記 号 処 理 20－4
（1982. 10. 18）

BY-PRS AND AN EXTENSION OF SUBRESULTANT THEORY

佐々木建昭，古川昭夫
（理研）　（都立大・数学）

This paper extends the polynomial remainder sequence and introduces a concept of by-PRS, or by-polynomial remainder sequence. Being given a polynomial H and the PRS $(P_1,P_2,\ldots,P_k)$, a by-PRS $(\tilde{P}_1,\tilde{P}_2,\ldots,\tilde{P}_k)$ is generated through the following formula: $\tilde{P}_1=H$, $\tilde{\beta}_i\tilde{P}_i=\tilde{\alpha}_i\tilde{P}_{i-1}-\tilde{Q}_iP_i$, $\deg(\tilde{P}_i)<\deg(P_i)$, $i=2,3,\ldots,k$ if $\deg(P_k)>0$, $i=2,3,\ldots,k-1$ if $\deg(P_k)=0$, where $\tilde{\alpha}_i,\tilde{\beta}_i \in I$, with I the coefficient domain of the PRS and H. The by-PRS can be used in many algebraic calculations, for example, in solving coupled Diophantine equations of polynomial coefficients. It is shown that the subresultant theory on PRS can be extended to include by-PRS, and two algorithms for by-PRS calculation are presented. The algorithms are analogous to the subresultant PRS algorithm.

§1. Introduction

The PRS is an abbreviation of polynomial remainder sequence, and it plays an important role in algebra, for example, for calculating polynomial greatest common divisors or as a Sturm sequence.

Let F(x) and G(x) be polynomials of degree ℓ and m, respectively, with coefficients in an integral domain I:

$$F(x) = f_\ell x^\ell + f_{\ell-1}x^{\ell-1} + \ldots + f_0, \quad f_i \in I, \tag{1.1}$$

$$G(x) = g_m x^m + g_{m-1}x^{m-1} + \ldots + g_0, \quad g_i \in I. \tag{1.2}$$

Assuming $\ell \geq m$ and putting $P_1=F$ and $P_2=G$, we can generate a PRS, $(P_1, P_2, \ldots, P_k \neq 0, P_{k+1}=0)$, by succesively calculating remainders through the following formula:

$$\beta_i P_{i+1} = \alpha_i P_{i-1} - Q_i P_i, \ \deg(P_{i+1})<\deg(P_i), \ i=2,3,\ldots,k, \tag{1.3}$$

where $\alpha_i, \beta_i \in I$. The choice $\alpha_i=1$, which is the case that (1.3) is the conventional polynomial division, does not guarantee that $P_i(x) \in I[x]$. In computer algebra, it is rather common to choose

$$\alpha_i = \{\mathrm{lc}(P_i)\}^{\deg(P_{i-1})-\deg(P_i)+1}, \tag{1.4}$$

where $\mathrm{lc}(P_i)$ is the leading coefficient of P_i. That is, we perform the pseudo-division instead of the division. Then, the pseudo-remainder (which we abbreviate by prem) is in I[x]. For example,

$$\mathrm{prem}(F,G) = \begin{vmatrix} g_m & g_{m-1} & \cdots & g_{2m-\ell} & x^{\ell-m}G \\ & g_m & g_{m-1} & \cdots & g_{2m-\ell+1} & x^{\ell-m-1}G \\ & & \cdots & \cdots & \cdots & \cdots \\ & & & g_m & & x^0 G \\ f_\ell & f_{\ell-1} & \cdots & \cdots & f_m & x^0 F \end{vmatrix} \tag{1.5}$$

Here, g_i is defined to be zero for negative i.

Calculation of PRS can be regarded as a succesive reduction of a set of two polynomials (P_1,P_2) to (P_i,P_{i+1}), i=2,3,...,k, by eliminating highest degree terms. In addition to the reduction of two polynomials, we are often necessary to reduce a set of many polynomials $(P_0^{(1)}, P_0^{(2)}, \ldots, P_0^{(n)})$ to another set $(P_i^{(1)}, P_i^{(2)}, \ldots, P_i^{(n)})$ by succesively eliminating highest degree terms. Such a case happens, for example, in solving coupled Diophantine equations of polynomial coefficients.

The necessity of reducing a set of many polynomials leads us to a concept of by-PRS, or by-polynomial remainder sequence. For simplicity, let us consider the case of three polynomials F(x), G(x) and H(x), with F and G given by (1.1) and (1.2), respectively, and H given by

$$H(x) = h_{\tilde{\ell}}x^{\tilde{\ell}} + h_{\tilde{\ell}-1}x^{\tilde{\ell}-1} + \ldots + h_0, \quad h_i \in I. \tag{1.6}$$

A by-PRS is a polynomial remainder sequence generated by H and the PRS $(P_1,P_2,\ldots,P_k)$ through the following formula:

$$\begin{aligned} &\tilde{P}_1 = H, \\ &\tilde{\beta}_i\tilde{P}_i = \tilde{\alpha}_i\tilde{P}_{i-1} - \tilde{Q}_iP_i, \quad \deg(\tilde{P}_i) < \deg(P_i), \\ &\qquad i=2,3,\ldots,k \text{ if } \deg(P_k)>0, \quad i=2,3,\ldots,k-1 \text{ if } \deg(P_k)=0, \end{aligned} \tag{1.7}$$

where $\tilde{\alpha}_i,\tilde{\beta}_i \in I$. When $\deg(P_k)=0$, we define $\tilde{P}_k=0$. Note that, without the sequence $(P_1,P_2,\ldots,P_k)$, we cannot calculate the by-PRS $(\tilde{P}_1,\tilde{P}_2,\ldots,\tilde{P}_k)$. In this sense, we may call the sequence $(P_1,P_2,\ldots,P_k)$ main-PRS.

From the above definition of by-PRS, it is clear that the reduction of a set of more than three polynomials $(F, G, H^{(1)}, H^{(2)}, \ldots, H^{(n)})$ through the formula (1.7) can be done by calculating by-PRS for each triple of the set $\{(F,G,H^{(1)}), (F,G,H^{(2)}), \ldots, (F,G,H^{(n)})\}$. Hence, this paper discusses only the case of three polynomials (F,G,H).

So far, we have not mentioned about the choice of β_i. The efficiency of PRS calculation depends very much on the choice of β_i [1,5]. For example, the choice $\beta_i=1$ makes the calculation of PRS extremely expensive because of a phenomenon of coefficient growth[5]. Different choices of $\beta_i \in I$ in (1.3) give different PRS's the coefficients of which are not always in I but may be in the quotient field of I. From the viewpoint of computer algebra, calculations are easier over I than over the quotient field of I. Hence, an important problem in computer algebra is to search for a suitable choice of β_i which makes the calculation of PRS reasonably efficient and makes the PRS be in I[x]. In 1966, Collins[2] analyzed the PRS generated through (1.3) and found an important choice of β_i. The choice is called the reduced PRS algorithm. Collins' work was deepened by himself[3] and by Brown and Traub[4], and the so-called subresultant PRS algorithm was found. These algorithms are based on the subresultant theory which we briefly survey in §2.

In this paper, we extend the subresultant theory so as to include by-PRS. The extension leads us to two algorithms for by-PRS calculation. The algorithms calculate by-PRS so that any polynomial in the by-PRS is equal to an extended subresultant and they are quite similar to the reduced-PRS algorithm.

§2. Survey of the subresultant theory on PRS

The leading coefficients of P_i and $\tilde{P}_i$ are denoted as c_i and $\tilde{c}_i$, respectively.

The degrees of P_i and $\tilde{P}_i$ are denoted as n_i and $\tilde{n}_i$, respectively.

The d_i denotes the following degree difference:

$$d_i = n_i - n_{i+1}. \tag{2.3}$$

(For other notations, see 'Extended Euclidian Algorithm and Determinants' [T.Sasaki: Kigoushori kenkyukai Shiryou 19 : 1982/5/20: Johou Shori Gakkai])

§3. An extension of the subresultant theory

We assume that $\deg(F) \geqq \deg(G), \deg(H)$, or $\ell \geqq m, \tilde{\ell}$. We define an extended subresultant $\tilde{S}_{j-1}(F,G,H)$ by the following determinant of order $\ell+m-2j+1$:

$$\tilde{S}_{j-1}(F,G,H) = \begin{vmatrix} f_\ell & f_{\ell-1} & \cdots & f_{2j+1-m} & x^{m-j-1}F \\ & f_\ell & f_{\ell-1} & \cdots & f_{2j+2-m} & x^{m-j-2}F \\ & & \cdots & & \cdots & \\ & & f_\ell & \cdots & f_j & x^0F \\ g_m & g_{m-1} & \cdots & & g_{2j+1-\ell} & x^{\ell-j-1}G \\ & g_m & g_{m-1} & \cdots & g_{2j+2-\ell} & x^{\ell-j-2}G \\ & & \cdots & & \cdots & \\ & & & g_m \cdots g_j & & x^0G \\ & & & h_{\tilde{\ell}} \cdots h_j & & x^0H \end{vmatrix} \begin{matrix} \\ \\ \\ \} m-j \text{ rows} \\ \\ \\ \} \\ \} \ell-j \text{ rows} \\ \\ \\ \\ \end{matrix}, \tag{3.1}$$

where $f_i = g_i = 0$ for $i<0$. Note that $\tilde{S}_{j-1}$ is a polynomial of degree $j-1$ or less, and $\tilde{S}_{j-1}$ can be defined only when $0<j\leqq m$. Note further that the above definition is meaningless when $j=m$ and $\tilde{\ell}=\ell$ because we cannot form the determinant. In the case of $j=m$ and $\tilde{\ell}=\ell$, we define $\tilde{S}_{m-1}(F,G,H)$ as follows:

$$\tilde{S}_{m-1} \ (\tilde{\ell}=\ell) = \begin{vmatrix} g_m & g_{m-1} & \cdots & g_{2m-\ell} & x^{\ell-m}G \\ & g_m & g_{m-1} & \cdots & g_{2m+1-\ell} & x^{\ell-m-1}G \\ & & \cdots & & \cdots & \\ & & & g_m & & x^0G \\ h_\ell & h_{\ell-1} & \cdots & h_m & & x^0H \end{vmatrix} \begin{matrix} \\ \\ \\ \} \ell-m+1 \text{ rows} \\ \\ \end{matrix}. \tag{3.1'}$$

The exceptional case of $j=m$ and $\tilde{\ell}=\ell$ is not important in the bellow because we are mainly interested in the case of $j<m$.

Let us consider the case of $\ell \geqq \tilde{\ell} \geqq m$ first.

Lemma 1. Let $\ell \geqq \tilde{\ell} \geqq m$, $F = QG + F'$ with $\deg(F')=n<m$, and $H = \tilde{Q}G + H'$ with $\deg(H')=\tilde{n}<m$:

$$\begin{aligned} F'(x) &= f'_n x^n + f'_{n-1}x^{n-1} + \cdots + f'_0, \\ H'(x) &= h'_{\tilde{n}}x^{\tilde{n}} + h'_{\tilde{n}-1}x^{\tilde{n}-1} + \cdots + h'_0. \end{aligned} \tag{3.2}$$

Then, for such j that $0<j<m$, we have the following equalities:

when $0<j<n$

$$\tilde{S}_{j-1}(F,G,H) = (-1)^{(\ell-j)(m-j)} g_m^{(\ell-n)} \tilde{S}_{j-1}(G,F',H'), \tag{3.3}$$

when $j=n\leqq\tilde{n}$

$$\tilde{S}_{n-1}(F,G,H) = (-1)^{(\ell-n)(m-n)} g_m^{(\ell-n)} f_n'^{(m-\tilde{n}-1)} \mathrm{prem}(H',F'), \tag{3.4}$$

when $j=n>\tilde{n}$

$$\tilde{S}_{n-1}(F,G,H) = (-1)^{(\ell-n)(m-n)} g_m^{(\ell-n)} f'^{(m-n)}_n H', \tag{3.5}$$

when ($j=n+1$ or $j=m-1$) and $n<\tilde{n}=m-1$

$$\tilde{S}_{j-1}(F,G,H) = (-1)^{(\ell-j+1)(m-j)} g_m^{(\ell-j)} f'^{(m-j-1)}_n h'_{m-1} F', \tag{3.6}$$

and in other cases, that is,

when $j=n+1$ and $\tilde{n}<m-1$ or when $n+1<j<m-1$ or when $j=m-1>n,\tilde{n}$

$$\tilde{S}_{j-1}(F,G,H) = 0. \tag{3.7}$$

(Proof) [shouryaku]

Let us next investigate the case of $\ell \geqq m > \tilde{\ell}$. In this case, only the replacement of upper m-j rows of (3.1) leads us to the determinant of the form (3.8). Hence, we obtain the following lemma:

Lemma 2. Let $\ell \geqq m > \tilde{\ell}$ and $F = QG + F'$ with $\deg(F')=n<m$. Then, for such j that $0<j<m$, we have the same equalities as (3.3)~(3.7) except that H', $\tilde{n}$, h'_{m-1} in (3.3)~(3.7) are replaced by H, $\tilde{\ell}$, h_{m-1}, respectively.//

This lemma is rather obvious since $H=H'$ for $\ell \geqq m > \tilde{\ell}$. Before going further, let us briefly investigate the case of $j=m$. When $j=m$, (3.1) contains no rows concerning F hence we can readily reduce (3.1) to yield the following lemma:

Lemma 3. The extended subresultant of degree m-1, $\tilde{S}_{m-1}(F,G,H)$, satisfies the following equalities:

when $\tilde{\ell}=\ell$

$$\tilde{S}_{m-1}(F,G,H) = S_{m-1}(G,H) = \mathrm{prem}(H,G), \tag{3.9}$$

when $\ell > \tilde{\ell} \geqq m$

$$\tilde{S}_{m-1}(F,G,H) = g_m^{(\ell-\tilde{\ell}-1)} \mathrm{prem}(H,G), \tag{3.10}$$

and when $m \geqq \tilde{\ell}+1$

$$\tilde{S}_{m-1}(F,G,H) = g_m^{(\ell-m)} H.// \tag{3.11}$$

In the below, we consider the case of $j<m$ mostly.

Using the lemmas 1 and 2, we can analyze the by-PRS.

Lemma 4. Let $(P_1,P_2,\ldots,P_k)$ be a PRS generated through (1.3) and $(\tilde{P}_1,\tilde{P}_2,\ldots,\tilde{P}_k)$ be a by-PRS generated through (1.7). Then for such j that $0<j<n_i$, we have the following equalities:

when $0<j<n_{i+1}$

$$\alpha_i^{(n_i-j)} \tilde{\alpha}_i \cdot \tilde{S}_{j-1}(P_{i-1},P_i,\tilde{P}_{i-1}) = (-1)^{(n_i-j)(n_{i-1}-j)} c_i^{(d_{i-1}+d_i)} \beta_i^{(n_i-j)} \tilde{\beta}_i \cdot \tilde{S}_{j-1}(P_i,P_{i+1},\tilde{P}_i), \tag{3.12}$$

when $j=n_{i+1}\leqq\tilde{n}_i$

$$\alpha_i^{d_i} \tilde{\alpha}_i \cdot \tilde{S}_{n_{i+1}-1}(P_{i-1},P_i,\tilde{P}_{i-1}) = (-1)^{d_i(d_{i-1}+d_i)} c_i^{(d_{i-1}+d_i)} c_{i+1}^{(n_i-\tilde{n}_i-1)} \beta_i^{d_i} \tilde{\beta}_i \cdot \mathrm{prem}(\tilde{P}_i,P_{i+1}), \tag{3.13}$$

when $j=n_{i+1}>\tilde{n}_i$

$$\alpha^{d_i} \tilde{\alpha}_i \cdot \tilde{S}_{n_{i+1}-1}(P_{i-1},P_i,\tilde{P}_{i-1}) = (-1)^{d_i(d_{i-1}+d_i)} c_i^{(d_{i-1}+d_i)} c_{i+1}^{d_i} \beta_i^{d_i} \tilde{\beta}_i \cdot \tilde{P}_i, \tag{3.14}$$

when ($j=n_{i+1}+1$ or $j=n_i-1$) and $n_{i+1}<\tilde{n}_i=n_i-1$

$$\alpha_i^{(n_i-j)} \tilde{\alpha}_i \cdot \tilde{S}_{j-1}(P_{i-1},P_i,\tilde{P}_{i-1}) = (-1)^{(n_i-j)(n_{i-1}-j+1)} c_i^{(n_{i-1}-j)} c_{i+1}^{(n_i-j-1)} \beta_i^{(n_i-j)} \tilde{c}_i \tilde{\beta}_i \cdot P_{i+1}, \tag{3.15}$$

and in other cases of $j<n_i$, that is,

when $j=n_{i+1}+1$ and $\tilde{n}_i<n_i-1$ or when $n_{i+1}+1<j<n_i-1$ or when $j=n_i-1>n_{i+1},\tilde{n}_i$

$$\tilde{S}_{j-1}(P_{i-1},P_i,\tilde{P}_{i-1}) = 0. \tag{3.16}$$

(Proof) (Shouryaku)

Now, we are ready to state the main theorem.

Theorem 2 (main theorem on by-PRS). The extended subresultant $\tilde{S}_{j-1}(P_1,P_2,\tilde{P}_1)$ satisfies the following equalities:

when $0<j<n_k$

$$\tilde{S}_{j-1}(P_1,P_2,\tilde{P}_1) = 0, \tag{3.17}$$

when $j=n_{i+1}\leqq\tilde{n}_i$, $i=2,3,\ldots,k-1$,

$$\tilde{S}_{n_{i+1}-1}(P_1,P_2,\tilde{P}_1)\prod_{r=2}^{i}\{\alpha_r^{(n_r-n_{i+1})}\tilde{\alpha}_r\} = c_{i+1}^{(n_i-\tilde{n}_i-1)}\cdot\mathrm{prem}(\tilde{P}_i,P_{i+1}) \times\prod_{r=2}^{i}\{(-1)^{(n_r-n_{i+1})(n_{r-1}-n_{i+1})}C_r^{(d_{r-1}+d_r)}\beta_r^{(n_r-n_{i+1})}\tilde{\beta}_r\}, \tag{3.18}$$

when $j=n_{i+1}>\tilde{n}_i$, $i=2,3,\ldots,k-1$,

$$\tilde{S}_{n_{i+1}-1}(P_1,P_2,\tilde{P}_1)\prod_{r=2}^{i}\{\alpha_r^{(n_r-n_{i+1})}\tilde{\alpha}_r\} = c_{i+1}^{d_i}\cdot\tilde{P}_i \times\prod_{r=2}^{i}\{(-1)^{(n_r-n_{i+1})(n_{r-1}-n_{i+1})}C_r^{(d_{r-1}+d_r)}\beta_r^{(n_r-n_{i+1})}\tilde{\beta}_r\}, \tag{3.19}$$

when ($j=n_{i+1}+1$ or $j=n_i-1$) and $n_{i+1}<\tilde{n}_i=n_i-1$, $i=2,3,\ldots,k-1$,

$$\tilde{S}_{j-1}(P_1,P_2,\tilde{P}_1)\prod_{r=2}^{i}\{\alpha_r^{(n_r-j)}\tilde{\alpha}_r\} = (-1)^{(n_i-j)}C_i^{(n_{i+1}-j)}C_{i+1}^{(n_i-j-1)}\tilde{C}_i\cdot P_{i+1} \times\prod_{r=2}^{i}\{(-1)^{(n_r-j)(n_{r-1}-j)}C_r^{(d_{r-1}+d_r)}\beta_r^{(n_r-j)}\tilde{\beta}_r\}, \tag{3.20}$$

and in other cases of $j<n_i$, $i=2,3,\ldots,k-1$, that is,

when $j=n_{i+1}+1$ and $\tilde{n}_i<n_i-1$ or when $n_{i+1}+1<j<n_i-1$ or when $j=n_i-1>n_{i+1},\tilde{n}_i$

$$\tilde{S}_{j-1}(P_1,P_2,\tilde{P}_1) = 0. \tag{3.21}$$

(Proof) (Shouryaku)

Let us comment on theorem 2. Since $\tilde{n}_i \geqq n_{i+1}$ in (3.18), $\mathrm{prem}(\tilde{P}_i,P_{i+1}) \sim \tilde{P}_{i+1}$ in (3.18), hence (3.18) states that

$$\tilde{S}_{n_{i+1}-1}(P_1,P_2,\tilde{P}_1) \sim \tilde{P}_{i+1}. \tag{3.23}$$

Similarly, (3.19) gives the same similarity because $\tilde{P}_i \sim \tilde{P}_{i+1}$ in this case (note that $n_{i+1}>\tilde{n}_i$ for (3.19)). That is, (3.18) and (3.19) represent the same similarity in two different cases, $n_{i+1}\leqq\tilde{n}_i$ and $n_{i+1}>\tilde{n}_i$. Note that we have either (3.18) or (3.19) in any case. Both (3.18) and (3.19) correspond to (2.7) for PRS, and no equality is obtained which corresponds to (2.10) for PRS. Eq.(3.20) is special because it exists only in special cases of $n_{i+1}<\tilde{n}_i=n_i-1$. For example, (3.20) is vacuous for normal PRS for which $n_{i+1}=n_i-1$, $i=2,3,\ldots,k-1$.

§4. Subresultant by-PRS algorithms

This section considers a problem of calculating by-PRS such that $\tilde{P}_i=\tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1)$. In this section we choose α_i as (1.4), or

$$\alpha_i = c_i^{d_{i-1}+1}. \tag{4.1}$$

The $\tilde{\alpha}_i$, β_i and $\tilde{\beta}_i$ are specified in the below.

We begin by defining normality for by-PRS:

Definition. A by-PRS is normal if $\tilde{n}_1\geqq n_2$ and $\tilde{n}_i=n_i-1$ for every $i=2,3,\ldots,k-1$ and for $i=k$ if $n_k>0$, otherwise the PRS is abnormal. (Note that a by-PRS can be normal even if the main-PRS is abnormal.)

[Case 1] Normal by-PRS, i.e., $\tilde{n}_1\geqq n_2$ and $\tilde{n}_i=n_i-1$ for all $i\geqq 2$. In this case, (3.18) becomes (with replacement $i+1\rightarrow i$)

$$\mathrm{prem}(\tilde{P}_{i-1},P_i) = \tilde{\lambda}_i\tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1)\prod_{r=2}^{i-1}(\tilde{\alpha}_r/\tilde{\beta}_r), \quad i=3,4,\ldots,k, \tag{4.2}$$

$$\tilde{\lambda}_i = \prod_{r=2}^{i-1}\{(-1)^{(n_r-n_i)(n_{r-1}-n_i)}C_r^{-(d_{r-1}+d_r)}(\alpha_r/\beta_r)^{(n_r-n_i)}\}. \tag{4.3}$$

Therefore, if we define $\tilde{\alpha}_i$ as

$$\tilde{\alpha}_2 = c_2^{\tilde{n}_1-n_2+1}, \qquad \tilde{\alpha}_i = c_i^{\tilde{n}_{i-1}-n_i+1} = c_i^{d_{i-1}}, \quad i=3,4,\ldots,k, \tag{4.4}$$

then $\tilde{\beta}_i\tilde{P}_i = \tilde{\alpha}_i\tilde{P}_{i-1} - \tilde{Q}_iP_i = \text{prem}(\tilde{P}_{i-1},P_i)$, $i\geq 2$. Hence, (4.2) becomes

$$\tilde{P}_i = \tilde{\lambda}_i\tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1)(1/\tilde{\beta}_2)\prod_{r=2}^{i-1}(\tilde{\alpha}_r/\tilde{\beta}_{r+1}). \tag{4.5}$$

[Case 2] Abnormal by-PRS with $\deg(\tilde{P}_{i-1})\geq\deg(P_i)$.

In this case, (3.18) becomes (with replacement $i+1 \rightarrow i$)

$$c_i^{(n_{i-1}-\tilde{n}_{i-1}-1)}\,\text{prem}(\tilde{P}_{i-1},P_i) = \tilde{\lambda}_i\tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1)\prod_{r=2}^{i-1}(\tilde{\alpha}_r/\tilde{\beta}_r). \tag{4.6}$$

Therefore, if we choose $\tilde{\alpha}_i$ as

$$\begin{aligned}\tilde{\alpha}_2 &= c_2^{\tilde{n}_1-n_2+1},\\ \tilde{\alpha}_i &= c_i^{n_{i-1}-n_i} = c_i^{d_{i-1}}, \quad i=3,4,\ldots,k,\end{aligned} \tag{4.7}$$

then $\tilde{\beta}_i\tilde{P}_i = \tilde{\alpha}_i\tilde{P}_{i-1} - \tilde{Q}_iP_i = c_i^{(n_{i-1}-\tilde{n}_{i-1}-1)}\,\text{prem}(\tilde{P}_{i-1},P_i)$,

and (4.6) is made coincide with (4.5).

[Case 3] Abnormal by-PRS with $\deg(\tilde{P}_{i-1})<\deg(P_i)$.

In this case, (3.19) becomes (with replacement $i+1 \rightarrow i$)

$$c_i^{d_{i-1}}\tilde{P}_{i-1} = \tilde{\lambda}_i\tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1)\prod_{r=2}^{i-1}(\tilde{\alpha}_r/\tilde{\beta}_r), \quad i\geq 3. \tag{4.8}$$

Since $\tilde{\beta}_i\tilde{P}_i = \tilde{\alpha}_i\tilde{P}_{i-1}$ in this case, we can choose $\tilde{\alpha}_i$ freely. Therefore, by choosing $\tilde{\alpha}_i$, $i\geq 3$, as (4.7), we can make (4.8) coincide with (4.5). The $\tilde{\alpha}_2$ can be chosen as (4.7) if $\tilde{n}_1\geq n_2$. If $\tilde{n}_1<n_2$, we can choose $\tilde{\alpha}_2=1$ without contradiciton with (4.5) because we have no constraint on $\tilde{P}_2$ except that $\tilde{P}_2 \in I[x]$.

Summarizing the above results, we see that formulas (3.18) and (3.19) are unified to (4.5) by the choice

$$\begin{aligned}&\tilde{\alpha}_2 = c_2^{\tilde{n}_1-n_2+1} \text{ if } \tilde{n}_1\geq n_2 \quad \text{else} \quad \tilde{\alpha}_2 = 1,\\ &\tilde{\alpha}_i = c_i^{d_{i-1}}, \quad i=3,4,\ldots,k.\end{aligned} \tag{4.4, 4.7}$$

Then, (4.5) suggests the following choice of $\tilde{\beta}_i$:

$$\begin{aligned}\tilde{\beta}_2 &= 1,\\ \tilde{\beta}_i &= \tilde{\alpha}_{i-1}, \quad i=3,4,\ldots,k,\end{aligned} \tag{4.9}$$

which reduces (4.5) to

$$\tilde{P}_i = \tilde{\lambda}_i\tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1), \quad i=3,4,\ldots,k. \tag{4.10}$$

Note that $\tilde{\lambda}_i$ depends only on main-PRS and not on by-PRS. Note further that

$$\tilde{\lambda}_i = c_i^{(d_{i-1}-1)}\lambda_i. \tag{4.11}$$

So far, we have not specified the main-PRS. In the rest of this section, two kinds of PRS's are considered: one is the reduced PRS and the other is the subresultant PRS.

[Case A] When $P_i=P_i^{(red)}$ (the reduced PRS).

In this case, β_i is chosen as (2.12). Substituting $c_i^{d_{i-1}+1}$ and $c_{i-1}^{d_{i-2}+1}$, respectively, for α_i and β_i in (4.3), we obtain

$$\tilde{\lambda}_i = \prod_{r=2}^{i-1}\{c_r^{d_{r-1}(d_r-1)}(-1)^{(n_{r-1}-n_i)(n_r-n_i)}\}. \tag{4.12}$$

Thus, $\tilde{\lambda}_i \in I$ and hence $\tilde{P}_i \in I[x]$. Furthermore, since $\tilde{\lambda}_i$ is easily calculated from the main-PRS, we can eliminate $\tilde{\lambda}_i$ from $\tilde{P}_i$ obtaining a polynomial $\hat{P}_i$ such that

$$\hat{P}_i = \tilde{P}_i/\tilde{\lambda}_i = \tilde{S}_{n_i-1}(P_1,P_2,\tilde{P}_1). \tag{4.13}$$

(We have introduced a new notaion $\hat{P}_i$ to emphasize the elimination of the factor $\tilde{\lambda}_i$ from $\tilde{P}_i$.) In order to calculate the sign factor in (4.12), we can use the following relation which is easily derived from (4.12):

$$\tilde{\lambda}_i/\tilde{\lambda}_{i-1} = c_{i-1}^{d_{i-2}(d_{i-1}-1)}(-1)^{(n_1-n_i+i-1)d_{i-1}}, \quad i=4,5,\ldots,k. \tag{4.14}$$

Noting that $\tilde{\lambda}_3 = c_2^{d_1(d_2-1)}(-1)^{(n_1-n_3)d_2}$, we can extend (4.14) to the case of $i=3$ by defining $\tilde{\lambda}_2=1$. Hence, we obtain the following algorithm.

Algorithm A (reduced PRS/subresultant by-PRS algorithm).

Input : polynomials F,G,H such that $\deg(F)\geq\deg(H)\geq\deg(G)$;

Output: reduced PRS $(P_1=F,P_2=G,P_3,\ldots,P_k)$ and

subresultant by-PRS $(\hat{P}_1=H,\hat{P}_2,\ldots,\hat{P}_k)$;

$\hat{P}_2 \leftarrow \tilde{P}_2 \leftarrow \mathrm{prem}(\tilde{P}_1,P_2)$;

$P_3 \leftarrow \mathrm{prem}(P_1,P_2)$;

$i \leftarrow 2$;

$\tilde{\lambda} \leftarrow 1$;

while $\deg(P_{i+1})>0$ do begin

$i \leftarrow i+1$;

if $i=3$ then $\tilde{\beta} \leftarrow c_2^{(\tilde{n}_1-n_2+1)}$ else $\tilde{\beta} \leftarrow c_{i-1}^{d_{i-1}}$;

if $\tilde{n}_{i-1}\geq n_i$ then $\tilde{P}_i \leftarrow \{c_i^{(n_{i-1}-\tilde{n}_{i-1}-1)}\mathrm{prem}(\tilde{P}_{i-1},P_i)\}/\tilde{\beta}$

else $\tilde{P}_i \leftarrow \{c_i^{d_{i-1}}\tilde{P}_{i-1}\}/\tilde{\beta}$;

$\tilde{\lambda} \leftarrow \tilde{\lambda}\cdot c_{i-1}^{d_{i-2}(d_{i-1}-1)}(-1)^{(n_i-n_{i-1}+i-1)d_{i-1}}$;

$\hat{P}_i \leftarrow \tilde{P}_i/\tilde{\lambda}$;

$P_{i+1} \leftarrow \mathrm{prem}(P_{i-1},P_i)/c_{i-1}^{(d_{i-2}+1)}$;

end;

return $(P_1,P_2,\ldots,P_i)$ and $(\hat{P}_1,\hat{P}_2,\ldots,\hat{P}_i)$.

[Case B] When $P_i=P_i^{(sub)}$ (the subresultant PRS).

Using the relation $(-1)^{i\times i}=(-1)^i$ which is valid for any integer i, we can derive the following relation from (2.11) and (4.3):

$$\tilde{\lambda}_i/\rho_i = \{(1/c_{i-1})\prod_{r=2}^{i-1}(\alpha_r/\beta_r)(-1)^{(n_{r-1}+n_r+1)}\}^{(d_{i-1}-1)}. \qquad (4.15)$$

Since $\rho_i=1$ for the subresultant PRS, (2.15), (2.17) and (4.15) give

$$\tilde{\lambda}_i = (-\zeta_i)^{(d_{i-1}-1)} = \{\mathrm{lc}[S_{n_{i-1}}(P_1,P_2)]\}^{(d_{i-1}-1)}. \qquad (4.16)$$

Thus, $\tilde{\lambda}_i \in I$ and hence $\tilde{P}_i \in I[x]$. Since ζ_i is obtained by the subresultant PRS calculation, we can eliminate $\tilde{\lambda}_i$ easily from $\tilde{P}_i$ obtaining the $\hat{P}_i$ defined by (4.13). Hence, we obtain the following algorithm.

Algorithm B (subresultant PRS/subresultant by-PRS algorithm).

Input : polynomials F,G,H such that $\deg(F)\geq\deg(H)\geq\deg(G)$;

Output: subresultant PRS $(P_1=F,P_2=G,P_3,\ldots,P_k)$ and

subresultant by-PRS $(\hat{P}_1=H,\hat{P}_2,\ldots,\hat{P}_k)$;

$\hat{P}_2 \leftarrow \tilde{P}_2 \leftarrow \mathrm{prem}(\tilde{P}_1,P_2)$;

$P_3 \leftarrow \mathrm{prem}(P_1,P_2)/(-1)^{d_1+1}$;

$i \leftarrow 2$;

$\zeta \leftarrow -1$;

while $\deg(P_{i+1})>0$ do begin

$i \leftarrow i+1$;

if $i=3$ then $\tilde{\beta} \leftarrow c_2^{(\tilde{n}_1-n_2+1)}$ else $\tilde{\beta} \leftarrow c_{i-1}^{d_{i-2}}$;

if $\tilde{n}_{i-1}\geq n_i$ then $\tilde{P}_i \leftarrow \{c_i^{(n_{i-1}-\tilde{n}_{i-1}-1)}\mathrm{prem}(\tilde{P}_{i-1},P_i)\}/\tilde{\beta}$

else $\tilde{P}_i \leftarrow \{c_i^{d_{i-1}}\tilde{P}_{i-1}\}/\tilde{\beta}$;

$\zeta \leftarrow (-c_{i-1})^{d_{i-2}}\zeta^{(1-d_{i-2})}$;

$\tilde{\lambda} \leftarrow (-\zeta)^{(d_{i-1}-1)}$;

$\hat{P}_i \leftarrow \tilde{P}_i/\tilde{\lambda}$;

$P_{i+1} \leftarrow \mathrm{prem}(P_{i-1},P_i)/(-c_{i-1}\zeta^{d_{i-1}})$;

end ;

return $(P_1,P_2,\ldots,P_i)$ and $(\hat{P}_1,\hat{P}_2,\ldots,\hat{P}_i)$.

§5. Examples

Let us present several examples. We calculate PRS's and by-PRS's with starting polynomials

$$F(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5,$$

$$G(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$

$$H(x) = 2x^8 + 2x^7 + 3x^5 - 4x^3 - 2x - 1.$$

Example 1 (original PRS / original by-PRS).

P_1: (1, 0, 1, 0, −3, −3, 8, 2, −5),
P_2: (3, 0, 5, 0, −4, −9, 21),
P_3: (−15, 0, 3, 0, −9), : $\beta_2=1$
P_4: (15795, 30375, −59535), : $\beta_3=1$
P_5: (1254542875143750, −1654608338437500), : $\beta_4=1$
P_6: (12593338795500743100931141992187500). : $\beta_5=1$

$\tilde{P}_1$: (2, 2, 0, 3, 0, −4, 0, −2, −1),
$\tilde{P}_2$: (−9, 222, 126, −336, −702, 603), : $\tilde{\beta}_2=1$
$\tilde{P}_3$: (27945, −65610, −156735, 105705), : $\tilde{\beta}_3=1$
$\tilde{P}_4$: (44436771365624, −85860272261250), : $\tilde{\beta}_4=1$
$\tilde{P}_5$: (−34189940388449881177593750000), : $\tilde{\beta}_5=1$
$\tilde{P}_6$: (0).

Example 2 (reduced PRS / subresultant by-PRS).

P_1: (1, 0, 1, 0, −3, −3, 8, 2, −5),
P_2: (3, 0, 5, 0, −4, −9, 21),
P_3: (−15, 0, 3, 0, −9), : $\beta_2=1$
P_4: (585, 1125, −2205), : $\beta_3=3^3$
P_5: (−18885150, 24907500), : $\beta_4=(-15)^3$
P_6: (527933700). : $\beta_5=585^3$

$\tilde{P}_1$: (2, 2, 0, 3, 0, −4, 0, −2, −1),
$\tilde{P}_2$: (−9, 222, 126, −336, −702, 603), : $\tilde{\beta}_2=1$
$\tilde{P}_3$: (1035, −2430, 5805, 3915), : $\tilde{\beta}_3=3^3$
$\tilde{P}_4$: (10033875, −19387350), : $\tilde{\beta}_4=(-15)^2$
$\tilde{P}_5$: (339584400), : $\tilde{\beta}_5=585^2$
$\tilde{P}_6$: (0).

$\hat{P}_2$: (−9, 222, 126, −336, −702, 603),
$\hat{P}_3$: (115, −270, −645, 435), : $\tilde{\lambda}_3=9$
$\hat{P}_4$: (4955, −9574), : $\tilde{\lambda}_4=2025$
$\hat{P}_5$: (−167696), : $\tilde{\lambda}_5=-2025$,
$\hat{P}_6$: (0).

Example 3 (subresultant PRS / subresultant by-PRS).

P_1: (1, 0, 1, 0, −3, −3, 8, 2, −5),
P_2: (3, 0, 5, 0, −4, −9, 21),
P_3: (15, 0, −3, 0, 9), : $\beta_2=-1$
P_4: (65, 125, −245), : $\beta_3=-3^5$
P_5: (9326, −12300), : $\beta_4=-15\cdot5^4$
P_6: (260708). : $\beta_5=65\cdot13^2$

$\tilde{P}_1$: (2, 2, 0, 3, 0, −4, 0, −2, −1),
$\tilde{P}_2$: (−9, 222, 126, −336, −702, 603), : $\tilde{\beta}_2=1$
$\tilde{P}_3$: (1035, 2430, −5805, 3915), : $\tilde{\beta}_3=3^3$
$\tilde{P}_4$: (123875, −239350), : $\tilde{\beta}_4=15^2$
$\tilde{P}_5$: (−167696), : $\tilde{\beta}_5=65^2$
$\tilde{P}_6$: (0).

$\hat{P}_2$: (−9, 222, 126, −336, −702, 603),
$\hat{P}_3$: (115, −270, −645, 435), : $\tilde{\lambda}_3=9$
$\hat{P}_4$: (4955, −9574), : $\tilde{\lambda}_4=25$
$\hat{P}_5$: (−167696), : $\tilde{\lambda}_5=1$
$\hat{P}_6$: (0).

References

1. D. E. Knuth, The art of computer programming, Vol.2: Seminumerical algorithms, §4.6, 1969, Addison-Wesley.
2. G. E. Collins, Polynomial remainder sequences and determinants, Amer. Math. Mon. 73, No.7, p.708, 1966.
3. G. E. Collins, Subresultants and reduced polynomial remainder sequences, J. ACM 14, No.1, p.128, 1967.
4. W. S. Brown and J. F. Traub, On Euclid's algorithm and the theory of subresultants, J. ACM 18, No.4, p.505, 1971.
5. W. S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors, J. ACM 18, No.4, p.478, 1971.
6. W. S. Brown, The subresultant PRS algorithm, ACM Trans. Math. Soft. 4, No.3, p.237, 1978.