definition 4.3,

$$\mathrm{PSyl}(F; f_1) = \begin{pmatrix} 1 & u_1^4 & 1 & 0 & 0 \\ 0 & 1 & u_1^2 & 1 & 0 \\ 0 & 0 & 1 & u_1 & 1 \\ u_1^2 & 0 & u_2^2 & 1 & 0 \\ 0 & u_1 & 0 & u_2 & 1 \\ 0 & u_1^2 & 0 & u_2^2 & 0 \\ 0 & 0 & u_1 & 0 & u_2 \end{pmatrix}.$$

Let $\phi_{\vec{a}}\colon \overline{\mathbb{F}_2}[u_1, u_2] \to \overline{\mathbb{F}_2}$ be a specialization induced by $(0, a_2) \in \overline{\mathbb{F}_2}^2$ with $a_2 \neq 0$, then

$$\phi_{\vec{a}}(\mathrm{PSyl}(F; f_1)) = \left(\begin{array}{ccccc} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ \hline 0 & 0 & a_2^2 & 1 & 0 \\ 0 & 0 & 0 & a_2 & 1 \\ 0 & 0 & 0 & a_2^2 & 0 \\ 0 & 0 & 0 & 0 & a_2 \end{array}\right),$$

with $\mathrm{Syl}(\phi_{\vec{a}}(F); \phi_{\vec{a}}(f_1)) = \begin{pmatrix} 1 & 0 & 1 \\ a_2^2 & 1 & 0 \\ 0 & a_2 & 1 \\ 0 & a_2^2 & 0 \\ 0 & 0 & a_2 \end{pmatrix}$.

4.2 Computing parametric GCRD by Gröbner bases for modules

Now, we will present the main theorem that the parametric GCRD can be obtained by computing the Gröbner basis of the module generated by the rows of the parametric Sylvester matrix.

Let F be a subset of $\mathcal{R}'$. In the following, $M(F; p)$ denotes the module generated by the rows of $\mathrm{PSyl}(F; p)$ over $k[U]$ in $k[U]^n$.

Similar to Theorem 3.4 for the non-parametric case, we obtain the following lemma for the parametric case.

Lemma 4.7. *Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}'$, and $p \in F$. Suppose that $\max\{\deg(f)\colon f \in F \setminus \{p\}\} > 0$. Let $\phi_{\vec{a}}$ be a specialization from $k[U]$ to k induced by $\vec{a} \in L^s$ with $\phi_{\vec{a}}(\mathrm{lc}_x(p)) \neq 0$. Assume $g = \mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell))$, then*

(1) *The reduced row echelon form of $\phi_{\vec{a}}(\mathrm{PSyl}(F; p))$ is as follows:*

$$G = \begin{pmatrix} I_r & C \\ O & O \end{pmatrix},\ C \in L^{r\times(n-r)},$$

Furthermore, suppose $\vec{w}_1, \ldots, \vec{w}_r$ are the first r rows of G, then

(a) $v_n^{-1}(\vec{w}_r) = g$;

(b) *There exist $\vec{q}_i \in M(F;p)$ such that $\phi_{\vec{a}}(\vec{q}_i) = \vec{w}_i$, for $i = 1, \ldots, r$.*

(2) *There exists $\vec{q} \in M(F;p)$ such that $\phi_{\vec{a}}(q) = g$ and $\phi_{\vec{a}}(\mathrm{lc}_x(q)) \neq 0$, where $q = v_n^{-1}(\vec{q})$.*

Proof. (1) The reduced row echelon form of $\phi_{\vec{a}}(\mathrm{PSyl}(F;p))$ and $g = v_n^{-1}(\vec{w}_r)$ can be directly derived by Proposition 4.5 and Theorem 3.4. We prove (1.b) as follows. Since $\phi_{\vec{a}}(\mathrm{PSyl}(F;p))$ can be reduced to G by Gaussian elimination, there exists $V \in k^{n\times n}$, such that

$$V \cdot \phi_{\vec{a}}(\mathrm{PSyl}(F;p)) = G.$$

Therefore, there exist $c_{ij} \in k$, $i = 1, \ldots, r$, $j = 1, \ldots, t$ such that

$$\vec{w}_i = \sum_{j=1}^{t} c_{ij}\phi_{\vec{a}}(\vec{v}_j), i = 1, \ldots, r,$$

where $\vec{v}_1, \ldots, \vec{v}_t$ are rows of $\mathrm{PSyl}(F;p)$. Let $\vec{q}_i = \sum_{j=1}^{t} c_{ij}\vec{v}_j, i = 1, \ldots, r$, then $\phi_{\vec{a}}(\vec{q}_i) = \vec{w}_i$.

(2) By the above conclusion (1), there exist $\vec{q}_1, \ldots, \vec{q}_r \in M$, such that $\phi_{\vec{a}}(\vec{q}_i) = \vec{w}_i$. Suppose

$$\begin{pmatrix}\vec{w}_1\\ \vec{w}_2\\ \vdots\\ \vec{w}_r\end{pmatrix} = \begin{pmatrix}1 & 0 & \cdots & 0 & c_{1,r+1} & \cdots & c_{1,n}\\ 0 & 1 & \cdots & 0 & c_{2,r+1} & \cdots & c_{2,n}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1 & c_{r,r+1} & \cdots & c_{r,n}\end{pmatrix}, \tag{4}$$

then $\mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell)) = x^{n-r} + c_{r,r+1}x^{n-r-1} + \cdots + c_{r,n}$. Let

$$Q = \begin{pmatrix}\vec{q}_1\\ \vec{q}_2\\ \vdots\\ \vec{q}_r\end{pmatrix} = \begin{pmatrix}q_{1,1} & \cdots & q_{1,r-1} & q_{1,r} & q_{1,r+1} & \cdots & q_{1,n}\\ q_{2,1} & \cdots & q_{2,r-1} & q_{2,r} & q_{2,r+1} & \cdots & q_{2,n}\\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ q_{r,1} & \cdots & q_{r,r-1} & q_{r,r} & q_{r,r+1} & \cdots & q_{r,n}\end{pmatrix}. \tag{5}$$

By Equation (4) and Equation (5), we have

$$\phi_{\vec{a}}(Q) = \begin{pmatrix}\phi_{\vec{a}}(\vec{q}_1)\\ \phi_{\vec{a}}(\vec{q}_2)\\ \vdots\\ \phi_{\vec{a}}(\vec{q}_r)\end{pmatrix} = \begin{pmatrix}1 & 0 & \cdots & 0 & c_{1,r+1} & \cdots & c_{1,n}\\ 0 & 1 & \cdots & 0 & c_{2,r+1} & \cdots & c_{2,n}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1 & c_{r,r+1} & \cdots & c_{r,n}\end{pmatrix}.$$

Assume that $q(x)$ is the determinant polynomial of Q. By definition of determinant polynomial (see [19], Definition 7.5.1),

$$q(x) = b_{n-r}x^{n-r} + b_{n-r-1}x^{n-r-1} + \cdots + b_1x + b_0,$$

where

$$b_i = \det\begin{pmatrix}q_{1,1} & \cdots & q_{1,r-1} & q_{1,n-i}\\ q_{2,1} & \cdots & q_{2,r-1} & q_{2,n-i}\\ \vdots & \ddots & \vdots & \vdots\\ q_{r,1} & \cdots & q_{r,r-1} & q_{r,n-i}\end{pmatrix}, i = 0, 1, \ldots, n-r.$$

Therefore, $\phi_{\vec{a}}(b_{n-r}) = 1$, $\phi_{\vec{a}}(b_i) = c_{r,n-i}$, $i = 0, \ldots, n-r-1$. Then $\phi_{\vec{a}}(q) = g$ and $\phi_{\vec{a}}(\mathrm{lc}_x(q)) = 1 \neq 0$. According to the property of determinant polynomial (see [19], Section 7.5), $\vec{q} = v_n(q)$ belongs to the module generated by the rows of Q. Since $\vec{q}_i \in M(F;p)$, then $\vec{q} \in M(F;p)$. Thus, there exists $\vec{q} \in M(F;p)$ such that $\phi_{\vec{a}}(q) = g$ and $\phi_{\vec{a}}(\mathrm{lc}_x(q)) \neq 0$. □

Theorem 4.8. *Let $F = \{f_1, \ldots, f_\ell\} \subset \mathcal{R}'$, $p \in F$, and $\phi_{\vec{a}}\colon k[U] \to k$ be a specialization induced by $\vec{a} \in L^s$ with $\phi_{\vec{a}}(\mathrm{lc}_x(p)) \neq 0$. Suppose that $\max\{\deg(f)\colon f \in F \setminus \{p\}\} > 0$, $\vec{\mathcal{G}}$ is a Gröbner basis of the module $M(F;p)$ with respect to a POT order $\succ$ with $\mathbf{e}_1 \succ \mathbf{e}_2 \succ \ldots \succ \mathbf{e}_n$, where $n = \max\{\deg_x(f)\colon f \in F \setminus \{p\}\} + \deg_x(p)$, $\mathcal{G} = \{g \in k[U][x]\colon v_n(g) \in \vec{\mathcal{G}}\}$ and $\mathcal{G}_i = \{g \in \mathcal{G}\colon \deg_x(g) = i\}$. Then the following conditions are equivalent:*

(1) *the degree of $\mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell))$ is greater than d;*

(2) *for all $g \in \bigcup_{i=0}^{d} \mathcal{G}_i$, $\phi_{\vec{a}}(\mathrm{lc}_x(g)) = 0$.*

Further, if the elements in $\mathcal{G}$ are ordered from small to large according to x-degree, then $\mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell)) = \phi_{\vec{a}}(g)$ (up to a non-zero constant), where g is the first element in $\mathcal{G}$ satisfying $\phi_{\vec{a}}(\mathrm{lc}_x(g)) \neq 0$.

Proof. (2) $\Rightarrow$ (1). Let $g = \mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell))$ in $\mathcal{R}$. Assume $\deg(g) = r \leq d$. By (2) in Lemma 4.7, there exists $\vec{q} \in M(F;p)$ such that $\deg_x(q) = \deg(g)$ and $\phi_{\vec{a}}(\mathrm{lc}_x(q)) \neq 0$. According to the property of Gröbner bases for the module $M(F;p)$, $\vec{q}$ can be reduced to the zero vector by $\{\vec{g}\colon g \in \mathcal{G}_i, i = 0, \ldots, d\}$ in $k[U]^n$. Therefore, there exist $\{c_g\colon g \in \mathcal{G}_r\} \subset k[U]$ such that

$$\mathrm{lc}_x(q) = \sum_{g\in\mathcal{G}_r} c_g\,\mathrm{lc}_x(g).$$

However, $\phi_{\vec{a}}(\mathrm{lc}_x(g)) = 0$ for all $g \in \mathcal{G}_r$, which implies that

$$\phi_{\vec{a}}(\mathrm{lc}_x(q)) = 0.$$

This is contradictory to the assumption.

(1) $\Rightarrow$ (2). Suppose there exists $\tilde{g} \in \mathcal{G}$ with $\deg_x(\tilde{g}) \leq d$ and $\phi_{\vec{a}}(\mathrm{lc}_x(\tilde{g})) \neq 0$. Let $g = \mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell))$. Since $\tilde{g}$ belongs to the left ideal generated by $f_1, \ldots, f_\ell$ in $\mathcal{R}'$, there exist $h_1, \ldots, h_\ell \in \mathcal{R}'$ such that $\tilde{g} = \sum_{i=1}^{\ell} h_i f_i$. By (2) in Lemma 4.2, we have

$$\phi_{\vec{a}}(\tilde{g}) = \sum_{i=1}^{\ell} \phi_{\vec{a}}(h_i)\phi_{\vec{a}}(f_i).$$

Therefore, $\phi_{\vec{a}}(\tilde{g})$ belongs to the left ideal $\langle\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell)\rangle = \langle g\rangle$, which implies that

$$\deg(g) \leq \deg(\phi_{\vec{a}}(\tilde{g})) = \deg_x(\tilde{g}) \leq d.$$

It contradicts the assumption that the degree of g is greater than d.

By the above conclusion, when the elements in $\mathcal{G}$ are ordered from small to large according to x-degree, we have

$$\mathrm{gcrd}(\phi_{\vec{a}}(f_1), \ldots, \phi_{\vec{a}}(f_\ell)) = \phi_{\vec{a}}(g)$$

where g is the first element in $\mathcal{G}$ satisfying $\phi_{\vec{a}}(\mathrm{lc}_x(g)) \neq 0$. □

5 THE PROPOSED ALGORITHM AND IMPLEMENTATION

Based on Theorem 4.8, we are ready to give an algorithm to compute a parametric GCRD for Ore polynomials.

5.1 Algorithm

Let $\mathcal{R} = k[x;\sigma,\delta]$ be an Ore polynomial ring and L a subset of k. Suppose that $\mathcal{R}' = k[U][x;\sigma',\delta']$ is the parametric Ore polynomial ring associated with $\mathcal{R}$ and L. Let $F = \{f_1, \ldots, f_\ell\} \subset k[U][x]$. We will present an algorithm to compute the parametric GCRD in Definition 2.4.

We first give some explanations for Algorithm 1.

Algorithm 1: Parametric GCRD for Ore polynomials

Input : $F = \{f_1, \ldots, f_t\} \subset k[U][x; \sigma', \delta']$.
Output: $D = \{(E_1, N_1, d_1), \ldots, (E_t, N_t, d_t)\}$ is the parametric GCRD of $f_1, \ldots, f_t$.

1 $D := \emptyset$; $E_0 := \{0\}$;
2 **while** $\langle E_0 \rangle \neq k[U]$ **do**
3 $F := \text{reduce}(F, E_0)$;
4 **if** $F = \{0\}$ **then**
5 $D := D \cup \{(E_0, \{1\}, \text{"any polynomial"})\}$
6 **return** D;
7 **end if**
8 $N_0 := \{f \in F : \deg_x(f) = 0\}$;
9 **if** $N_0 \neq \emptyset$ **then**
10 $D := D \cup \{(E_0, N_0, 1)\}$
11 $E_0 := E_0 \cup N_0$;
12 **go to line 3**;
13 **end if**
14 $p := f, f \in F$ with minimal x-degree;
15 $N := \{\text{lc}_x(p)\}$;
16 $M := \text{PSyl}(F; p)$;
17 $\vec{\mathcal{G}}$:= the Gröbner basis of the module generated by the rows of M;
18 $\mathcal{G}_0 := \{g : \vec{g} \in \vec{\mathcal{G}},\ \deg_x(g) = 0\}$;
19 $D := D \cup \{(E_0, \mathcal{G}_0 \times N, 1)\}$;
20 $i := 1$;
21 $m := \max\{\deg_x(f) : f \in F\}$;
22 $E := \mathcal{G}_0$;
23 **while** $\langle E \rangle \neq k[U]$ and $i \leq m$ **do**
24 $\mathcal{G}_i := \{g : \vec{g} \in \vec{\mathcal{G}},\ \deg_x(g) = i\}$;
25 **for** $g \in \mathcal{G}_i$ **do**
26 $D := D \cup \{(E, N \times \{\text{lc}_x(g)\}, g)\}$;
27 $E := E \cup \{\text{lc}_x(g)\}$;
28 **end for**
29 $i := i + 1$;
30 **end while**
31 $E_0 := E_0 \cup N$;
32 **end while**
33 **return** D.

- In line 3, $P := \text{reduce}(P, E_0)$ means to reduce P by the Gröbner basis of $\langle E_0 \rangle$;
- In line 19, $\mathcal{G}_0 \times N = \{g \cdot f : g \in \mathcal{G}_0, f \in N\}$.

Theorem 5.1. *The algorithm is correct and terminates in finitely many steps.*

Proof. The correctness is based on Theorem 4.8.

Termination. In line 3, we reduce F by the Gröbner basis of $\langle E_0 \rangle \subset k[U]$ and get a new F. Therefore, the leading term of the non-zero polynomials in the new F does not belong to $\langle E_0 \rangle$. Then in line 31, the ideal $\langle E_0 \rangle$ increases strictly. Finally, F will be zero or $\langle E_0 \rangle = k[U]$. The algorithm terminates. □

Here we use an example to illustrate the steps in Algorithm 1.

Example 5.2. Let $\mathcal{R} = \overline{\mathbb{F}_2}[x; \sigma, 0]$ with $\sigma(c) = c^2$ for $c \in \overline{\mathbb{F}_2}$. Let $L = \overline{\mathbb{F}_2}$. The parametric Ore polynomial ring associated with $\mathcal{R}$ and L is $\mathcal{R}' = \overline{\mathbb{F}_2}[u_1, u_2][x; \sigma', 0]$, where

$$\sigma' : \overline{\mathbb{F}_2}[u_1, u_2] \to \overline{\mathbb{F}_2}[u_1, u_2], \qquad h(u_1, u_2) \mapsto h(u_1, u_2)^2.$$

Let $f_1 = u_2x^2 + x + u_1$, $f_2 = u_2x^3 + x^2$, $f_3 = u_1x^2 + 1 \in \mathbb{F}_2[u_1, u_2][x]$.

Initial: $D := \emptyset$; $E_0 := \{0\}$, $F := \{f_1, f_2, f_3\}$;

Now $\langle E_0 \rangle \neq k[U]$. We choose $p = f_1$. Then $N := \{\text{lc}_x(p)\} = \{u_2\}$,

$$M := \text{PSyl}(F; p) = \begin{pmatrix} u_2^4 & 1 & u_1^4 & 0 & 0 \\ 0 & u_2^2 & 1 & u_1^2 & 0 \\ 0 & 0 & u_2 & 1 & u_1 \\ u_2^2 & 1 & 0 & 0 & 0 \\ 0 & u_2 & 1 & 0 & 0 \\ 0 & u_1^2 & 0 & 1 & 0 \\ 0 & 0 & u_1 & 0 & 1 \end{pmatrix}.$$

By computation, the Gröbner basis of the module generated by the rows of M under the POT order with the degree reverse lexicographic order where $u_1 > u_2$ is

$$\vec{\mathcal{G}} := \{(0,0,0,0,u_2^2 + u_2 + 1), (0,0,0,0,u_1^2 + 1), (0,0,0,1,u_1u_2 + u_1), (0,0,1,0,u_1), (0,1,0,0,u_1u_2 + u_1), (u_2^2,0,0,0,u_1u_2 + u_1)\}.$$

Then $\mathcal{G}_0 := \{u_2^2 + u_2 + 1, u_1^2 + 1\}$. Thus,

$$D := D \cup \{(E_0, \{u_2^2 + u_2 + 1, u_1^2 + 1\} \times N, 1)\}$$
$$= \{(\{0\}, \{(u_2^2 + u_2 + 1)u_2, (u_1^2 + 1)u_2\}, 1)\}.$$

Now, let $E := \{u_2^2 + u_2 + 1, u_1^2 + 1\}$.

Since $\langle E \rangle \neq k[U]$, we consider $\mathcal{G}_1 := \{x + u_1u_2 + u_1\}$. Therefore,

$$D := D \cup \{(E, \{\text{lc}_x(x + u_1u_2 + u_1)\} \times N, x + u_1u_2 + u_1)\}$$
$$= D \cup \{\{u_2^2 + u_2 + 1, u_1^2 + 1\}, \{u_2\}, x + u_1u_2 + u_1\}.$$

Updating $E := E \cup \{\text{lc}_x(x + u_1u_2 + u_1)\} = \{u_2^2 + u_2 + 1, u_1^2 + 1, 1\}$. Now $\langle E \rangle = k[U]$.

Let $E_0 := E_0 \cup N = \{u_2\}$. Since $\langle E_0 \rangle \neq k[U]$,

$$F := \text{reduce}(F, E_0) = \{x + u_1, x^2, u_1x^2 + 1\}.$$

Choosing $p = x + u_1$, $N := \{1\}$, then

$$M := \text{PSyl}(F; p) = \begin{pmatrix} 1 & u_1^2 & 0 \\ 0 & 1 & u_1 \\ 1 & 0 & 0 \\ u_1 & 0 & 1 \end{pmatrix}.$$

By computing, the Gröbner basis of the module generated by the rows of M is $\vec{\mathcal{G}} = \{(1,0,0), (0,1,0), (0,0,1)\}$. Thus $D := D \cup \{(E_0, \{1\} \times N, 1)\} = D \cup \{(u_2, \{1\}, 1)\}$.

Updating $E_0 := E_0 \cup N = \{u_2, 1\}$. We have $\langle E_0 \rangle = k[U]$. Hence, the algorithm terminates.

In summary, the parametric GCRD of $\{u_2x^2 + x + u_1, u_2x^3 + x^2, u_1x^2 + 1\}$ is $D = \{(\{0\}, \{(u_2^2 + u^2 + 1)u_2, (u_1^2 + 1)u_2\}, 1), (\{u_2^2 + u_2 + 1, u_1^2 + 1\}, \{u_2\}, x + u_1u_2 + u_1), (\{u_2\}, \{1\}, 1)\}$.

It means that for $(a_1, a_2) \in \overline{\mathbb{F}_2}^2$, we have

(1) If $(a_2^2 + a_2 + 1)a_2 \neq 0$ or $(a_1^2 + 1)a_2 \neq 0$, then
$$\text{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = 1.$$
(2) If $a_2^2 + a_2 + 1 = 0$, $a_1^2 + 1 = 0$ and $a_2 \neq 0$, then
$$\text{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = x + a_1a_2 + a_1.$$
(3) If $a_2 = 0$, then $\text{gcrd}(\phi_{\vec{a}}(f_1), \phi_{\vec{a}}(f_2), \phi_{\vec{a}}(f_3)) = 1$.

5.2 Implementation

The proposed algorithm has been implemented in the computer algebra system Singular (4-3-0) with $\mathcal{R} = \overline{\mathbb{F}_2}[x, \sigma, 0]$ and $L = \overline{\mathbb{F}_2}$. The codes and examples are available on the web: http://www.mmrc.iss.ac.cn/~dwang/software.html. We randomly generate ten sets to show the performance of the proposed algorithm. The ten examples and their implementation are as follows.

$F_1 = \{x^5 + u_1x^2 + 1, x^4 + u_2x^3 + 1\}$;

$F_2 = \{x^3 + u_1^2x^2 + u_2x + u_1, u_2x^3 + (u_1 + 1)x^2 + (u_1 + u_2)x\}$;

$F_3 = \{u_2x^2 + x + u_1, u_2x^3 + x^2, u_1x^2 + 1\}$;

$F_4 = \{x^4 + u_1x^3 + u_2, x^4 + u_3x^3 + u_4, x^4 + u_5x^3 + u_6\}$;

$F_5 = \{x^4 + u_2x^2 + u_1x + u_2, u_2x^4 + u_1x^3 + u_1, x^2 + u_2x + u_1\}$;

$F_6 = \{x^5 + u_2x^2 + u_1x + u_2, u_2x^5 + u_1x^3 + u_1x^2 + u_2, x^5 + u_2x^3 + u_1\}$;

$F_7 = \{x^6 + u_1x^4 + u_2, u_2x^5 + u_1x^3 + u_3, u_1x^4 + u_2x^2 + u_1\}$;

$F_8 = \{u_3x^6 + u_1x^4 + u_3x^2 + u_1, u_2x^5 + u_1x^3 + u_3x^2, u_1x^5 + u_2x^2 + u_1\}$;

$F_9 = \{x^2 + u_1x + u_2, x^2 + u_3x + u_4, x^2 + u_5x + u_6, x^2 + u_7x + u_8\}$;

$F_{10} = \{x^4 + u_1x^2 + u_2, x^4 + u_3x^2 + u_4, x^2 + u_5x^2 + u_6, x^4 + u_7x^2 + u_8\}$.

Table 1: Implementation

Ex.	Timings	Br.	Deg.	Size	Ex.	Timings	Br.	Deg.	Size
F_1	0.044	3	35	76	F_6	0.024	4	11	24
F_2	0.035	3	20	49	F_7	4.623	5	42	592
F_3	0.016	3	3	3	F_8	2.164	8	26	99
F_4	0.099	6	22	144	F_9	0.016	5	5	16
F_5	0.011	3	8	16	F_{10}	0.093	5	18	56

- Timings (in seconds) were obtained on Intel(R) Core(TM) i5-8250U CPU @1.60GHz 1.80 GHz with 8GB Memory running Windows 10.
- "Br." is the number of branches that $\mathbb{V}_L(E_i) \setminus \mathbb{V}_L(N_i)$ is non-empty.
- Deg. = max{total degree of $f : f \in E_i \cup N_i, i = 1, \ldots, \text{Br.}\}$.
- Size = max{number of terms of $f : f \in E_i \cup N_i, i = 1, \ldots, \text{Br.}\}$.

6 CONCLUDING REMARKS

In this paper, a new algorithm to compute the parametric GCRD for a set of Ore polynomials based on Gröbner bases for modules is presented. To compute the parametric GCRD, we define the parametric Ore polynomial ring. Furthermore, if the parametric Ore polynomial ring can be constructed, then we can compute the parametric GCRD by Gröbner basis of the module generated by the rows of the parametric Sylvester matrix. In this way, we convert the problem from the non-commutative ring into the commutative module and solve the problem using commutative Gröbner bases for modules. However, if the parametric Ore polynomial ring can not be constructed, we do not know how to compute the parametric GCRD yet. This problem will be considered in further work.

ACKNOWLEDGMENTS

The research was supported partially by the National Science Foundation of China under Grant Nos. 12171469 and 12201210, and the National Key Research and Development Project 2020YFA0712300.

REFERENCES

[1] Sergei A Abramov and K Yu Kvashenko. 1993. On the greatest common divisor of polynomials which depend on a parameter. In *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation*. 152–156.

[2] Sergei A Abramov, Ha Quang Le, and Ziming Li. 2005. Univariate Ore polynomial rings in computer algebra. *Journal of Mathematical Sciences* 131, 5 (2005), 5885–5903.

[3] Ali Ayad. 2010. Complexity of algorithms for computing greatest common divisors of parametric univariate polynomials. *International Journal of Algebra* 4, 4 (2010), 173–188.

[4] Delphine Boucher, Philippe Gaborit, Willi Geiselmann, Olivier Ruatta, and Felix Ulmer. 2010. Key exchange and encryption schemes based on non-commutative skew polynomials. In *International Workshop on Post-Quantum Cryptography*. Springer, 126–141.

[5] Delphine Boucher, Willi Geiselmann, and Félix Ulmer. 2007. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing* 18, 4 (2007), 379–389.

[6] Delphine Boucher and Felix Ulmer. 2014. Linear codes using skew polynomials with automorphisms and derivations. *Designs, codes and cryptography* 70, 3 (2014), 405–431.

[7] Manuel Bronstein and Marko Petkovšek. 1996. An introduction to pseudo-linear algebra. *Theoretical Computer Science* 157, 1 (1996), 3–33.

[8] Xavier Caruso and Jérémy Le Borgne. 2017. Fast multiplication for skew polynomials. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. 77–84.

[9] Mark Giesbrecht. 1998. Factoring in skew-polynomial rings over finite fields. *Journal of Symbolic Computation* 26, 4 (1998), 463–486.

[10] Mark Giesbrecht, Qiao-Long Huang, and Éric Schost. 2020. Sparse multiplication for skew polynomials. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*. 194–201.

[11] Mark Giesbrecht, Qiao-Long Huang, and Éric Schost. 2021. Sparse multiplication of multivariate linear differential operators. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*. 155–162.

[12] Peter E Glotov. 1998. On the greatest common right divisor of Ore polynomials with polynomial coefficients which depend on a parameter. *Programming and Computer Software Journal* 24, 6 (1998), 275–283.

[13] Hoon Hong and Jing Yang. 2023. Computing greatest common divisor of several parametric univariate polynomials via generalized subresultant polynomials. arXiv:cs.SC/2401.00408

[14] Deepak Kapur, Dong Lu, Michael Monagan, Yao Sun, and Dingkang Wang. 2021. Algorithms for computing greatest common divisors of parametric multivariate polynomials. *Journal of Symbolic Computation* 102 (2021), 3–20.

[15] Deepak Kapur, Yao Sun, and Dingkang Wang. 2013. An efficient method for computing comprehensive Gröbner bases. *Journal of Symbolic Computation* 52 (2013), 124–142.

[16] Manuel Kauers, Maximilian Jaroschek, and Fredrik Johansson. 2015. Ore polynomials in Sage. In *Computer algebra and polynomials*. Springer, 105–125.

[17] Ziming Li. 1998. A subresultant theory for Ore polynomials with applications. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*. 132–139.

[18] Ziming Li and István Nemes. 1997. A modular algorithm for computing greatest common right divisors of Ore polynomials. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*. 282–289.

[19] Bhubaneswar Mishra. 1993. *Algorithmic algebra*. Springer.

[20] Antonio Montes. 2002. A new algorithm for discussing Gröbner bases with parameters. *Journal of Symbolic Computation* 33, 2 (2002), 183–208.

[21] Katsusuke Nabeshima. 2007. A speed-up of the algorithm for computing comprehensive Gröbner systems. In *Proceedings of the 2007 international symposium on Symbolic and Algebraic Computation*. 299–306.

[22] Kosaku Nagasaka. 2017. Parametric greatest common divisors using comprehensive Gröbner systems. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. 341–348.

[23] Øystein Ore. 1964. Theory of non-commutative polynomials. *Annals of Mathematics* 34, 3 (1964), 480–508.

[24] Marko Petkovšek and Manuel Bronstein. 1993. On Ore rings, linear operators and factorisation. *ETH, Eidgenössische Technische Hochschule Zürich, Departement Informatik, Institut für Wissenschaftliches Rechnen* 200 (1993).

[25] Raqeeb Rasheed. 2021. Resultant-based elimination for skew polynomials. In *2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*. IEEE, 11–18.

[26] Akira Suzuki and Yosuke Sato. 2006. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *Proceedings of the 2006 international symposium on Symbolic and Algebraic Computation*. 326–331.

[27] Dingkang Wang, Hesong Wang, and Fanghui Xiao. 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*. 442–449.

[28] Volker Weispfenning. 1992. Comprehensive Gröbner bases. *Journal of Symbolic Computation* 14, 1 (1992), 1–29.

[29] Manuela Wiesinger-Widi. 2011. Gröbner bases and generalized Sylvester matrices. *ACM Communications in Computer Algebra* 45, 1/2 (2011), 137–138.

[30] Yang Zhang. 2010. A secret sharing scheme via skew polynomials. In *2010 International Conference on Computational Science and Its Applications*. 33–38.