多重多項式剰余列の線形不定方程式への応用

古川昭夫（東京都立大学理学部）
佐々木建昭（理化学研究所）

（概要）

多項式剰余列（PRS）の概念は，Computer Algebra において最も有益な概念の1つであり，多項式GCDの効率的計算法とならんで，ハビヒト，コリンズ，ブラウン，トラウブらによって研究されてきた。

2つの多項式 $P_1(x)$，$P_2(x)$（但し $\deg P_1 \geq \deg P_2$）が与えられたとき，PRSは，(P_i, P_{i+1}) の P_i の高次の項を $P_{i+1}=0$ なる関係式で消去することによって，

$(P_1, P_2) \to (P_2, P_3) \to \cdots \to (P_i, P_{i+1}) \to (P_{i+1}, P_{i+2}) \to \cdots$

と次数を落として reduction する計算だとみなすことができる。

この事に注目して，我々は，

$(P_1, P_2, \widetilde{P_1}) \to (P_2, P_3, \widetilde{P_2}) \to (P_3, P_4, \widetilde{P_3}) \to$

なる reduction の計算として 副多項式剰余列を考察し，

$(P_0^{(1)}, P_0^{(2)}, \ldots, P_0^{(m)}) \to (P_1^{(1)}, P_1^{(2)}, \ldots, P_1^{(m)}) \to$

なる reduction の計算として 多重多項式剰余列を考察し，それに対応する部分終結式の理論を構成した。

今回は，多項式係数の線形不定方程式系の多項式解を求めるアルゴリズムに多重多項式剰余列の理論を適用することによって，効率的なアルゴリズムを構成することができることを示す。

（おことわり）

前回と内容の一部が重複いたしますので，§2，§3 は大幅に省略させていただきました。§2，§3 の内容については，第22回の研究会の資料をご参照下さい。なお，この論文の full paper は，「Eurocal '83」の論文集（Springer より発刊予定）にて発表される予定です。

（おしらせ）

MULTI POLYNOMIAL REMAINDER SEQUENCE AND ITS APPLICATION TO LINEAR DIOPHANTINE EQUATIONS

- shortened version -

Akio Furukawa*) and Tateaki Sasaki**)

*) Department of Mathematics, Tokyo Metropolitan University
Setagaya-ku, Tokyo 158, Japan
**) The Institute of Physical and Chemical Research
Wako-shi, Saitama 351, Japan

§1. Motivation and introduction

The polynomial remainder sequence (PRS in short) is one of the most useful concepts in computer algebra, and it was thoroughly investigated by Habicht[1], Collins[2,3], Brown and Traub[4], and Brown[5]. (See, also [6].) We can regard the calculation of PRS as a reduction of a set of two polynomials, that is, $(P_1(x),P_2(x)) \rightarrow (P_2(x),P_3(x)) \rightarrow \cdots \rightarrow (P_k(x),P_{k+1}(x))$, where the reduction is made by eliminating high degree terms of a polynomial in each set. In many cases of algebraic computation, we encounter the necessity of reducing not only a set of two polynomials but also a set of $m(\geq 3)$ polynomials. A typical example is the calculation of elementary divisors of a matrix with polynomial elements. The main step of this calculation is to transform the matrix into a diagonal form by applying row/column eliminations repeatedly. The row/column elimination is nothing but the calculation of remainders or pseudo-remainders of a set of polynomials by choosing a suitable element of the matrix as the divisor.

The notion of reduction of a set of more than two polynomials leads us to a concept of multi-polynomial remainder sequence (multi-PRS in short) as a natural generalization of PRS. As for the conventional PRS, an elegant theory of subresultant has been developed [1,2,3,4,5] making the calculation of PRS quite efficient. We reasonably expect that the concept of subresultant can be generalized to the case of multi-PRS, and a generalization was performed in our recent paper[7]. However, it turned out that the generalization necessitated us to introduce several new concepts concerning the subresultant.

In section 2, we define multi-PRS and explain how the subresultant is generalized to the case of multi-PRS. The main results of our study of multi-PRS are surveyed in section 3. Section 3 also explains a concept of "secondary-PRS" which is obtained by a special choice of divisor polynomials in multi-PRS. In section 4, we show an application of multi-PRS to solving a system of linear Diophantine equations with polynomial coefficients. Section 5 presents an example of solving a Diophantine equation.

§2. Multi-PRS and PRS-matrix

Given a set of starting polynomials $\{P_0^{(1)}(x),\ldots,P_0^{(m)}(x)\}$ with coefficients in an integral domain I, we generate a sequence of sets of remainders $\{P_i^{(1)}(x),\ldots,P_i^{(m)}(x)\}$, $i=1,2,\ldots$, successively by the following formulas:

$$
\left.
\begin{array}{l}
\nu_i \in \{1,2,\ldots,m\}, \\
\beta_i^{(\mu)} P_{i+1}^{(\mu)} = \alpha_i^{(\mu)} P_i^{(\mu)} - Q_i^{(\mu)} P_i^{(\nu_i)}, \quad \deg(P_{i+1}^{(\mu)}) < \deg(P_i^{(\nu_i)}), \\
\qquad \text{for } \mu \text{ such that } \deg(P_i^{(\mu)}) \geqq \deg(P_i^{(\nu_i)}), \ \mu \neq \nu_i, \\
\beta_i^{(\mu)} P_{i+1}^{(\mu)} = \alpha_i^{(\mu)} P_i^{(\mu)} \\
\qquad \text{for } \mu \text{ such that } \deg(P_i^{(\mu)}) < \deg(P_i^{(\nu_i)}), \\
\alpha_i^{(\mu)}, \beta_i^{(\mu)} \in I, \\
P_{i+1}^{(\nu_i)} = P_i^{(\nu_i)} \quad \text{or} \quad \alpha_i^{(\nu_i)} = \beta_i^{(\nu_i)} = 1.
\end{array}
\right\} \qquad (1)
$$

We call the sequence $(\{P_0^{(1)},\ldots,P_0^{(m)}\}, \{P_1^{(1)},\ldots,P_1^{(m)}\}, \cdots)$ multi-PRS. Note that, in formulas (1), only one polynomial $P_i^{(\nu_i)}$ is used as a divisor to generate the set of (i+1)st remainders $\{P_{i+1}^{(1)},\ldots,P_{i+1}^{(m)}\}$. We can define a more general multi-PRS in which the (i+1)st remainders are generated by more than one divisor polynomial. Therefore, we had better call the sequence defined by (1) the multi-PRS in a narrow sense. Although the multi-PRS in a wide sense is also important in practice, this paper considers only the sequence defined by (1) and we simply call it multi-PRS.

Let F, G, H be polynomials of degrees ℓ, m, n, respectively, with coefficients in I:

$$
\left.
\begin{array}{ll}
F(x) = f_\ell x^\ell + f_{\ell-1} x^{\ell-1} + \ldots + f_0, & f_i \in I, \\
G(x) = g_m x^m + g_{m-1} x^{m-1} + \ldots + g_0, & g_i \in I, \\
H(x) = h_n x^n + h_{n-1} x^{n-1} + \ldots + h_0, & h_i \in I.
\end{array}
\right\} \qquad (2)
$$

Let $\ell \geqq m$ and the sequence $(P_1=F, P_2=G, P_3, P_4, \cdots)$ be a PRS. The subresultant theory asserts that, for each polynomial P_i in the PRS, there exists a matrix M_i such that

$$P_i(x) \sim |M_i|, \qquad (3)$$

where $\sim$ denotes the similarity, i.e., $A(x) \sim B(x)$ if $aA(x)=bB(x)$ for some nonzero a and b in I, and every nonzero element of the matrix M_i is either $x^k F$, $x^k G$, k=0,1,..., or a coefficient of F or G.

Let $\{P_i^{(1)},\ldots,P_i^{(m)}\}$, i=0,1,2,..., be a multi-PRS, and let $M_{i,j}^{(\mu)}$, $1 \leqq \mu \leqq m$, $0 \leqq j \leqq i-1$, denote a square matrix, where nonzero elements in the first column of $M_{i,j}^{(\mu)}$ are $x^k P_j^{(\mu')}$, k=0,1,..., $1 \leqq \mu' \leqq m$, and other nonzero elements of $M_{i,j}^{(\mu)}$ are coefficients of $P_j^{(\mu')}$. Main problems in the theory of multi-PRS are (1) to find an $M_{i,j}^{(\mu)}$ such that $P_j^{(\mu)} \sim |M_{i,j}^{(\mu)}|$, (2) to determine the proportional factor $\lambda_{i,j}^{(\mu)}$ such that $P_j^{(\mu)} = \lambda_{i,j}^{(\mu)} |M_{i,j}^{(\mu)}|$, and (3) to find efficient algorithms for calculating multi-PRS over I.

§3. Main theorems and secondary-PRS

The main theorems we have obtained on multi-PRS are as follows (lengthy proofs are found in [7]).

Theorem 1: For each polynomial $P_i^{(\mu)}(x)$ in the multi-PRS $\{P_i^{(1)},\ldots,P_i^{(m)}\}$, i=1,2,..., generated by (1), there exist PRS-matrices $M_{i,j}^{(\mu)}$, j=0,1,...,i-1, such that

$$P_i^{(\mu)}(x) \sim |M_{i,j}^{(\mu)}|. \qquad (5)$$

§4. Application to linear Diophantine equations

The multi-PRS, in particular the secondary-PRS, is nicely applicable to solving a system of linear Diophantine equations with polynomial coefficients. Let the ring R be Z (the ring of rational integers) or $Z[x_1,\ldots,x_s]$, and let the quotient field of R be S. We consider the following system of linear Diophantine equations:

$$\left.\begin{array}{l} a_{11}y_1 + \cdots + a_{1m}y_m = b_1, \\ \cdot \quad \cdots \quad \cdot \quad \cdot \\ a_{n1}y_1 + \cdots + a_{nm}y_m = b_n, \end{array}\right\} \tag{13}$$

where m>n, $a_{ij} \in R[x]$, $b_i \in R[x]$, and we want to obtain the solution

$$\bar{y} \equiv (y_1, \ldots, y_m) \tag{14}$$

such that $y_i \in S[x]$, i=1,...,m, if any. That is, we search for the solution which is polynomial in x with rational coefficients. Note that the Cramer's formula gives the solutions which are rational in x.

It is well known that (13) has not always a solution. Furthermore, since the number of equations, n, is less than the number of unknowns, m, the possible solutions of (13) are not unique. The general solution of (13), if it exists, is represented as

$$\bar{y} = \bar{y}_0 + c_1\bar{y}_1 + \cdots + c_r\bar{y}_r, \tag{15}$$

where $m-1 \geq r \geq m-n$, $\bar{y}_0$ is a particular solution of (13), $\{\bar{y}_1, \ldots, \bar{y}_r\}$ is a basis of the space of the solutions of homogeneous equations

$$\left.\begin{array}{l} a_{11}y_1 + \cdots + a_{1m}y_m = 0, \\ \cdot \quad \cdots \quad \cdot \quad \cdot \\ a_{n1}y_1 + \cdots + a_{nm}y_m = 0, \end{array}\right\} \tag{16}$$

and $c_1, \ldots, c_r$ are arbitrary elements in S[x].

We solve (13) in the following way [10], where the calculation is performed in R[x] as far as possible. We first solve the equation

$$a_{11}y_1 + \cdots + a_{1m}y_m = b_1$$

(an actual method is given later), and obtain the general solution

$$\bar{y} = \bar{y}_0^{(1)} + c_1^{(1)}\bar{y}_1^{(1)} + \cdots + c_{m-1}^{(1)}\bar{y}_{m-1}^{(1)}, \tag{17}$$

if it exists. Here, $c_1^{(1)}, \ldots, c_{m-1}^{(1)}$ are any elements in S[x], hence we represent them by indeterminates $y_{m+1}, \ldots, y_{2m-1}$:

$$\bar{y} = \bar{y}_0^{(1)} + y_{m+1}\bar{y}_1^{(1)} + \cdots + y_{2m-1}\bar{y}_{m-1}^{(1)}. \tag{17'}$$

Substituting (17') for $y_1, \ldots, y_m$ in the rest n-1 equations of (13), we obtain a reduced system of n-1 equations in m-1 unknowns $y_{m+1}, \ldots, y_{2m-1}$:

$$\left.\begin{array}{l} a'_{11}y_{m+1} + \cdots + a'_{1,m-1}y_{2m-1} = b'_1, \\ \cdot \quad \cdots \quad \cdot \quad \cdot \\ a'_{n-1,1}y_{m+1} + \cdots + a'_{n-1,m-1}y_{2m-1} = b'_{n-1}, \end{array}\right\} \tag{13'}$$

where we reduce $\bar{y}_i^{(1)}$, i=0,...,m-1, to a common denominator, hence $a'_{ij} \in R[x]$ and $b'_i \in R[x]$. Note that some equation in (13') may be nil. If this is the case, the dimension of the solution space increases, i.e., r>m-n.

Continuing the above reduction, we finally obtain a Diophantine equation in r+1 unknowns $y_{\mu+1}, \ldots, y_{\mu+r+1}$:

$$a''_1 y_{\mu+1} + \cdots + a''_{r+1}y_{\mu+r+1} = b'', \tag{13''}$$

where a''_i, $b'' \in R[x]$ and each of $y_1, \ldots, y_m$ is linearly related to $y_{\mu+1}, \ldots, y_{\mu+r+1}$. We solve (13'') and, if the solution exists, obtain the general solution

$$\bar{y}'' = \bar{y}''_0 + c_1\bar{y}''_1 + \cdots + c_r\bar{y}''_r, \tag{17''}$$

where $\bar{y}'' \equiv (y_{\mu+1}, \ldots, y_{\mu+r+1})$, $\bar{y}''_0$ is a particular solution of (13''), $\{\bar{y}''_1, \ldots, \bar{y}''_r\}$ is a basis of the space of the solutions of homogeneous equation, and $c_1, \ldots, c_r$ are arbitrary elements in S[x]. Substituting $\bar{y}''$ into $y_1, \ldots, y_m$, we obtain the general solution of (13) in the form (15).

Our problem is, therefore, reduced to solving the following linear Diophantine equation:

$$P_0^{(1)}(x)\, y_1 + \cdots + P_0^{(m)}(x)\, y_m = P_0^{(m+1)}(x), \tag{18}$$

where $P_0^{(i)}(x) \in R[x]$, $i=1,\dots,m+1$, and we want to obtain the solution $y_i \in S[x]$, $i=1,\dots,m$, if any. Equation (18) can be solved by successively eliminating higher degree terms of $P_0^{(1)}, \dots, P_0^{(m)}$ as follows. Let $P_0^{(\nu)} \in \{P_0^{(1)},\dots,P_0^{(m)}\}$, where $\deg_x(P_0^{(\nu)}) \leq \deg_x(P_0^{(\mu)})$ for at least one $\mu \neq \nu, m+1$. Performing pseudo-divisions of $P_0^{(\mu)}$, $\mu\neq\nu$, by $P_0^{(\nu)}$, we have

$$\left.\begin{aligned} \alpha_0 P_0^{(\mu)} &\equiv Q_0^{(\mu)} P_0^{(\nu)} + P_1^{(\mu)}, \quad \mu=1,\dots,\nu-1,\nu+1,\dots,m, \\ P_0^{(\nu)} &\equiv P_1^{(\nu)}, \end{aligned}\right\} \qquad (19)$$

where α_0 is chosen so that $P_1^{(\mu)} \in R[x]$, $\mu=1,\dots,m$. Substituting $P_0^{(i)}$ in (18) by the r.h.s. expressions in (19), we have

$$P_0^{(\nu)}\{Q_0^{(1)}y_1 + \cdots + \alpha_0 y_\nu + \cdots + Q_0^{(m)}y_m\}$$
$$+ P_1^{(1)}y_1 + \cdots + P_1^{(\nu-1)}y_{\nu-1} + P_1^{(\nu+1)}y_{\nu+1} + \cdots + P_1^{(m)}y_m = \alpha_0 P_0^{(m+1)}$$

Hence, introducing a new unknown y'_ν defined by

$$y'_\nu = Q_0^{(1)}y_1 + \cdots + \alpha_0 y_\nu + \cdots + Q_0^{(m)}y_m, \qquad (20)$$

we can rewrite (18) as

$$P_1^{(1)}y_1 + \cdots + P_1^{(\nu)}y'_\nu + \cdots + P_1^{(m)}y_m = \alpha_0 P_0^{(m+1)} \equiv P_1^{(m+1)}. \qquad (18')$$

Equation (18') is simpler than (18) in the sense that the degrees, in x, of coefficient polynomials are reduced.

Continuing the above reduction, we finally obtain

$$P_k^{(1)}(x)\, y''_1 + \cdots + P_k^{(m)}(x)\, y''_m = P_k^{(m+1)}(x), \qquad (18'')$$

where either $\deg_x(P_k^{(i)})=0$ for every $i\leq m$ and $P_k^{(\nu)}\neq 0$ for some $\nu\leq m$, or $\deg_x(P_k^{(\nu)})>0$ and $P_k^{(i)}=0$ for every $i=1,\dots,\nu-1,\nu+1,\dots,m$. Note that some of $P_k^{(i)}$, $i=1,\dots,m$, may be zero.

<u>Case 1</u>: $\deg_x(P_k^{(i)})=0$ for $i=1,\dots,m$ and $P_k^{(\nu)}\neq 0$ for some $\nu\leq m$. In this case, we can rewrite (18") as

$$P_k^{(\nu)} y''_\nu = P_k^{(m+1)} - \sum_{i=1,\neq\nu}^{m} P_k^{(i)} y''_i. \qquad (21)$$

Hence, $\{y''_\nu = P_k^{(m+1)}/P_k^{(\nu)},\ y''_{j\neq\nu}=0\}$ is a particular solution of (18"), and $\{y''_i=1,\ y''_\nu = -P_k^{(i)}/P_k^{(\nu)},\ y''_{j\neq i,\nu}=0\}$, $i=1,\dots,\nu-1,\nu+1,\dots,m$, constitute a basis of the space of the solutions of homogeneous equation. Since $y_1, \dots, y_m$ are linearly related to $y''_1, \dots, y''_m$, backward substitution of this solution gives the solution of (18) in the form (15).

<u>Case 2</u>: $\deg_x(P_k^{(\nu)})>0$ and $P_k^{(i)}=0$ for $i=1,\dots,\nu-1,\nu+1,\dots,m$. In this case, (18") turns out to be $P_k^{(\nu)}y''_\nu = P_k^{(m+1)}$ which has a solution only if

$$P_k^{(\nu)}(x) \mid P_k^{(m+1)}(x). \qquad (22)$$

If the condition (22) is satisfied, then $\{y''_\nu = P_k^{(m+1)}/P_k^{(\nu)},\ y''_{j\neq\nu}=0\}$ is a particular solution of (18") and $\{y''_i=1,\ y''_{j\neq i}=0\}$, $i=1,\dots,\nu-1,\nu+1,\dots,m$, constitute a basis of the space of the solutions of homogeneous equation.

Although the method described above is quite simple in principle, actual computation requires a large amount of time ([10] gives a time complexity analysis). In fact, the situation is much worse than the calculation of PRS, because the above method is a repetition of multi-PRS calculation and fraction reduction to a common denominator. Using the theorem 2, however, we can improve the situation considerably.

When calculating the (i+1)st remainders $P_{i+1}^{(\mu)}$, $\mu=1,\dots,m$, from the i-th remainders $P_i^{(\mu)}$, formula (19) should be read as

$$\left.\begin{aligned} \alpha_i P_i^{(\mu)} &= Q_i^{(\mu)} P_i^{(\nu_i)} + P_{i+1}^{(\mu)}, \quad \mu=1,\dots,\nu-1,\nu+1,\dots,m, \\ P_i^{(\nu_i)} &= P_{i+1}^{(\nu_i)}, \quad \alpha_i P_i^{(m+1)} = P_{i+1}^{(m+1)}, \end{aligned}\right\} \qquad (19')$$

where

$$\alpha_i = [\mathrm{lc}(P_i^{(\nu_i)})]^{d_i+1}, \quad d_i = \max[\deg(P_i^{(\mu)}) - \deg(P_i^{(\nu_i)}), \mu=1,\dots,m]. \qquad (23)$$

Our improvement is to use, instead of (19'), the following formulas:

$$\left.\begin{aligned}\alpha_i P_i^{(\mu)} &= Q_i^{(\mu)} P_i^{(\nu_i)} + \beta_i P_{i+1}^{(\mu)}, \quad \mu=1,\dots,\nu-1,\nu+1,\dots,m,\\ P_i^{(\nu_i)} &= P_{i+1}^{(\nu_i)}, \quad \alpha_i P_i^{(m+1)} = \beta_i P_{i+1}^{(m+1)},\end{aligned}\right\} \quad (24)$$

where β_i is determined by the multi-PRS theory so that $P_{i+1}^{(\mu)} \in R[x]$, $\mu=1,\dots,m+1$. Correspondingly, (20) should be replaced by

$$\beta_i y'_\nu = Q_i^{(1)} y_1 + \cdots + \alpha_i y_\nu + \cdots + Q_i^{(m)} y_m. \quad (25)$$

Noting that the factors independent of x are irrelative to the essence of the multi-PRS calculation, we can improve the calculation method further by putting

$$P_i^{(\mu)} = \gamma_i^{(\mu)} \tilde{P}_i^{(\mu)}, \quad \mu=1,\dots,m+1, \quad (26)$$

where we calculate $\tilde{P}_i^{(\mu)}$ by a multi-PRS algorithm with

$$\alpha_i^{(\mu)} = [\mathrm{lc}(P_i^{(\nu_i)})]^{d_i^{(\mu)}+1}, \quad d_i^{(\mu)} = \max[-1, \deg(P_i^{(\mu)}) - \deg(P_i^{(\nu_i)})]. \quad (27)$$

Since $\alpha_i^{(\mu)} \mid \alpha_i$ and $\tilde{P}_i = \pm \left| M_{i,0}^{(\mu)} \right|$ for every μ, we find

$$\gamma_i^{(\mu)} = \prod_{j=0}^{i-1} [\mathrm{lc}(P_j^{(\nu_j)})]^{e(\mu,i,j)}, \quad e(\mu,i,j) \text{ is an integer} \geqq 0, \quad (28)$$

and it is easy to obtain $\gamma_i^{(\mu)}$ in this factored form. Hence, calculating $P_i^{(\mu)}$ in the factored form (26), we can improve the reduction step for solving (18) drastically. Note that, in the above formulas, we had better calculate $\tilde{P}_i^{(\mu)}$, $\mu=3,4,\dots,m$, as secondary-PRSs with the divisor polynomial $\tilde{P}_i^{(1)}$ or $\tilde{P}_i^{(2)}$, because the expressions $\tilde{P}_i^{(\mu)}$ become almost smallest in this case.

§5. Example

Let us solve, for example, the following Diophantine equation:

$$F_1 y_1 + F_2 y_2 + \tilde{F}_1 y_3 = 1, \quad (29)$$

where

$$F_1 = x^4 + x^3 - 3x^2 + 1,$$
$$F_2 = 3x^4 + 5x^3 - 9x^2 + 21,$$
$$\tilde{F}_1 = 2x^4 - x^3 - 2x^2 + 1.$$

We first apply the formulas (19') and (23) to solve (29). Denoting the general solution of (29) as $\bar{y} = \bar{y}_0 + c_3\bar{y}_3 + c_7\bar{y}_7$, we obtain

$$\left.\begin{aligned}
y_1 = \{&(281715378192x^3+757904884992x^2+363625526592x-1751359292784)\\
&+c_3(-1383865015680x^3+1062147867840x^2-2317918368960x-11423735363520)\\
&+c_7(3x^4+5x^3-9x+21)\}/10102066528320,\\
y_2 = \{&(-93905126064x^3-190031544288x^2+224591148144x+564448848624)\\
&+c_3(461288338560x^3-661574848320x^2+137349898560x+62936611200)\\
&+c_7(-x^4-x^3+3x^2-1)\}/10102066528320,\\
y_3 = c_3&.
\end{aligned}\right\} \quad (30)$$

In deriving (30), we generated PRS $(F_1, F_2, \dots, F_6)$ and secondary-PRS $(\tilde{F}_1, \tilde{F}_2, \dots, \tilde{F}_5)$ with the starting polynomials F_1, F_2, and $\tilde{F}_1$. The secondary-PRS generated is

$$\tilde{F}_2 = -13x^3 - 6x^2 + 18x - 39,$$
$$\tilde{F}_3 = 210x^2 - 162x + 312,$$
$$\tilde{F}_4 = 5969052x - 3584412,$$
$$\tilde{F}_5 = 84244166694535680.$$

We next apply the formulas (24) and (23) with $\beta_{i+1} = \alpha_i$. Then, the large coefficients in the PRS and secondary-PRS are reduced and we obtain the following solution:

$$\left.\begin{aligned} y_1 &= \{\ (15219x^3+40944x^2+19644x-94613) \\ &\quad + c_3(-74760x^3+57380x^2-125220x-617140) \\ &\quad + c_7(3x^4+5x^3-9x+21)\ \}/545740, \\ y_2 &= \{\ (-5073x^3-10266x^2+12133x+30493) \\ &\quad + c_3(24920x^3-35740x^2+7420x+3400) \\ &\quad + c_7(-x^4-x^3+3x^2-1)\ \}/545740, \\ y_3 &= c_3. \end{aligned}\right\} \qquad (30')$$

We see that the calculation was improved remarkably. Note that (30) and (30') are the same solution because c_3 and c_7 are arbitrary rational numbers.

Acknowledgement

One of the authors (T.S.) acknowledges The Kurata Foundation for partially supporting this work..

References

[1] W. Habicht, Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens, Comm. Math. Helvetici 21, pp.99-116 (1948).

[2] G. E. Collins, Polynomial remainder sequences and determinants, Amer. Math. Mon. 73, No.7, pp.708-712 (1966).

[3] G. E. Collins, Subresultants and reduced polynomial remainder sequences, J. ACM 14, No.1, pp.128-142 (1967).

[4] W. S. Brown and J. F. Traub, On Euclid's algorithm and the theory of subresultants, J. ACM 18, No.4, pp.505-514 (1971).

[5] W. S. Brown, The subresultant PRS algorithm, ACM Trans. Math. Soft. 4, No.3, pp.237-249 (1978).

[6] R. Loos, Generalized polynomial remainder sequences, Computing Suppl. 4, "Computer Algebra," eds. B. Buchberger, G. E. Collins and R. Loos, pp.115-137, Springer-Verlag, 1982.

[7] T. Sasaki and A. Furukawa, Theory of multi-polynomial remainder sequence, preprint of IPCR, November 1982 (submitted for publication).

[8] T. Sasaki and A. Furukawa, Secondary-polynomial remainder sequence and an extension of subresultant theory, preprint of IPCR, May 1982 (submitted for publication).

[9] T. Sasaki, Extended Euclidean algorithm and determinants, preprint of IPCR, April 1982 (submitted for publication).

[10] A. Furukawa, Algebraic methods for linear Diophantine equations and theory of secondary-polynomial remainder sequence (in Japanese), Master Thesis, Tokyo Metropolitan Univ, March 1982.