Subresultants of Several Ore Polynomials (Extended Abstract)

Jiaqi Meng[1,2] and Jing Yang[2][0000−0002−9032−1443]

[1] Wuzhou Vocational College, Wuzhou 543002, China
[2] SMS–HCIC–School of Mathematical Sciences,
Center for Applied Mathematics of Guangxi,
Guangxi Minzu University, Nanning 530006, China
yangjing0930@gmail.com

Abstract. In this paper, we extend the definition of subresultants for two Ore polynomials to several Ore polynomials. Using the generalized concept, we establish a connection between the generalized subresultants and the greatest common right divisor (GCRD) of several Ore polynomials. Based on this connection, we develop a method for computing the parametric GCRD of several Ore polynomials.

Keywords: Ore polynomial · parametric GCRD · subresultant.

1 Introduction

Subresultants are fundamental objects in polynomial algebra, with wide-ranging applications in polynomial system solving, greatest common divisor (GCD) computation [3,1], quantifier elimination, and beyond. The theory of subresultants for *two* commutative polynomials is now well-established, with significant contributions spanning from their origins [16] to modern treatments [3,1,6,5,12,17]. The subsequent development of the theory has proceeded along two main, increasingly challenging, directions: (i) extending the concept to *several* polynomials, and (ii) generalizing it to *non-commutative* polynomial rings.

The generalization of subresultants to several polynomials is a more recent endeavor. Early work by Kakié [11] established a connection between the Sylvester-type resultant matrix of several univariate polynomials and the degree of their greatest common divisor. Building on this foundation, Ho [6] presented a parallel algorithm for computing the GCD of several univariate polynomials with numeric coefficients. In recent work, Hong and Yang [9] have significantly advanced this direction. They introduced the concept of *generalized subresultants* for several polynomials and established the connection between the generalized subresultants and the GCD of a given set of polynomials.

The study of subresultants in non-commutative settings, particularly for Ore polynomials [15], presents distinct algebraic challenges. Chardin [2] pioneered this line of inquiry for two differential polynomials, presenting resultant formulas linked to their solutions. This was extended to the broader class of Ore polynomials by Li [13,14]. Hong [7,8] provided an alternative, solution-based formulation for two Ore polynomials, differing from Li's approach. Later, Jaroschek [10] adapted techniques for improving commutative subresultant bounds to the Ore case, deriving new bounds on coefficient sizes. More recently, Csajbók [4] investigated q-analogues of the principal coefficients of subresultants, applying the results to determine the rank of an $\mathbb{F}q$-linear transformation of $\mathbb{F}q^n$.

Motivated by the generalized subresultant framework for several *commutative* polynomials, this paper introduces a generalization to the non-commutative setting of Ore polynomials. Our main contributions are summarized as follows:

– We generalize the definition of subresultants from two to *several* Ore polynomials.

- Using this generalized framework, we establish a fundamental connection between the generalized subresultants and the greatest common right divisor (GCRD) of several Ore polynomials.
- Based on this connection, we develop a new method for computing the *parametric GCRD* for a set of several Ore polynomials.

This work therefore unifies the two aforementioned directions, extending a mature theory for commutative systems to a significantly more general algebraic context.

2 Preliminaries

In this section, we give a brief review of Ore polynomials and subresultants of two Ore polynomials. For this purpose, we first recall some notations and concepts in Ore algebra. Readers may refer to [15,13,14] for more details.

2.1 Review of Ore polynomials

We begin by making the following settings:

- $\mathcal{K}$ is a field;
- σ is an injective endomorphism from $\mathcal{K}$ to $\mathcal{K}$, called a conjugate operator;
- δ is an endomorphism of the additive group $(\mathcal{K}, +, 0)$, called a pseudo-derivation, such that
  - for all $a, b \in \mathcal{K}$, $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$,
  - for all $a \in \mathcal{K}$,
$$Xa = \sigma(a)X + \delta(a). \tag{1}$$

Definition 1. *The triple $(\mathcal{K}[X], \sigma, \delta)$ is called an Ore polynomial ring.*

Remark 1. The commutation rule (1) defines a non-commutative multiplication in $\mathcal{K}[X]$.

For the sake of simplicity, we use the shorthand notations $\mathcal{K}[X]$, σa and δa respectively for $(\mathcal{K}[X], \sigma, \delta)$, $\sigma(a)$ and $\delta(a)$ in the rest of the paper. Moreover, for $A \in \mathcal{K}[X]$, the leading coefficient of A in terms of X is abbreviated as $\mathrm{lc}(A)$.

Definition 2. *For $a \in \mathcal{K}$ and $k \in \mathbb{N}$, the k-th σ-factorial of a, written as $a^{[k]}$, is defined by*

$$a^{[k]} = \begin{cases} 1, & \text{if } k = 0 \\ \prod_{i=0}^{k-1} \sigma^i a, & \text{otherwise} \end{cases}$$

The following fact can be proved by induction.

Proposition 1. $\forall k \in \mathbb{N}$, $\mathrm{lc}\left(X^k A\right) = \sigma^k \mathrm{lc}(A)$.

2.2 Review of subresultants of two Ore polynomials

The subresultant of two Ore polynomials is often represented as a determinant polynomial of a certain matrix whose entries are the coefficients of the given polynomials [13,14]. Thus we recall the definition of determinant polynomial below.

Definition 3 (Determinant polynomial of matrix). *Let $M \in \mathcal{K}^{p \times q}$ where $p \leq q$ (that is, M is square or wide). The* determinant polynomial *of M, written as $\mathrm{dp}(M)$, is defined by*

$$\mathrm{dp}(M) = \sum_{0 \leq j \leq q-p} c_j X^j$$

where $c_j = \det[M_1 \ \cdots \ M_{p-1} \ M_{q-j}]$ and M_k stands for the k-th column of M.

Definition 4 (Coefficient matrix of a list of polynomials). *Let* $\mathcal{Q} = (Q_1, \ldots, Q_t)$ *where*

$$Q_i = \sum_{0 \le j \le q_i} b_{ij} X^j \in \mathcal{K}[X]$$

and $q_i = \deg Q_i$. *Let* $m = \max_{1 \le i \le t} q_i$. *Then the* coefficient matrix *of* $\mathcal{Q}$, *written as* $\mathrm{cm}(\mathcal{Q})$, *is defined as the* $t \times (m+1)$ *matrix whose* (i,j)*-th entry is the coefficient of* Q_i *in the term* X^{m+1-j}.

Definition 5 (Determinant polynomial of a list of polynomials). *Let* $\mathcal{Q} = (Q_1, \ldots, Q_t)$ *be such that* $\mathrm{cm}(\mathcal{Q})$ *is square or wide. Then we will use the following shorthand notation:*

$$\mathrm{dp}(\mathcal{Q}) = \mathrm{dp}(\mathrm{cm}(\mathcal{Q}))$$

which is called the determinant polynomial of $\mathcal{Q}$.

Definition 6. *Let* $F_0, F_1 \in \mathcal{K}[X]$ *with* $\deg(F_i) = d_i$ *and* $d_0 \le d_1$. *Let* $0 < k \le d_0$. *The* k-subresultant *of* F_0 *and* F_1, *written as* $R_k(F_0, F_1)$, *is defined by*

$$R_k(F_0, F_1) = \mathrm{dp}\left(X^{d_1-(d_0-k)-1}F_0, \ldots, X^0 F_0, X^{k-1}F_1, \ldots, X^0 F_1\right)$$

The principal leading coefficient of $R_k(F_0, F_1)$ *is defined as the coefficient of* $R_k(F_0, F_1)$ *in the term* X^{d_0-k}, *denoted by* $\overline{R_k(F_0, F_1)}$.

One can extend the above definition to the case when $k = 0$. In this case, it is required that $d_0 \ne d_1$. Then

$$R_0(F_0, F_1) = a_{0d_0}^{[d_1-d_0]} F_0$$

where a_{0d_0} is the leading coefficient of F_0.

The subresultant of two Ore polynomials can be applied to formulate their GCRD. For this purpose, we recall the following definitions.

Definition 7. *Let* $Q, D_1, D_2 \in \mathcal{K}[X]$. *If* $Q = D_1 D_2$, *then* D_2 *is called a* right divisor *of* Q, *denoted as* $D_2|_r Q$.

Definition 8 (GCRD). *A non-zero polynomial in* $\mathcal{K}[X]$ *is called a* greatest common right divisor *of* $Q_1, \ldots, Q_t$, *denoted as* $\mathrm{GCRD}(Q_1, \ldots, Q_t)$, *if it is a right divisor of all* $Q_1, \ldots, Q_t$ *with the highest degree.*

In [14, Proposition 6.1], Li discovered the relation between the GCRD of two Ore polynomials and their subresultants. We recall the result below.

Proposition 2. *Let* $k = \deg(\mathrm{GCRD}(F_0, F_1))$, *then* $R_{d_0-k}(F_0, F_1)$ *is the GCRD of* F_0 *and* F_1.

Let $\mathcal{R}(F_0, F_1) = (R_0, R_1, \ldots, R_{d_0})$. The last non-zero entry of the sequence $\mathcal{R}(F_0, F_1)$ is exactly $\mathrm{GCRD}(F_0, F_1)$. Therefore, we can compute the GCRD of two polynomials in the following manner.

Proposition 3. *Let* $j = \max_{\overline{R_k(F_0,F_1)} \ne 0} k$. *We have*

$$\mathrm{GCRD}(F_0, F_1) = R_j(F_0, F_1)$$

3 Main Result

In this section, we extend the concept of subresultant for two Ore polynomials to several Ore polynomials and establish the relationship between generalized subresultant and the GCRD of several Ore polynomials. This relationship can be viewed as a further extension of the generalized Sylvester's theorem developed in [9] for several commutative polynomials.

To present the main result, we need the following notations.

Notation 1 – $d = (d_0, \ldots, d_n) \in \mathbb{N}^{n+1}$ *where* $d_0 = \min d$;
– $\mathcal{F} = (F_0, \ldots, F_n)$ *where* $F_i = \sum_{j=0}^{d_i} a_{ij} X^j \in \mathcal{K}[X]$;
– $\mathcal{P}(d_0, n) = \{(\delta_1, \ldots, \delta_n) \in \mathbb{N}^n : |\delta| = \delta_1 + \cdots + \delta_n \leq d_0\}$.

Definition 9. *Let* $\mathcal{F}$ *be as in Notation 1 and* $\delta \in \mathcal{P}(d_0, n)$.

– *The* δ-subresultant matrix *of* $\mathcal{F}$, *written as* $\mathrm{Syl}_\delta(\mathcal{F})$, *is defined by*

$$\mathrm{Syl}_\delta(\mathcal{F}) = \mathrm{cm}\left(\mathcal{F}_{0\delta_0}, \mathcal{F}_{1\delta_1}, \ldots, \mathcal{F}_{n\delta_n}\right)$$

where $\mathcal{F}_{ij} = \left(X^{j-1}F_i, \ldots, X^0 F_i\right)$ *and*

$$\delta_0 = \begin{cases} c(\delta) - d_0 & \text{if } c(\delta) \geq d_0 \text{ and } d_0 \geq 1; \\ 1 & \text{else,} \end{cases}$$

with $c(\delta) = \#\,\mathrm{col}\,\mathrm{cm}\left(\mathcal{F}_{1\delta_1}, \ldots, \mathcal{F}_{n\delta_n}\right)$[1].
– *The* δ-subresultant *of* $\mathcal{F}$, *written as* $R_\delta(\mathcal{F})$, *is defined by*

$$R_\delta(\mathcal{F}) = \mathrm{dp}\left(\mathrm{Syl}_\delta(\mathcal{F})\right)$$

– *The* principal leading coefficient *of* $R_\delta(\mathcal{F})$ *is defined as the coefficient of* $R_\delta(\mathcal{F})$ *in the term* $X^{d_0 - |\delta|}$, *denoted by* $\overline{R_\delta(\mathcal{F})}$.

Remark 2. One can readily verify that $\delta_0 \geq 1$. Moreover, we have

$$\#\,\mathrm{col}\,\mathrm{Syl}_\delta(\mathcal{F}) = \delta_0 + d_0 \geq \delta_0 + |\delta| = \#\,\mathrm{row}\,\mathrm{Syl}_\delta(\mathcal{F})$$ [2]

Thus, the determinant polynomial $R_\delta(\mathcal{F})$ is well-defined for every $\mathcal{F}$ and δ in Notation 1.

Example 1. Let $d = (3, 4, 3)$. Then

$$\mathcal{P}(d_0, n) = \{(3,0), (2,1), (1,2), (0,3), (2,0), (1,1), (0,2), (1,0), (0,1), (0,0)\}$$

Choose $\delta = (1,1) \in \mathcal{P}(3,2)$. We have

$$\mathcal{F}_{11} = X^0 F_1, \quad \mathcal{F}_{21} = X^0 F_2$$

Thus

$$\mathrm{cm}\left(\mathcal{F}_1, \mathcal{F}_2\right) = \mathrm{cm}\left(X^0 F_1, X^0 F_2\right) = \begin{bmatrix} a_{14} & a_{13} & a_{12} & a_{11} & a_{10} \\ & a_{23} & a_{22} & a_{21} & a_{20} \end{bmatrix}$$

$$c(\delta) = \#\,\mathrm{col} \begin{bmatrix} a_{14} & a_{13} & a_{12} & a_{11} & a_{10} \\ & a_{23} & a_{22} & a_{21} & a_{20} \end{bmatrix} = 5$$

Hence

$$\delta_0 = 5 - 3 = 2$$

It follows that

$$R_{(1,1)}(\mathcal{F}) = \mathrm{dp} \begin{bmatrix} \sigma a_{03} & \delta a_{03} + \sigma a_{02} & \delta a_{02} + \sigma a_{01} & \delta a_{01} + \sigma a_{00} & \delta a_{00} \\ & a_{03} & a_{02} & a_{01} & a_{00} \\ a_{14} & a_{13} & a_{12} & a_{11} & a_{10} \\ & a_{23} & a_{22} & a_{21} & a_{20} \end{bmatrix}$$

$$= \det \begin{bmatrix} \sigma a_{03} & \delta a_{03} + \sigma a_{02} & \delta a_{02} + \sigma a_{01} & \delta a_{01} + \sigma a_{00} \\ & a_{03} & a_{02} & a_{01} \\ a_{14} & a_{13} & a_{12} & a_{11} \\ & a_{23} & a_{22} & a_{21} \end{bmatrix} X$$

[1] The notation $\#\,\mathrm{col}\,M$ is interpreted as the number of columns of the matrix M.
[2] The notation $\#\,\mathrm{row}\,M$ is interpreted as the number of rows of the matrix M.

$$+\det\begin{bmatrix} \sigma a_{03} & \delta a_{03}+\sigma a_{02} & \delta a_{02}+\sigma a_{01} & \delta a_{00} \\ & a_{03} & a_{02} & a_{00} \\ a_{14} & a_{13} & a_{12} & a_{10} \\ & a_{23} & a_{22} & a_{20} \end{bmatrix}$$

$$\overline{R_{(1,1)}(\mathcal{F})} = \det\begin{bmatrix} \sigma a_{03} & \delta a_{03}+\sigma a_{02} & \delta a_{02}+\sigma a_{01} & \delta a_{01}+\sigma a_{00} \\ & a_{03} & a_{02} & a_{01} \\ a_{14} & a_{13} & a_{12} & a_{11} \\ & a_{23} & a_{22} & a_{21} \end{bmatrix}$$

Remark 3. We show that Definition 9 specializes to Definition 6. Consider the case $n = 1$. Then Notation 1 reduces to

- $d = (d_0, d_1) \in \mathbb{N}^2$ with $d_0 \le d_1$;
- $\mathcal{F} = (F_0, F_1)$ with $F_i = \sum_{j=0}^{d_i} a_{ij} X^j \in \mathcal{K}[X]$;
- $\mathcal{P}(d_0, 1) = \{(\delta_1) : 0 \le \delta_1 \le d_0\}$.

For $\delta = (\delta_1) \in \mathcal{P}(d_0, 1)$ with $\delta_1 > 0$ (which implies $d_0 \ge 1$), we have $c(\delta) = d_1 + \delta_1 > d_0$, and hence

$$\delta_0 = c(\delta) - d_0 = d_1 + \delta_1 - d_0$$

Therefore,

$$\begin{aligned} R_{(\delta_1)}(\mathcal{F}) &= \mathrm{dp}\big(X^{\delta_0-1}F_0, \ldots, X^0F_0,\ X^{\delta_1-1}F_1, \ldots, X^0F_1\big) \\ &= \mathrm{dp}\Big(X^{d_1-(d_0-\delta_1)-1}F_0, \ldots, X^0F_0,\ X^{\delta_1-1}F_1, \ldots, X^0F_1\Big) \end{aligned}$$

which is precisely Definition 6 with $k = \delta_1$.

For the boundary case $\delta_1 = 0$, we have $\delta_0 = 1$, and thus

$$R_{(0)}(\mathcal{F}) = \mathrm{dp}(F_0) = F_0$$

which agrees with the extension of Definition 6 up to multiplication by a non-zero left scalar.

Hence, Definition 9 specializes to Definition 6 when $n = 1$.

As done in [9], we use the graded decreasing order to sort the members in $\mathcal{P}(d_0, n)$. More explicitly, for any two sequences $\delta, \gamma \in \mathcal{P}(d_0, n)$, we say that $\delta \succ_{\mathrm{glex}} \gamma$ if one of the following occurs:

1. $|\delta| > |\gamma|$, or
2. $|\delta| = |\gamma|$ and there exists $i \le n$ such that $(\delta_i > \gamma_i) \wedge \Big(\bigwedge_{1 \le j < i} (\delta_j = \gamma_j)\Big)$.

Now we are ready to present the main theoretical result of this paper.

Theorem 1 (Main). *Let $\mathcal{F}$ be as in Notation 1. Let*

$$\theta = \max_{\substack{\delta \in \mathcal{P}(d_0, n) \\ \overline{R_\delta(\mathcal{F})} \neq 0}} \delta$$

where max *is with respect to the order $\succ_{\mathrm{glex}}$. Then*

$$\mathrm{GCRD}(\mathcal{F}) = R_\theta(\mathcal{F})$$

Remark 4. We emphasize that in this paper we do *not* impose any monicity condition on the GCRD. Since a GCRD of Ore polynomials is unique only up to multiplication by a non-zero left scalar, all references to the GCRD in this paper should be interpreted modulo left associates. In particular, the equality in Theorem 1 means that the generalized subresultant $R_\theta(F)$ is a representative of the same left-associate class as the GCRD. This convention does not affect either the generalized subresultant construction or its applications, while avoiding the need for an additional normalization step.

Example 2. Let $\mathcal{F} = (F_0, F_1, F_2)$ and $D = \frac{d}{dt}$, where

$$\begin{aligned}
F_0 &= 2D^2 + (3t)D + t^2 + 2\\
F_1 &= 2D^3 + (3t+4)D^2 + (t^2+6t+4)D + 2t^2 + t + 4\\
F_2 &= D^3 + (2t+2)D^2 + (t^2+4t+3)D + 2t^2 + 2t + 2
\end{aligned}$$

Ordering the tuples in $\mathcal{P}(2,2)$ according to $\succ_{\text{glex}}$, we have

$$\mathcal{P}(2,2) = \{(2,0), (1,1), (0,2), (1,0), (0,1), (0,0)\}.$$

We compute $R_\delta(\mathcal{F})$ for each $\delta \in \mathcal{P}(2,2)$. We first compute $R_{(2,0)}(\mathcal{F})$. By Definition 9,

$$R_{(2,0)}(\mathcal{F}) = \text{dp}(D^2F_0, D^1F_0, D^0F_0, D^1F_1, D^0F_1)$$

To compute $R_{(2,0)}(\mathcal{F})$, we first expand D^2F_0, D^1F_0, D^0F_0, D^1F_1 and D^0F_1 as follows:

$$\begin{aligned}
D^2F_0 &= 2D^4 + 3tD^3 + (t^2+8)D^2 + 4tD + 2\\
D^1F_0 &= 2D^3 + 3tD^2 + (t^2+5)D + 2t\\
D^0F_0 &= 2D^2 + 3tD + t^2 + 2\\
D^1F_1 &= 2D^4 + (3t+4)D^3 + (t^2+6t+7)D^2 + (2t^2+3t+10)D + 4t + 1\\
D^0F_1 &= 2D^3 + (3t+4)D^2 + (t^2+6t+4)D + 2t^2 + t + 4
\end{aligned}$$

Then we have

$$\begin{aligned}
R_{(2,0)}(\mathcal{F}) &= \text{dp}\ (D^2F_0, D^1F_0, D^0F_0, D^1F_1, D^0F_1)\\
&= \text{dp}\begin{bmatrix}
2 & 3t & t^2+8 & 4t & 2\\
0 & 2 & 3t & t^2+5 & 2t\\
0 & & 2 & 3t & t^2+2\\
2 & 3t+4 & t^2+6t+7 & 2t^2+3t+10 & 4t+1\\
0 & 2 & 3t+4 & t^2+6t+4 & 2t^2+t+4
\end{bmatrix} = 0
\end{aligned}$$

Similarly,

$$\begin{aligned}
R_{(1,1)}(\mathcal{F}) &= \text{dp}(D^1F_0, D^0F_0, D^0F_1, D^0F_2)\\
&= \text{dp}\begin{bmatrix}
2 & 3t & t^2+5 & 2t\\
 & 2 & 3t & t^2+2\\
2 & 3t+4 & t^2+6t+4 & 2t^2+t+4\\
1 & 2t+2 & t^2+4t+3 & 2t^2+2t+2
\end{bmatrix} = 0\\
R_{(0,2)}(\mathcal{F}) &= \text{dp}(D^2F_0, D^1F_0, D^0F_0, D^1F_2, D^0F_2)\\
&= \text{dp}\begin{bmatrix}
2 & 3t & t^2+8 & 4t & 2\\
0 & 2 & 3t & t^2+5 & 2t\\
0 & & 2 & 3t & t^2+2\\
1 & 2t+2 & t^2+4t+5 & 2t^2+4t+6 & 4t+2\\
0 & 1 & 2t+2 & t^2+4t+3 & 2t^2+2t+2
\end{bmatrix} = 0\\
R_{(1,0)}(\mathcal{F}) &= \text{dp}(D^1F_0, D^0F_0, D^0F_1)\\
&= \text{dp}\begin{bmatrix}
2 & 3t & t^2+5 & 2t\\
 & 2 & 3t & t^2+2\\
2 & 3t+4 & t^2+6t+4 & 2t^2+t+4
\end{bmatrix} = -4(D+t)
\end{aligned}$$

Clearly, $\max\limits_{\substack{\delta\in\mathcal{P}(d_0,n)\\ R_\delta(\mathcal{F})\neq 0}} \delta = (1,0)$. By Theorem 1, we have

$$\text{GCRD}(\mathcal{F}) = R_{(1,0)}(\mathcal{F}) = -4(D+t)$$

In fact, Theorem 1 immediately yields the following procedure for computing the parametric GCRD of several Ore polynomials.

Given $\mathcal{F}$ with degree d as in Notation 1 and parametric coefficients, let $\mathcal{P}(d_0, n) = [\delta^1, \delta^2, \ldots, \delta^p]$ where the tuples are decreasing under $\succ_{\text{glex}}$. Theorem 1 yields the following procedure:

$$\operatorname{GCRD}(\mathcal{F}) = \begin{cases} R_{\delta^1}(\mathcal{F}) & \text{if} \quad \overline{R_{\delta^1}(\mathcal{F})} \neq 0; \\ R_{\delta^2}(\mathcal{F}) & \text{else if} \quad \overline{R_{\delta^2}(\mathcal{F})} \neq 0; \\ \quad\vdots & \quad\vdots \quad\quad \vdots \\ R_{\delta^p}(\mathcal{F}) & \text{else if} \quad \overline{R_{\delta^p}(\mathcal{F})} \neq 0. \end{cases}$$

Note $\delta^p = (0, \ldots, 0)$, in turn $R_{\delta^p}(\mathcal{F}) = F_0$ and $\overline{R_{\delta^p}(\mathcal{F})} = a_{0d_0}$, which is always non-zero. Hence the last condition $\overline{R_{\delta^p}(\mathcal{F})} \neq 0$ is vacuously true and thus can be omitted. Moreover, some conditions may be inconsistent, in which case the corresponding branches can be removed.

4 Proof Sketch of the Main Theorem

In this section, we provide an overview of the proof for Theorem 1.

Proof (Sketch). The proof proceeds in three steps. The key idea is to characterize the critical generalized subresultant by means of the incremental cofactor degree.

First, we introduce the notion of the incremental cofactor degree

$$\operatorname{icdeg}(\mathcal{F}) = (\deg C_1, \ldots, \deg C_n),$$

where each C_i satisfies

$$\operatorname{GCRD}(F_0, \ldots, F_{i-1}) = C_i \cdot \operatorname{GCRD}(F_0, \ldots, F_i)$$

More precisely, $\operatorname{icdeg}(\mathcal{F})$ records the degree decrease of the successive GCRDs obtained by incrementally adjoining the input Ore polynomials. This tuple determines the critical index at which the generalized subresultant matrix encodes the common right divisor of all the input polynomials.

Next, let

$$\theta = \operatorname{icdeg}(\mathcal{F}).$$

We then show that the row echelon form of $\operatorname{Syl}_\theta(\mathcal{F})$ consists of rows whose entries are the coefficients of $H_j \operatorname{GCRD}(\mathcal{F})$, where each H_j is an Ore polynomial of degree j. Consequently, the determinant polynomial of this row echelon matrix, namely $R_\theta(\mathcal{F})$, is similar to $\operatorname{GCRD}(\mathcal{F})$.

Finally, we prove that θ is precisely the largest element of $\mathcal{P}(d_0, n)$, with respect to the graded lexicographic order, whose principal leading coefficient is non-zero. Therefore, $R_\theta(\mathcal{F})$ is exactly the first generalized subresultant selected by the criterion in the theorem. Combining these two observations, we conclude that $R_\theta(\mathcal{F})$ is a representative of the same left-associate class as $\operatorname{GCRD}(\mathcal{F})$. Hence, $R_\theta(\mathcal{F})$ is a representative of the GCRD of $\mathcal{F}$, or equivalently, a GCRD of $\mathcal{F}$.

Acknowledgments. The authors' work was supported by National Natural Science Foundation of China (Grant No.: 12261010), Beijing Natural Science Foundation (Grant No.: 1262015) and Bagui Outstanding Young Talents Program.

References

1. Brown, W.S., Traub, J.F.: On Euclid's algorithm and the theory of subresultants. Journal of the ACM **18**(4), 505–514 (1971). https://doi.org/10.1145/321662.321665

2. Chardin, M.: Differential resultants and subresultants. In: Proceedings of Fundamentals of Computation Theory, Lecture Notes in Computer Science. pp. 180–189. Springer (1991). https://doi.org/10.1007/3-540-54458-5_62
3. Collins, G.E.: Subresultants and reduced polynomial remainder sequences. Journal of the ACM **14**(1), 128–142 (1967). https://doi.org/10.1145/321371.321381
4. Csajbók, B.: Scalar q-subresultants and Dickson matrices. Journal of Algebra **547**, 116–128 (2020). https://doi.org/10.1016/j.jalgebra.2019.10.056
5. Diaz-Toca, G.M., Gonzalez-Vega, L.: Various new expressions for subresultants and their applications. Applicable Algebra in Engineering, Communication and Computing **15**, 233–266 (2004). https://doi.org/10.1007/s00200-004-0158-4
6. Ho, C.J.: Topics in algebraic computing: Subresultants, GCD, factoring and primary ideal decomposition. Ph.D. thesis, New York University (1989), https://api.semanticscholar.org/CorpusID:124175774
7. Hong, H.: Ore principal subresultant coefficients in solutions. Applicable Algebra in Engineering, Communication and Computing **11**, 227–237 (2001), https://api.semanticscholar.org/CorpusID:25217916
8. Hong, H.: Ore subresultant coefficients in solutions. Applicable Algebra in Engineering, Communication and Computing **12**, 421–428 (2001), https://api.semanticscholar.org/CorpusID:23037149
9. Hong, H., Yang, J.: Computing the greatest common divisor of several parametric univariate polynomials via generalized subresultants. Journal of Symbolic Computation **137**, 102567 (2026). https://doi.org/10.1016/j.jsc.2026.102567
10. Jaroschek, M.: Improved polynomial remainder sequences for Ore polynomials. ACM Communications in Computer Algebra **46**(3/4), 100–101 (2013). https://doi.org/10.1016/j.jsc.2013.05.012
11. Kakié, K.: The resultant of several homogeneous polynomials in two indeterminates. Proceedings of the American Mathematical Society **54**, 1–7 (1976). https://doi.org/10.1090/S0002-9939-1976-0387256-5
12. Li, Y.: A new approach for constructing subresultants. Applied Mathematics and Computation **183**(1), 471–476 (2006). https://doi.org/10.1016/j.amc.2006.05.120
13. Li, Z.: A subresultant theory for linear differential, linear difference and Ore polynomials, with applications. Ph.D. thesis, Johannes Kepler University (1996)
14. Li, Z.: A subresultant theory for Ore polynomials with applications. In: Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (ISSAC '98). pp. 132–139. ACM (1998). https://doi.org/10.1145/281508.281594
15. Ore, O.: Theory of non-commutative polynomials. Annals of Mathematics **34**, 480–508 (1933). https://doi.org/10.2307/1968173
16. Sylvester, J.J.: On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraical common measure. Philosophical Transactions of the Royal Society of London (143), 407–548 (1853)
17. Terui, A.: Recursive polynomial remainder sequence and its subresultants. Journal of Algebra **320**(2), 633–659 (2008). https://doi.org/10.1016/j.jalgebra.2007.12.023