Subresultants in Recursive Polynomial Remainder Sequence*

Akira Terui

Institute of Mathematics
University of Tsukuba
Tsukuba, 305-8571 Japan
terui@math.tsukuba.ac.jp

Abstract. We introduce concepts of "recursive polynomial remainder sequence (PRS)" and "recursive subresultant," and investigate their properties. In calculating PRS, if there exists the GCD (greatest common divisor) of initial polynomials, we calculate "recursively" with new PRS for the GCD and its derivative, until a constant is derived. We call such a PRS a *recursive PRS*. We define *recursive subresultants* to be determinants representing the coefficients in recursive PRS by coefficients of initial polynomials. Finally, we discuss usage of recursive subresultants in approximate algebraic computation, which motivates the present work.

1 Introduction

The polynomial remainder sequence (PRS) is one of fundamental tools in computer algebra. Although the Euclidean algorithm (see Knuth ([1]) for example) for calculating PRS is simple, coefficient growth in PRS makes the Euclidean algorithm often very inefficient. To overcome this problem, the mechanism of coefficient growth has been extensively studied through the theory of subresultants; see Collins ([2]), Brown and Traub ([3]), Loos ([4]), etc. By the theory of subresultant, we can remove extraneous factors of the elements of PRS systematically.

In this paper, we consider a variation of the subresultant. When we calculate PRS for polynomials which have a nontrivial GCD, we usually stop the calculation with the GCD. However, it is sometimes useful to continue the calculation by calculating the PRS for the GCD and its derivative; this is necessary for calculating the number of real zeros including their multiplicities. We call such a PRS a "recursive PRS."

Although the theory of subresultants has been developed widely, the corresponding theory for recursive PRS is still unknown within the author's knowledge: this is the main problem which we investigate in this paper. By "recursive subresultants," we denote determinants which represent elements of recursive PRS by the coefficients of initial polynomials.

This paper is organized as follows. In Sect. 2, we introduce the concept of recursive PRS. In Sect. 3, we define recursive subresultant and show its relationship to recursive PRS. In Sect. 4, we discuss briefly using recursive subresultants in approximate algebraic computation.

2 Recursive Polynomial Remainder Sequence (PRS)

First, we review the PRS, then define the recursive PRS. At last, we show recursive Sturm sequence as an example of recursive PRS.

2.1 Definition of Recursive PRS

Let R be an integral domain and polynomials F and G be in $R[x]$. We define a polynomial remainder sequence as follows.

* This research was partially supported by Japanese Ministry of Education, Culture, Sports, Science and Technology under Grant-in-Aid for Young Scientists (B), 14780181, 2002.

Definition 1 (Polynomial Remainder Sequence (PRS)). *Let F and G be polynomials in $R[x]$ of degree m and n ($m > n$), respectively. A sequence*

$$(P_1, \dots, P_l) \tag{1}$$

of nonzero polynomials is called a polynomial remainder sequence (PRS) *for F and G, abbreviated to* $\mathrm{prs}(F, G)$*, if it satisfies*

$$P_1 = F, \quad P_2 = G, \quad \alpha_i P_{i-2} = q_{i-1} P_{i-1} + \beta_i P_i, \tag{2}$$

for $i = 3, \dots, l$, where $\alpha_3, \dots, \alpha_l$, $\beta_3, \dots, \beta_l$ are elements of R and $\deg(P_{i-1}) > \deg(P_i)$. A sequence $((\alpha_3, \beta_3), \dots, (\alpha_l, \beta_l))$ is called a division rule *for* $\mathrm{prs}(F, G)$ *(see von zur Gathen and Lücking* ([6])*). If P_l is a constant, then the PRS is called* complete. □

If F and G are coprime, the last element in the complete PRS for F and G is a constant. Otherwise, it equals the GCD of F and G up to a constant: we have $\mathrm{prs}(F, G) = (P_1 = F, P_2 = G, \dots, P_l = \gamma \cdot \gcd(F, G))$ for some $\gamma \in R$. Then, we can calculate new PRS, $\mathrm{prs}(P_l, \frac{d}{dx} P_l)$, and if this PRS ends with a non-constant polynomial, then calculate another PRS for the last element, and so on. By repeating this calculation, we can calculate several PRSs "recursively" such that the last polynomial in the last sequence is a constant. Thus, we define "recursive PRS" as follows.

Definition 2 (Recursive PRS). *Let F and G be the same as in Definition 1. Then, a sequence*

$$(P_1^{(1)}, \dots, P_{l_1}^{(1)}, P_1^{(2)}, \dots, P_{l_2}^{(2)}, \dots, P_1^{(t)}, \dots, P_{l_t}^{(t)}) \tag{3}$$

of nonzero polynomials is called a recursive polynomial remainder sequence *(recursive PRS) for F and G, abbreviated to* $\mathrm{rprs}(F, G)$*, if it satisfies*

$$\begin{aligned}
&P_1^{(1)} = F, \quad P_2^{(1)} = G, \quad P_{l_1}^{(1)} = \gamma_1 \cdot \gcd(P_1^{(1)}, P_2^{(1)}) \quad \textit{with } \gamma_1 \in R, \\
&(P_1^{(1)}, P_2^{(1)}, \dots, P_{l_1}^{(1)}) = \mathrm{prs}(P_1^{(1)}, P_2^{(1)}), \\
&P_1^{(k)} = P_{l_{k-1}}^{(k-1)}, \quad P_2^{(k)} = \frac{d}{dx} P_{l_{k-1}}^{(k-1)}, \quad P_{l_k}^{(k)} = \gamma_k \cdot \gcd(P_1^{(k)}, P_2^{(k)}) \quad \textit{with } \gamma_k \in R, \\
&(P_1^{(k)}, P_2^{(k)}, \dots, P_{l_k}^{(k)}) = \mathrm{prs}(P_1^{(k)}, P_2^{(k)}),
\end{aligned} \tag{4}$$

for $k = 2, \dots, t$. If $\alpha_i^{(k)}$, $\beta_i^{(k)} \in R$ satisfy

$$\alpha_i^{(k)} P_{i-2}^{(k)} = q_{i-1}^{(k)} P_{i-1}^{(k)} + \beta_i^{(k)} P_i^{(k)} \tag{5}$$

for $k = 1, \dots, t$ and $i = 3, \dots, l_k$, then a sequence $((\alpha_3^{(1)}, \beta_3^{(1)}), \dots, (\alpha_{l_t}^{(t)}, \beta_{l_t}^{(t)}))$ is called a division rule *for* $\mathrm{rprs}(F, G)$*. Furthermore, if $P_{l_t}^{(t)}$ is a constant, then the recursive PRS is called complete.* □

2.2 Example of Recursive PRS: Recursive Sturm Sequence

Sturm sequence is a variant of PRS, which is used in Sturm's method, for calculating the number of real zeros of univariate polynomial (for detail, see Cohen ([7]) for example). Note that Sturm's theorem is valid for not only polynomials having simple zeros but also those having multiple zeros (see Bochnak, Coste and Roy ([8]) for example). Here, we define "recursive Sturm sequence" to calculate the number of real zeros including multiplicities, as follows.

Definition 3 (Recursive Sturm Sequence). *Let $P(x)$ be a real polynomial of degree m. Let a sequence of nonzero polynomials be defined by a recursive PRS in Definition 2, calculated as*

$$\text{(complete) } \mathrm{rprs}(P(x), \frac{d}{dx} P(x)), \tag{6}$$

with division rule given by

$$(\alpha_i^{(k)}, \beta_i^{(k)}) = (1, -1), \tag{7}$$

for $k = 1, \dots, t$ and $i = 3, \dots, l_k$. Then, the sequence (6) *is called the* recursive Sturm sequence *of $P(x)$.* □

Example 1 (Recursive Sturm Sequence). Let $P(x) = (x+2)^2\{(x-3)(x+1)\}^3$, and calculate the recursive Sturm sequence of $P(x)$. The first sequence $L_1 = (P_1^{(1)}, \ldots, P_4^{(1)})$ has the following elements:

$$\begin{aligned}
P_1^{(1)} &= P(x) = (x+2)^2\{(x-3)(x+1)\}^3, \\
P_2^{(1)} &= \frac{d}{dx}P(x) = 8x^7 - 14x^6 - 102x^5 + 80x^4 + 460x^3 + 66x^2 - 558x - 324, \\
P_3^{(1)} &= \frac{75}{16}x^6 - \frac{45}{16}x^5 - 60x^4 - \frac{225}{8}x^3 + \frac{3315}{16}x^2 + \frac{4815}{16}x + \frac{945}{8}, \\
P_4^{(1)} &= \frac{128}{25}x^5 - \frac{256}{25}x^4 - \frac{256}{5}x^3 + \frac{1024}{25}x^2 + \frac{4224}{25}x + \frac{2304}{25}.
\end{aligned} \tag{8}$$

The second sequence $L_2 = (P_1^{(2)}, \ldots, P_4^{(2)})$ has the following elements:

$$\begin{aligned}
P_1^{(2)} &= P_4^{(1)} = \frac{128}{25}x^5 - \frac{256}{25}x^4 - \frac{256}{5}x^3 + \frac{1024}{25}x^2 + \frac{4224}{25}x + \frac{2304}{25}, \\
P_2^{(2)} &= \frac{d}{dx}P_4^{(1)} = \frac{128}{5}x^4 - \frac{1024}{25}x^3 - \frac{768}{5}x^2 + \frac{2048}{25}x + \frac{4224}{25}, \\
P_3^{(2)} &= \frac{14848}{625}x^3 - \frac{1536}{125}x^2 - \frac{88576}{625}x - \frac{66048}{625}, \\
P_4^{(2)} &= \frac{12800}{841}x^2 - \frac{25600}{841}x - \frac{38400}{841}.
\end{aligned} \tag{9}$$

The last sequence $L_3 = (P_1^{(3)}, \ldots, P_3^{(3)})$ has the following elements:

$$\begin{aligned}
P_1^{(3)} &= P_4^{(2)} = \frac{12800}{841}x^2 - \frac{25600}{841}x - \frac{38400}{841}, \\
P_2^{(3)} &= \frac{d}{dx}P_4^{(2)} = \frac{25600}{841}x - \frac{25600}{841}, \\
P_3^{(3)} &= \frac{51200}{841}.
\end{aligned} \tag{10}$$

For PRS L_k, $k = 1, 2, 3$, define sequences of nonzero real numbers $\lambda(L_k, -\infty)$ and $\lambda(L_k, +\infty)$ as

$$\begin{aligned}
\lambda(L_k, -\infty) &= ((-1)^{n_1^{(k)}}\operatorname{lc}(P_1^{(k)}), \ldots, (-1)^{n_{l_k}^{(k)}}\operatorname{lc}(P_{l_k}^{(k)})), \\
\lambda(L_k, +\infty) &= (\operatorname{lc}(P_1^{(k)}), \ldots, \operatorname{lc}(P_{l_k}^{(k)})),
\end{aligned} \tag{11}$$

where $n_i^{(k)} = \deg(P_i^{(k)})$ denotes the degree of $P_i^{(k)}$ and $\operatorname{lc}(P_i^{(k)})$ denotes the leading coefficients of $P_i^{(k)}$. Then, $\lambda(L_k, -\infty)$ and $\lambda(L_k, +\infty)$ for $k = 1, 2, 3$ are

$$\begin{aligned}
\lambda(L_1, \pm\infty) &= (1, \pm 8, \frac{75}{16}, \pm\frac{128}{25}), \\
\lambda(L_2, \pm\infty) &= (\pm\frac{128}{25}, \frac{128}{5}, \pm\frac{18848}{625}, \frac{12800}{841}), \\
\lambda(L_3, \pm\infty) &= (\frac{12800}{841}, \pm\frac{25600}{841}, \frac{51200}{841}).
\end{aligned} \tag{12}$$

For a sequence of nonzero real numbers $L = (a_1, \ldots, a_m)$, let $V(L)$ be the number of sign variations of the elements of L. Then, we calculate the number of the real zeros of $P(x)$, including multiplicity, as

$$\sum_{k=1}^{3}\{V(\lambda(L_k, -\infty)) - V(\lambda(L_k, +\infty))\} = 3 + 3 + 2 = 8. \tag{13}$$

□

3 Subresultants for Recursive PRS

Let F and G be polynomials in $R[x]$ such that

$$F(x) = f_m x^m + \cdots + f_0 x^0, \quad G(x) = g_n x^n + \cdots + g_0 x^0, \quad \text{with } m \geq n > 0. \tag{14}$$

To make this paper self-contained and to use notations for our definitions, we first review the fundamental theorem of subresultants, then discuss subresultants for recursive PRS.

3.1 Fundamental Theorem of Subresultants

There exist several different definitions of subresultants. Here, we follow definitions and notations basically by von zur Gathen and Lücking ([6]).

Definition 4 (Sylvester Matrix). *Let F and G be as in* (14). *The* Sylvester matrix *of F and G, denoted by* $\mathrm{Syl}(F,G)$, *is an $(m+n)\times(m+n)$ matrix constructed from the coefficients of F and G, such that*

$$\mathrm{Syl}(F,G) = \underbrace{\begin{pmatrix} f_m & & & g_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ f_0 & & f_m & g_0 & & g_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & f_0 & & & g_0 \end{pmatrix}}_{n \qquad\qquad m}. \tag{15}$$

□

Next, we define the "subresultant matrix" to derive polynomial subresultants.

Definition 5 (Subresultant Matrix). *Let F and G be defined as in* (14). *For $j < n$, the j-th* subresultant matrix *of F and G, denoted by $N^{(j)}(F,G)$, is an $(m+n-j)\times(m+n-2j)$ sub-matrix of* $\mathrm{Syl}(F,G)$ *obtained by taking the left $n-j$ columns of coefficients of F and the left $m-j$ columns of coefficients of G, such that*

$$N^{(j)}(F,G) = \underbrace{\begin{pmatrix} f_m & & & g_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ f_0 & & f_m & g_0 & & g_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & f_0 & & & g_0 \end{pmatrix}}_{n-j \qquad\qquad m-j}. \tag{16}$$

□

Definition 6 (Subresultant). *Let F and G be defined as in* (14). *For $j < n$ and $k = 0, \dots, j$, let $N_k^{(j)} = N_k^{(j)}(F,G)$ be a sub-matrix of $N^{(j)}(F,G)$ obtained by taking the top $m+n-2j-1$ rows and the $(m+n-j-k)$-th row (note that $N_k^{(j)}(F,G)$ is a square matrix). Then, the polynomial*

$$\mathrm{S}_j(F,G) = \det(N_j^{(j)})x^j + \cdots + \det(N_0^{(j)})x^0 \tag{17}$$

is called the j-th subresultant *of F and G.* □

Theorem 1 (Fundamental Theorem of Subresultants [3]). *Let F and G be defined as in (14), $(P_1,\ldots,P_k) = \mathrm{prs}(F,G)$ be complete PRS, and $((\alpha_3,\beta_3),\ldots,(\alpha_k,\beta_k))$ be its division rule. Let $n_i = \deg(P_i)$ and $c_i = \mathrm{lc}(P_i)$ for $i = 1,\ldots,k$, and $d_i = n_i - n_{i+1}$ for $i = 1,\ldots,k-1$. Then, we have*

$$\mathrm{S}_j(F,G) = 0 \quad \text{for } 0 \le j < n_k, \tag{18}$$

$$\mathrm{S}_{n_i}(F,G) = P_i c_i^{d_{i-1}-1} \prod_{l=3}^{i} \left\{ \left(\frac{\beta_l}{\alpha_l}\right)^{n_{l-1}-n_i} c_{l-1}^{d_{l-2}+d_{l-1}} (-1)^{(n_{l-2}-n_i)(n_{l-1}-n_i)} \right\}, \tag{19}$$

$$\mathrm{S}_j(F,G) = 0 \quad \text{for } n_i < j < n_{i-1}-1, \tag{20}$$

$$\mathrm{S}_{n_{i-1}-1}(F,G) = P_i c_{i-1}^{1-d_{i-1}} \prod_{l=3}^{i} \left\{ \left(\frac{\beta_l}{\alpha_l}\right)^{n_{l-1}-n_{i-1}+1} c_{l-1}^{d_{l-2}+d_{l-1}} (-1)^{(n_{l-2}-n_{i-1}+1)(n_{l-1}-n_{i-1}+1)} \right\}, \tag{21}$$

for $i = 3,\ldots,k$. □

By the above theorem, we can express coefficients of PRS by determinants of matrices whose elements are the coefficients of initial polynomials.

3.2 Recursive Subresultants

We construct "recursive subresultant matrix" whose determinants represent elements of recursive PRS by the coefficients of initial polynomials.

To make help for readers, we first show an example of recursive subresultant matrix for recursive Sturm sequence in Example 1.

Example 2 (Recursive Subresultant Matrix). We express $P(x)$ and $\frac{d}{dx}P(x)$ in Example 1 by

$$P(x) = f_8x^8 + \cdots + f_0x^0, \quad \frac{d}{dx}F(x) = g_7x^7 + \cdots + g_0x^0. \tag{22}$$

Let $M^{(1,5)}(F,G) = N^{(1,5)}(F,G)$, then the matrices $M_U^{(1,5)}(F,G)$, $M_L^{(1,5)}(F,G)$ and $M_L^{'(1,5)}(F,G)$ are given as

$$M^{(1,5)}(F,G) = \begin{pmatrix} M_U^{(1,5)} \\ \hline M_L^{(1,5)} \end{pmatrix} = \left(\begin{array}{ccccc} f_8 & & g_7 & & \\ f_7 & f_8 & g_6 & g_7 & \\ f_6 & f_7 & g_5 & g_6 & g_7 \\ f_5 & f_6 & g_4 & g_5 & g_6 \\ \hline f_4 & f_5 & g_3 & g_4 & g_5 \\ f_3 & f_4 & g_2 & g_3 & g_4 \\ f_2 & f_3 & g_1 & g_2 & g_3 \\ f_1 & f_2 & g_0 & g_1 & g_2 \\ f_0 & f_1 & & g_0 & g_1 \\ & f_0 & & & g_0 \end{array}\right), \quad M_L^{'(1,5)}(F,G) = \begin{pmatrix} 5f_4 & 5f_5 & 5g_3 & 5g_4 & 5g_5 \\ 4f_3 & 4f_4 & 4g_2 & 4g_3 & 4g_4 \\ 3f_2 & 3f_3 & 3g_1 & 3g_2 & 3g_3 \\ 2f_1 & 2f_2 & 2g_0 & 2g_1 & 2g_2 \\ f_0 & f_1 & & g_0 & g_1 \end{pmatrix}, \tag{23}$$

where horizontal lines in matrices divide them into the upper and the lower components. Note that the matrix $M^{'(1,5)}(F,G)$ is derived from $M_L^{(1,5)}(F,G)$ by multiplying the l-th row by $6-l$ for $l = 1,\ldots,5$ and deleting the lowest row. Similarly, the $(2,3)$-th recursive subresultant matrix $M^{(2,3)}(F,G)$ is constructed as

$$M^{(2,3)}(F,G) = \left(\begin{array}{c|c|c} M_U^{(1,5)} & & \\ \cline{1-1} & M_U^{(1,5)} & \\ \cline{2-2} & & M_U^{(1,5)} \\ \hline & & 0\cdots0 \\ \cline{3-3} M_L^{(1,5)} & M_L^{'(1,5)} & \\ & & M_L^{'(1,5)} \\ \cline{2-2} & 0\cdots0 & \end{array}\right). \tag{24}$$

□

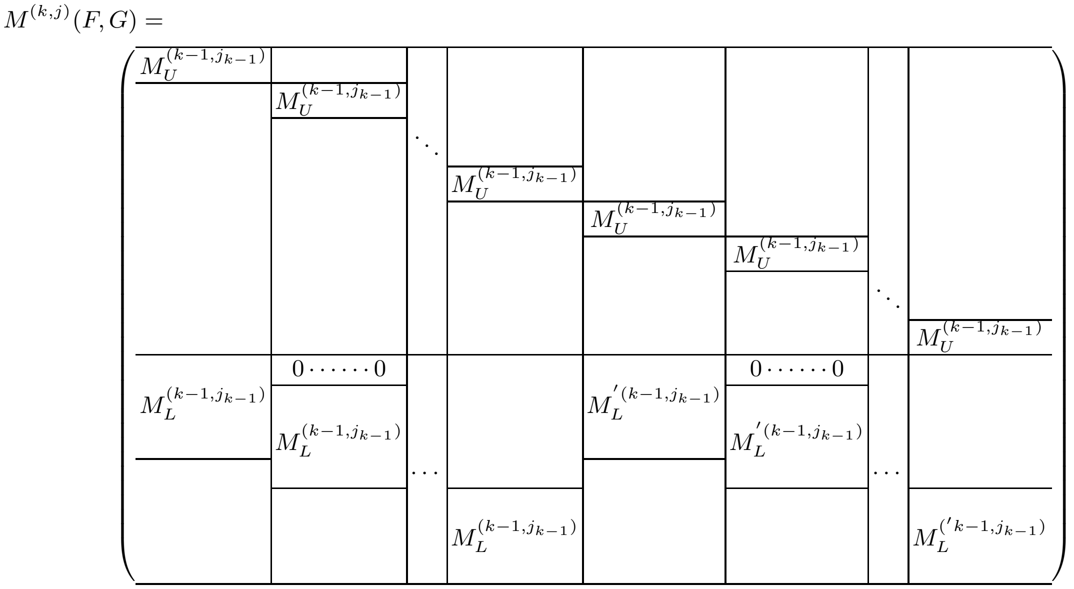

Fig. 1. Illustration of $M^{(k,j)}(F,G)$. Note that the number of blocks $M_L^{(k-1,j_{k-1})}$ is $j_{k-1}-j-1$, whereas that of $M_L^{'(k-1,j_{k-1})}$ is $j_{k-1}-j$; see Definition 7 for details.

Definition 7 (Recursive Subresultant Matrix). *Let F and G be defined as in* (14), *and let* $(P_1^{(1)},\ldots,P_{l_1}^{(1)},\ldots,P_1^{(t)},\ldots,P_{l_t}^{(t)})$ *be complete recursive PRS for F and G as in Definition 2. Let $j_0=m$ and $j_k=n_l^{(k)}$ for $k=1,\ldots,t$. Then, for each tuple of numbers (k,j) with $k=1,\ldots,t$ and $j=j_{k-1}-2,\ldots,0$, define matrix $M^{(k,j)}(F,G)$ as follows.*

1. *For $k=1$, let $M^{(1,j)}(F,G)=N^{(j)}(F,G)$.*
2. *For $k>1$, let $M^{(k,j)}(F,G)$ consist of the upper block and the lower block, defined as follows:*
   (a) *The upper block is partitioned into $(j_{k-1}-j_k-1)\times(j_{k-1}-j_k-1)$ blocks with diagonal blocks filled with $M_U^{(k-1,j_{k-1})}$, where $M_U^{(k-1,j_{k-1})}$ is a sub-matrix of $M^{(k-1,j_{k-1})}(F,G)$ obtained by deleting the bottom $j_{k-1}+1$ rows.*
   (b) *Let $M_L^{(k-1,j_{k-1})}$ be a sub-matrix of $M^{(k-1,j_{k-1})}(F,G)$ obtained by taking the bottom $j_{k-1}+1$ rows, and let $M_L^{'(k-1,j_{k-1})}$ be a sub-matrix of $M_L^{(k-1,j_{k-1})}$ by multiplying the $(j_{k-1}+1-\tau)$-th rows by τ for $\tau=j_{k-1},\ldots,1$, then by deleting the bottom row. Then, the lower block consists of $j_{k-1}-j-1$ blocks of $M_L^{(k-1,j_{k-1})}$ such that the leftmost block is placed at the top row of the container block and the right-side block is placed down by 1 row from the left-side block, then followed by $j_{k-1}-j$ blocks of $M_L^{'(k-1,j_{k-1})}$ placed by the same manner as $M_L^{(k-1,j_{k-1})}$.*

As a result, $M^{(k,j)}(F,G)$ becomes as shown in Fig. 1. Then, $M^{(k,j)}(F,G)$ is called the (k,j)-th recursive subresultant matrix *of F and G.* □

Proposition 1. *For $k=1,\ldots,t$ and $j<j_{k-1}-1$, the numbers of rows and columns of $M^{(k,j)}(F,G)$, the (k,j)-th recursive subresultant matrix of F and G are*

$$(m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\right\}(2j_{k-1}-2j-1)+j \tag{25}$$

and

$$(m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\right\}(2j_{k-1}-2j-1), \tag{26}$$

respectively.

Proof. By induction on k. For $k = 1$, by definition of the subresultant matrix, we see that $M^{(1,j)}(F,G)$ is a $(m+n-j) \times (m+n-2j)$ matrix. Let us assume that equations (25) and (26) are valid for $1,\dots,k-1$. Then, we calculate the numbers of the rows and columns of $M^{(k,j)}(F,G)$ as follows.

1. The numbers of rows of $M_L^{(k-1,j_{k-1})}$ and $M_L^{'(k-1,j_{k-1})}$ are equal to $j_{k-1}+1$ and j_{k-1}, respectively, hence the number of rows a block which consists of $M_L^{(k-1,j_{k-1})}$ and $M_L^{'(k-1,j_{k-1})}$ in $M^{(k,j)}(F,G)$ equals
$$2j_{k-1} - j - 1. \tag{27}$$
On the other hand, the number of rows of $M_U^{(k-1,j_{k-1})}$ is equal to $(m+n-2j_1)\{\prod_{l=2}^{k-1}(2j_{l-1} - 2j_l - 1)\} - 1$, hence the number of rows of diagonal blocks in $M^{(k,j_k)}(F,G)$ is equal to
$$(m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1} - 2j_l - 1) - 1\right\}(2j_{k-1} - 2j - 1). \tag{28}$$
By adding formulas (27) and (28), we obtain (25).
2. The number of columns of $M^{(k-1,j_{k-1})}(F,G)$ is equal to $(m+n-2j_1)\{\prod_{l=2}^{k-1}(2j_{l-1} - 2j_l - 1)\}$, hence the number of columns of $M^{(k,j)}(F,G)$ is equal to (26).

This proves the proposition. □

Now, we define recursive subresultants by recursive subresultant matrices.

Definition 8 (Recursive Subresultant). *Let F and G be defined as in* (14)*, and let $(P_1^{(1)},\dots,P_{l_1}^{(1)},\dots,P_1^{(t)},\dots,P_{l_t}^{(t)})$ be complete recursive PRS for F and G as in Definition 2. Let $j_0 = m$ and $j_k = n_l^{(k)}$ for $k = 1,\dots,t$. For $j = j_{k-1}-2,\dots,0$ and $\tau = j,\dots,0$, let $M_\tau^{(k,j)} = M_\tau^{(k,j)}(F,G)$ be a sub-matrix of the (k,j)-th recursive subresultant matrix $M^{(k,j)}(F,G)$ obtained by taking the top $(m+n-2j_1)\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\}(2j_{k-1}-2j-1)-1$ rows and the $((m+n-2j_1)\{\prod_{l=2}^{k-1}(2j_{l-1}-2j_l-1)\}(2j_{k-1}-2j-1)+j-\tau)$-th row (note that $M_\tau^{(k,j)}$ is a square matrix). Then, the polynomial*
$$\bar{\mathrm{S}}_{k,j}(F,G) = \det(M_j^{(k,j)})x^j + \cdots + \det(M_0^{(k,j)})x^0 \tag{29}$$
*is called the (k,j)-*th recursive subresultant *of F and G.* □

Finally, we derive the relation between recursive subresultants and coefficients in recursive PRS.

Lemma 1. *Let F and G be defined as in* (14)*, and let $(P_1^{(1)},\dots,P_{l_1}^{(1)},\dots,P_1^{(t)},\dots,P_{l_t}^{(t)})$ be complete recursive PRS for F and G as in Definition 2. Let $c_i^{(k)} = \mathrm{lc}(P_i^{(k)})$, $n_i^{(k)} = \deg(P_i^{(k)})$, $j_0 = m$ and $j_k = n_l^{(k)}$ for $k = 1,\dots,t$ and $i = 1,\dots,l_k$, and let $d_i^{(k)} = n_i^{(k)} - n_{i+1}^{(k)}$ for $k = 1,\dots,t$ and $i = 1,\dots,l_k - 1$. Furthermore, for $k = 1,\dots,t-1$ and $j = j_{k-1}-2,\dots,0$, define*
$$\begin{aligned} u_{k,j} &= (m+n-2j_1)\left\{\prod_{l=2}^{k-1}(2j_{l-1} - 2j_l - 1)\right\}(2j_{k-1} - 2j - 1),\\ B_k &= (c_{l_k}^{(k)})^{d_{l_k-1}^{(k)}-1}\prod_{l=3}^{l_k}\left\{\left(\frac{\beta_l^{(k)}}{\alpha_l^{(k)}}\right)^{n_{l-1}^{(k)}-n_{l_k}^{(k)}}(c_{l-1}^{(k)})^{(d_{l-2}^{(k)}+d_{l-1}^{(k)})}(-1)^{(n_{l-2}^{(k)}-n_{l_k}^{(k)})(n_{l-1}^{(k)}-n_{l_k}^{(k)})}\right\}, \end{aligned} \tag{30}$$
and let $u_k = u_{k,j_k}$. For $k = 2,\dots,t$ and $j = j_{k-1}-2,\dots,0$, define
$$b_{k,j} = 2j_{k-1} - 2j - 1, \quad r_{k,j} = (-1)^{(u_{k-1}-1)(1+2+\cdots+(b_{k,j}-1))}, \tag{31}$$
and let $b_k = b_{k,j_k}$ and $r_k = r_{k,j_k}$. Then, for the (k,j)-th recursive subresultant of F and G with $k = 1,\dots,t$ and $j = j_{k-1}-2,\dots,0$, we have
$$\bar{\mathrm{S}}_{k,j}(F,G) = R_{k,j}\cdot \mathrm{S}_j(P_1^{(k)}, P_2^{(k)}), \tag{32}$$
where $R_{1,j} = 1$ and $R_{k,j} = ((\cdots((B_1^{b_2}\cdot r_2B_2)^{b_3}\cdot r_3B_3)^{b_4}\cdots)^{b_{k-1}}\cdot r_{k-1}B_{k-1})^{b_{k,j}}\cdot r_{k,j}$ for $k > 1$.

Proof. For a univariate polynomial $P(x) = a_n x^n + \cdots + a_0 x^0$ with $a_j \in R$ for $j = 0, \ldots, n$, let us denote the coefficient vector for $P(x)$ by $\boldsymbol{p} = {}^t(a_n, \ldots, a_0)$.

We prove the lemma by induction on k. For $k = 1$, it follows immediately from the Fundamental Theorem of subresultants (Theorem 1). Let us assume that (32) is valid for $1, \ldots, k-1$. Then, we have

$$\bar{\mathrm{S}}_{k-1,j_{k-1}}(F,G) = R_{k-1,j_{k-1}} \cdot \mathrm{S}_{j_{k-1}}(P_1^{(k-1)}, P_2^{(k-1)}), \tag{33}$$

hence we have

$$\det(M_\tau^{(k-1,j_{k-1})}) = R_{k-1,j_{k-1}} \cdot \det(N_\tau^{(j_{k-1})}(P_1^{(k-1)}, P_2^{(k-1)})), \tag{34}$$

for $\tau = j_{k-1}, \ldots, 0$. Therefore, there exists a matrix W_{k-1} such that $\det(W_{k-1}) = R_{k-1,j_{k-1}}$ and that we can transform $M^{(k-1,j_{k-1})}(F,G)$ to

$$\tilde{M}^{(k-1,j_{k-1})}(F,G) = \left(\begin{array}{c|c} W_{k-1} & \boldsymbol{O} \\ \hline * & N^{(j_{k-1})}(P_1^{(k-1)}, P_2^{(k-1)}) \end{array}\right), \tag{35}$$

by eliminations on columns. Furthermore, by eliminations and exchanges on columns in the block $N^{(j_{k-1})}(P_1^{(k-1)}, P_2^{(k-1)})$ as shown in Brown and Traub ([3]), we can transform $\tilde{M}^{(k-1,j_{k-1})}(F,G)$ to

$$\bar{M}^{(k-1,j_{k-1})}(F,G) = \left(\begin{array}{c|c|c} W_{k-1} & \multicolumn{2}{c}{\boldsymbol{O}} \\ \hline & \bar{N}_U^{(j_{k-1})} & \\ \cline{2-2} * & & \boldsymbol{p}_1^{(k)} \end{array}\right), \tag{36}$$

such that $\bar{N}_U^{(j_{k-1})}$ is a lower triangular matrix with all diagonal elements equal to 1 and that $\det(\tilde{M}_\tau^{(k-1,j_{k-1})}(F,G)) = B_{k-1} \cdot \det(\bar{M}_\tau^{(k-1,j_{k-1})}(F,G))$, where $\tilde{M}_\tau^{(k-1,j_{k-1})}(F,G)$ and $\bar{M}_\tau^{(k-1,j_{k-1})}(F,G)$ are sub-matrices of $\tilde{M}^{(k-1,j_{k-1})}(F,G)$ and $\bar{M}^{(k-1,j_{k-1})}(F,G))$, respectively, obtained by the same manner as we have obtained $M_\tau^{(k-1,j_{k-1})}(F,G)$. Therefore, we have

$$\det(M_\tau^{(k-1,j_{k-1})}(F,G)) = B_{k-1} \cdot \det(\bar{M}_\tau^{(k-1,j_{k-1})}(F,G)). \tag{37}$$

Similarly, let $M'^{(k-1,j_{k-1})}(F,G) = \left(\frac{M_U^{(k-1,j_{k-1})}}{M_L'^{(k-1,j_{k-1})}}\right)$. Then, by the same transformations in the above, we can transform $M'^{(k-1,j_{k-1})}(F,G)$ to

$$\bar{M}'^{(k-1,j_{k-1})}(F,G) = \left(\begin{array}{c|c|c} W_{k-1} & \multicolumn{2}{c}{\boldsymbol{O}} \\ \hline & \bar{N}_U^{(j_{k-1})} & \\ \cline{2-2} * & & \boldsymbol{p}_2^{(k)} \end{array}\right), \tag{38}$$

satisfying

$$\det(M_\tau'^{(k-1,j_{k-1})}(F,G)) = B_{k-1} \cdot \det(\bar{M}_\tau'^{(k-1,j_{k-1})}(F,G)), \tag{39}$$

where $M_\tau'^{(k-1,j_{k-1})}(F,G)$ and $\bar{M}_\tau'^{(k-1,j_{k-1})}(F,G))$ are sub-matrices of $M'^{(k-1,j_{k-1})}(F,G)$ and $\bar{M}'^{(k-1,j_{k-1})}(F,G))$, respectively, obtained by taking the top $u_{k-1} - 1$ rows and the $(u_{k-1} + j_{k-1} - \tau)$-th row for $\tau = j_{k-1} \ldots, 1$. Therefore, for $j < j_{k-1} - 1$, we can transform $M^{(k,j)}(F,G)$ to $\bar{M}^{(k,j)}(F,G)$ as shown in Fig. 2 by eliminations and exchanges on columns in each column block, and let $\bar{M}_\tau^{(k,j)}(F,G)$ be sub-matrix of $\bar{M}^{(k,j)}(F,G)$ obtained by the same manner as we have obtained $M_\tau^{(k,j)}(F,G)$. Then, we have

$$\det(M_\tau^{(k,j)}(F,G)) = (B_{k-1})^{b_{k,j}} \cdot \det(\bar{M}_\tau^{(k,j)}(F,G)), \tag{40}$$

from (37) and (39) and since there exist $b_{k,j}$ blocks of $\bar{M}^{(k-1,j_{k-1})}(F,G)$ and $\bar{M}'^{(k-1,j_{k-1})}(F,G)$ in $\bar{M}^{(k,j)}(F,G)$ with each of which divided into the upper and the lower block.

Furthermore, by exchanges on columns, we can transform $\bar{M}^{(k,j)}(F,G)$ to $\hat{M}^{(k,j)}(F,G)$ as shown in Fig. 3, and let $\hat{M}_\tau^{(k,j)}(F,G)$ be sub-matrix of $\hat{M}^{(k,j)}(F,G)$ obtained by the same manner as we have obtained $M_\tau^{(k,j)}(F,G)$. Then, we have

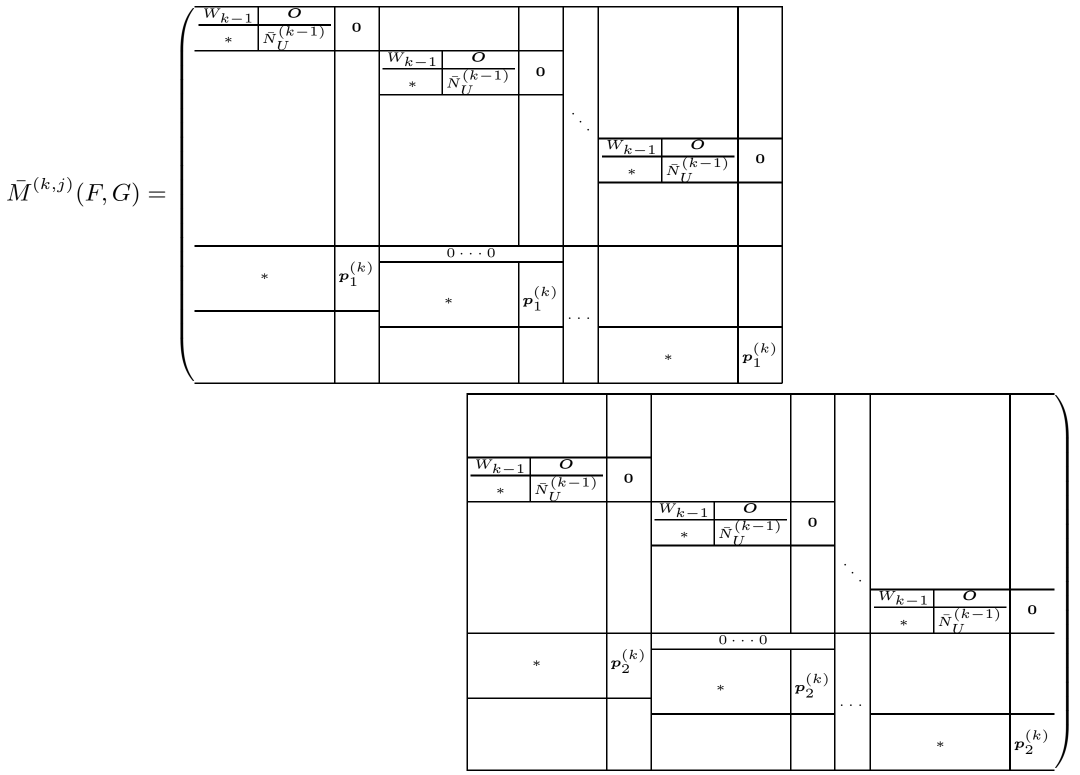

Fig. 2. Illustration of $\bar{M}^{(k,j)}(F,G)$. See Lemma 1 for details.

$$\det(\bar{M}_{\tau}^{(k,j)}(F,G)) = r_{k,j} \cdot \det(\hat{M}_{\tau}^{(k,j)}(F,G)), \tag{41}$$

because the $(u_{k,j} - (l-1)u_{k-1})$-th column in $\bar{M}^{(k,j)}(F,G)$ was moved to the $(u_{k,j} - (l-1))$-th column in $\hat{M}^{(k,j)}(F,G)$ for $l = 1, \ldots, b_{k,j}$. Furthermore, we have

$$\det(\hat{M}_{\tau}^{(k,j)}(F,G)) = (R_{k-1,j_{k-1}} B_{k-1})^{b_{k,j}} \cdot N_{\tau}^{(j)}(P_1^{(k)}, P_2^{(k)}), \tag{42}$$

because the lower-right block of $\boldsymbol{p}_1^{(k)}$ and $\boldsymbol{p}_2^{(k)}$ in $\hat{M}^{(k,j)}(F,G)$ is equal to $N^{(j)}(P_1^{(k)}, P_2^{(k)})$.

Finally, from (40), (41) and (42), we have

$$\begin{aligned} \det(M_{\tau}^{(k,j)}(F,G)) &= r_{k,j} \cdot (R_{k-1,j_{k-1}} B_{k-1})^{b_{k,j}} \cdot \det(N_{\tau}^{(j)}(P_1^{(k)}, P_2^{(k)})) \\ &= R_{k,j} \cdot \det(N_{\tau}^{(j)}(P_1^{(k)}, P_2^{(k)})). \end{aligned} \tag{43}$$

Therefore, by the definitions of recursive subresultant, we obtain (32). This proves the lemma. □

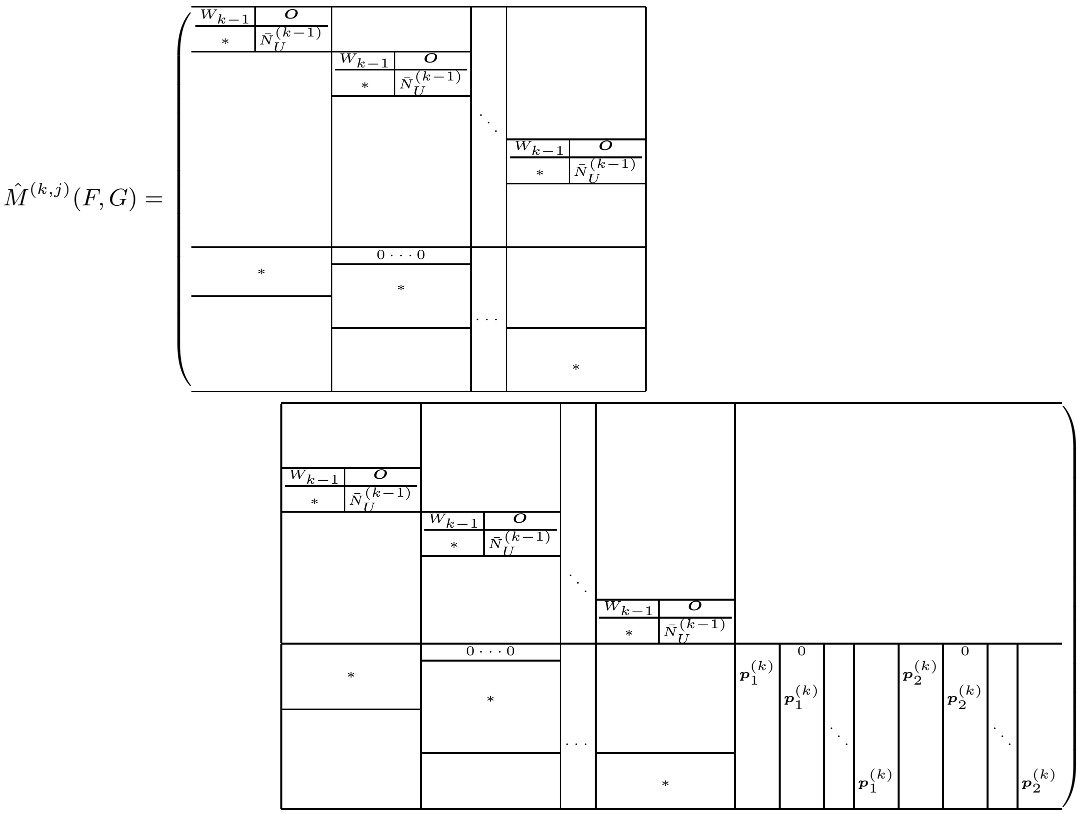

Fig. 3. Illustration of $\hat{M}^{(k,j)}(F,G)$. Note that the lower-right block which consists of $\boldsymbol{p}_1^{(k)}$ and $\boldsymbol{p}_2^{(k)}$ is equal to $N^{(j_k)}(P_1^{(k)}, P_2^{(k)})$, and the number of blocks W_{k-1} and $\bar{N}_U^{(k-1)}$ is $b_{k,j} = 2j_{k-1} - 2j - 1$: see Lemma 1 for details.

Theorem 2. *With the same conditions as in Lemma 1, and for $k = 1, \ldots, t$ and $i = 3, 4, \ldots, l_k$, we have*

$$\bar{\mathrm{S}}_{k,j}(F,G) = 0 \quad \text{for } 0 \le j < n_{l_k}^{(k)}, \tag{44}$$

$$\begin{aligned}\bar{\mathrm{S}}_{k,n_i^{(k)}}(F,G) &= P_i^{(k)} (c_i^{(k)})^{d_{i-1}^{(k)}-1} R_{k,n_i^{(k)}} \\ &\quad \times \prod_{l=3}^{i} \left\{ \left(\frac{\beta_l^{(k)}}{\alpha_l^{(k)}} \right)^{n_{l-1}^{(k)} - n_i^{(k)}} (c_{l-1}^{(k)})^{(d_{l-2}^{(k)} + d_{l-1}^{(k)})} (-1)^{(n_{l-2}^{(k)} - n_i^{(k)})(n_{l-1}^{(k)} - n_i^{(k)})} \right\},\end{aligned} \tag{45}$$

$$\bar{\mathrm{S}}_{k,j}(F,G) = 0 \quad \text{for } n_i^{(k)} < j < n_{i-1}^{(k)} - 1, \tag{46}$$

$$\begin{aligned}\bar{\mathrm{S}}_{k,n_{i-1}^{(k)}-1}(F,G) &= P_i^{(k)} (c_{i-1}^{(k)})^{1-d_{i-1}^{(k)}} R_{k,n_{i-1}^{(k)}-1} \\ &\quad \times \prod_{l=3}^{i} \left\{ \left(\frac{\beta_l^{(k)}}{\alpha_l^{(k)}} \right)^{n_{l-1}^{(k)} - n_{i-1}^{(k)} + 1} (c_{l-1}^{(k)})^{(d_{l-2}^{(k)} + d_{l-1}^{(k)})} (-1)^{(n_{l-2}^{(k)} - n_{i-1}^{(k)} + 1)(n_{l-1}^{(k)} - n_{i-1}^{(k)} + 1)} \right\}.\end{aligned} \tag{47}$$

Proof. By substituting $\mathrm{S}_j(P_1^{(k)}, P_2^{(k)})$ in (32) by (18)–(21), we obtain (44)–(47), respectively. □

We show an example of the proof of Lemma 1 for recursive subresultant matrix in Example 2.

Example 3. Let us express $P_i^{(k)}$ in Example 1 by

$$P_i^{(k)}(x) = a_{i,n_i^{(k)}}^{(k)} x^{n_i^{(k)}} + \cdots + a_{i,0}^{(k)} x^0, \tag{48}$$

with $n_i^{(k)} = \deg(P_i^{(k)})$. By eliminations and exchanges of columns as shown in Brown and Traub ([3]), we can transform $M^{(1,5)}(F,G) = \begin{pmatrix} M_U^{(1,5)} \\ \hline M_L^{(1,5)} \end{pmatrix}$ and $M'^{(1,5)}(F,G) = \begin{pmatrix} M_U^{(1,5)} \\ \hline M_L'^{(1,5)} \end{pmatrix}$ in (24) to $\bar{M}^{(1,5)}(F,G)$ and $\bar{M}'^{(1,5)}(F,G)$, respectively, as

$$
\bar{M}^{(1,5)}(F,G) = \left(\begin{array}{c|c} \bar{N}_U^{(5)} & \mathbf{0} \\ \hline * & \boldsymbol{p}_1^{(2)} \end{array}\right) = \left(\begin{array}{cccc|c}
1 & & & & \\
\bar{a}_{2,6}^{(1)} & 1 & & & \\
\bar{a}_{2,5}^{(1)} & \bar{a}_{2,6}^{(1)} & 1 & & \\
\bar{a}_{2,4}^{(1)} & \bar{a}_{2,5}^{(1)} & \bar{a}_{3,5}^{(1)} & 1 & \\
\hline
\bar{a}_{2,3}^{(1)} & \bar{a}_{2,4}^{(1)} & \bar{a}_{3,4}^{(1)} & \bar{a}_{3,5}^{(1)} & a_{4,5}^{(1)} \\
\bar{a}_{2,2}^{(1)} & \bar{a}_{2,3}^{(1)} & \bar{a}_{3,3}^{(1)} & \bar{a}_{3,4}^{(1)} & a_{4,4}^{(1)} \\
\bar{a}_{2,1}^{(1)} & \bar{a}_{2,2}^{(1)} & \bar{a}_{3,2}^{(1)} & \bar{a}_{3,3}^{(1)} & a_{4,3}^{(1)} \\
\bar{a}_{2,0}^{(1)} & \bar{a}_{2,1}^{(1)} & \bar{a}_{3,1}^{(1)} & \bar{a}_{3,2}^{(1)} & a_{4,2}^{(1)} \\
 & \bar{a}_{2,0}^{(1)} & \bar{a}_{3,0}^{(1)} & \bar{a}_{3,1}^{(1)} & a_{4,1}^{(1)} \\
 & & & \bar{a}_{3,0}^{(1)} & a_{4,0}^{(1)}
\end{array}\right), \tag{49}
$$

$$
\bar{M}'^{(1,5)}(F,G) = \left(\begin{array}{c|c} \bar{N}_U^{(5)} & \mathbf{0} \\ \hline * & \boldsymbol{p}_2^{(2)} \end{array}\right) = \left(\begin{array}{cccc|c}
1 & & & & \\
\bar{a}_{2,6}^{(1)} & 1 & & & \\
\bar{a}_{2,5}^{(1)} & \bar{a}_{2,6}^{(1)} & 1 & & \\
\bar{a}_{2,4}^{(1)} & \bar{a}_{2,5}^{(1)} & \bar{a}_{3,5}^{(1)} & 1 & \\
\hline
5\bar{a}_{2,3}^{(1)} & 5\bar{a}_{2,4}^{(1)} & 5\bar{a}_{3,4}^{(1)} & 5\bar{a}_{3,5}^{(1)} & 5a_{4,5}^{(1)} \\
4\bar{a}_{2,2}^{(1)} & 4\bar{a}_{2,3}^{(1)} & 4\bar{a}_{3,3}^{(1)} & 4\bar{a}_{3,4}^{(1)} & 4a_{4,4}^{(1)} \\
3\bar{a}_{2,1}^{(1)} & 3\bar{a}_{2,2}^{(1)} & 3\bar{a}_{3,2}^{(1)} & 3\bar{a}_{3,3}^{(1)} & 3a_{4,3}^{(1)} \\
2\bar{a}_{2,0}^{(1)} & 2\bar{a}_{2,1}^{(1)} & 2\bar{a}_{3,1}^{(1)} & 2\bar{a}_{3,2}^{(1)} & 2a_{4,2}^{(1)} \\
 & \bar{a}_{2,0}^{(1)} & \bar{a}_{3,0}^{(1)} & \bar{a}_{3,1}^{(1)} & a_{4,1}^{(1)}
\end{array}\right),
$$

where $\bar{a}_{i,j}^{(1)} = a_{i,j}^{(1)} / a_{2,7}^{(1)}$. Furthermore, we have

$$
\begin{aligned}
\det(M_\tau^{(1,5)}(F,G)) &= B_1 \cdot \det(\bar{M}_\tau^{(1,5)}(F,G)) \quad \text{for } \tau = 5, \ldots, 0, \\
\det(M_\tau'^{(1,5)}(F,G)) &= B_1 \cdot \det(\bar{M}_\tau'^{(1,5)}(F,G)) \quad \text{for } \tau = 5, \ldots, 1,
\end{aligned} \tag{50}
$$

with

$$
B_1 = -(a_{2,7}^{(1)})^2 (a_{3,6}^{(1)})^2, \tag{51}
$$

where $M_\tau^{(1,5)}(F,G)$ and $M_\tau'^{(1,5)}(F,G))$ are sub-matrices of $M^{(1,5)}(F,G)$ and $M'^{(1,5)}(F,G)$, respectively, obtained by taking the top 4 rows and the $(10-\tau)$-th row. Therefore, by eliminations and exchanges on columns, we can transform $M^{(2,3)}(F,G)$ in (24) to $\bar{M}^{(2,3)}(F,G)$ as

$$
\bar{M}^{(2,3)}(F,G) = \left(\begin{array}{cc|cc|cc}
\bar{N}_U^{(5)} & \mathbf{0} & & & & \\
 & & \bar{N}_U^{(5)} & \mathbf{0} & & \\
 & & & & \bar{N}_U^{(5)} & \mathbf{0} \\
\hline
 & & & & \multicolumn{2}{c}{0 \cdots 0} \\
* & \boldsymbol{p}_1^{(2)} & * & \boldsymbol{p}_2^{(2)} & * & \boldsymbol{p}_2^{(2)} \\
 & & \multicolumn{2}{c}{0 \cdots 0} & &
\end{array}\right), \tag{52}
$$

satisfying $\det(M_\tau^{(2,3)}(F,G)) = (B_1)^3 \cdot \det(\bar{M}_\tau^{(2,3)}(F,G))$. Furthermore, by exchanges on columns, we can transform $\bar{M}^{(2,3)}(F,G)$ to $\hat{M}^{(2,3)}(F,G)$ as

$$
\begin{aligned}
\hat{M}^{(2,3)}(F,G) &= \left(\begin{array}{cccccc}
\bar{N}_U^{(5)} & & & & & \\
 & \bar{N}_U^{(5)} & & & & \\
 & & \bar{N}_U^{(5)} & & & \\
\hline
 & & 0\cdots0 & & & 0 \\
* & * & * & \boldsymbol{p}_1^{(2)} & \boldsymbol{p}_2^{(2)} & \\
 & & & & & \boldsymbol{p}_2^{(2)} \\
 & 0\cdots0 & & & 0 &
\end{array}\right) \qquad (53) \\
&= \left(\begin{array}{cccc}
\bar{N}_U^{(5)} & & & \\
 & \bar{N}_U^{(5)} & & \\
 & & \bar{N}_U^{(5)} & \\
\hline
\multicolumn{3}{c}{*} & N^{(3)}(P_1^{(2)}, P_2^{(2)})
\end{array}\right),
\end{aligned}
$$

satisfying $\det(\bar{M}_\tau^{(2,3)}(F,G)) = r_{2,3} \cdot \det(\hat{M}_\tau^{(2,3)}(F,G)) = r_{2,3} \cdot \det(N_\tau^{(3)}(P_1^{(2)}, P_2^{(2)}))$. Therefore, we have

$$
\det(M_\tau^{(2,3)}(F,G)) = (B_1)^3 r_{2,3} \cdot \det(N_\tau^{(3)}(P_1^{(2)}, P_2^{(2)})) = R_{2,3} \cdot \det(N_\tau^{(3)}(P_1^{(2)}, P_2^{(2)})), \qquad (54)
$$

for $\tau = 3, \dots, 0$, and we have

$$
\bar{\mathrm{S}}_{2,3}(F,G) = R_{2,3} \cdot \mathrm{S}_3(P_1^{(2)}, P_2^{(2)}) = \{(a_{2,7}^{(1)})^2 (a_{3,6}^{(1)})^2\}^3 (a_{2,4}^{(2)})^2 \cdot P_3^{(2)}. \qquad (55)
$$

□

4 Conclusion and Motivation

In this paper, we have defined recursive PRS as well as recursive subresultants, and proved a similar theorem as the fundamental theorem of subresultant.

The concept of recursive subresultant is inspired, in approximate algebraic computation, by representing coefficients in recursive PRS by the coefficients of initial polynomials. For example, consider calculating recursive Sturm sequence of a polynomial with floating-point number coefficients by floating-point arithmetic. In the case the initial polynomial has multiple or close zeros, there may exist a polynomial in the sequence such that it is difficult to decide whether the polynomial becomes zero or not. Also, zero recognition of very small leading coefficient is another important problem because it plays crucial role in calculating the number of real zeros.

For the problem of zero recognition of very small leading coefficients, the present author and Sasaki ([5]) have proposed a criterion for calculating the number of real zeros correctly by Sturm's method: if the Sturm sequence satisfy certain condition on Sylvester matrix, then we can neglect the small leading coefficient which makes computation of the Sturm sequence more stable. We expect that the recursive subresultant (matrix) will be useful for zero recognition of a polynomial in recursive Sturm sequence, by representing its coefficients by the coefficients of initial polynomials then analyzing it by numerical methods; this is the problem on which we are working now.

Acknowledgments

The author thank Prof. Tateaki Sasaki very much for revising the original manuscript, and the referees for their helpful suggestions.

References

1. Knuth, D.: The Art of Computer Programming. Third edn. Volume 2: Seminumerical Algorithms. Addison-Wesley (1998)

2. Collins, G.E.: Subresultants and Reduced Polynomial Remainder Sequences. J. ACM **14** (1967) 128–142
3. Brown, W.S., Traub, J.F.: On Euclid's Algorithm and the Theory of Subresultants. J. ACM **18** (1971) 505–514
4. Loos, R.: Generalized polynomial remainder sequences. In Buchberger, B., Collins, G.E., Loos, R., eds.: Computer Algebra: Symbolic and Algebraic Computation. Second edn. Springer-Verlag (1983) 115–137
5. Terui, A., Sasaki, T.: "Approximate zero-points" of Real univariate polynomial with large error terms. IPSJ J. **41** (2000) 974–989
6. von zur Gathen, J., Lücking, T.: Subresultants revisited (extended abstract). In Gonnet, G.H., Panario, D., Viola, A., eds.: LATIN 2000: Theoretical Informatics. Volume 1776 of Lecture Notes in Computer Science. Springer (2000) 318–342
7. Cohen, H.: A Course in Computational Algebraic Number Theory. Volume 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin (1993)
8. Bochnak, J., Coste, M., Roy, M.F.: Real Algebraic Geometry. Volume 36 of A Series of Modern Surveys in Mathematics. Springer-Verlag, Berlin Heidelberg (1998)