Publ. RIMS, Kyoto Univ.
20 (1984), 367-399

Theory of Multiple Polynomial Remainder Sequence†)

By

Tateaki SASAKI* and Akio FURUKAWA**

Abstract

Given a set of polynomials $\{P_0^{(1)}(x), \ldots, P_0^{(m)}(x)\}$, with coefficients in an integral domain I, we can generate a sequence of sets of remainders $\{P_i^{(1)}(x), \ldots, P_i^{(m)}(x)\}$, $i=1, 2, \ldots$, through $\beta_i^{(\mu)}P_{i+1}^{(\mu)}=\alpha_i^{(\mu)}P_i^{(\mu)}-Q_i^{(\mu)}P_i^{(\nu_i)}$, $\deg(P_{i+1}^{(\mu)})<\deg(P_i^{(\nu_i)})$, $\mu=1, \ldots, \nu_i-1, \nu_i+1, \ldots, m$, $\nu_i \in \{1, \ldots, m\}$, with $\alpha_i^{(\mu)}$, $\beta_i^{(\mu)} \in I$. We call the sequence of sets $\{P_i^{(1)}(x), \ldots, P_i^{(m)}(x)\}$, $i=1, 2, \ldots$, multiple polynomial remainder sequence (multi-PRS). This paper proves that, for each polynomial $P_i^{(\mu)}$, there exists a matrix $M_{i,j}^{(\mu)}$, $0 \leqq j<i$, such that $P_i^{(\mu)} \backsim |M_{i,j}^{(\mu)}|$, each nonzero element of the first column of $M_{i,j}^{(\mu)}$ is $x^l P_j^{(k)}$ with l a nonnegative integer and $k \in \{1, \ldots, m\}$, and each of the other nonzero elements is a coefficient of $P_j^{(k)}$. Furthermore, three algorithms for calculating multi-PRS over I are given.

§ 1. Introduction

Let $F(x)$, $G(x)$, and $H(x)$ be polynomials of degrees l, m, n, respectively, over an integral domain I such as the ring of integers or multivariate polynomials:

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

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

$$H(x) = h_n x^n + h_{n-1}x^{n-1} + \ldots + h_0, \quad h_i \in I. \tag{1.3}$$

Using F and G with $l \geqq m$, we can generate a *polynomial remainder sequence*, or *PRS* in short, $(P_1, P_2, \ldots, P_k \neq 0, P_{k+1}=0)$, by successively calculating remainders through the following formulas:

$$P_1(x)=F(x), \quad P_2(x)=G(x),$$
$$\beta_i P_{i+1}=\alpha_i P_{i-1}-Q_i P_i, \quad \deg(P_{i+1})<\deg(P_i), \quad i=2, 3, \ldots, k, \tag{1.4}$$

where α_i, $\beta_i \in I$, and deg denotes the degree w. r. t. x.

Communicated by S. Hitotumatu, March 19, 1983.

* The Institute of Physical and Chemical Research, Wako-shi, Saitama 351, Japan.

** Department of Mathematics, Tokyo Metropolitan University, Setagaya-ku, Tokyo 158, Japan.

†) Work supported in part by The Kurata Foundation.

For many years, mathematicians know that each polynomial in the PRS $\{P_1, P_2, \ldots, P_k\}$ can be represented in a determinant form, i.e., $P_i \sim |M_i|$, where the matrix M_i is composed of F, G, and their coefficients, and "$\sim$" denotes *similarity*, that is $A \sim B$ if $aA = bB$ for some nonzero a, $b \in I$. Since the PRS plays an important role in computer algebra, Collins,[1,2] Brown and Traub,[3] and Brown[4] investigated the matrix M_i in details, and developed the so-called subresultant theory. According to their theory, M_i is given by

$$(1.5)\qquad M_i = \begin{pmatrix} x^0F & f_{j+1} & \cdots & & f_{l-1} & f_l & & & \\ x^1F & f_j & \cdots & & & f_{l-1} & f_l & & \\ \vdots & & & & & & & & \\ x^{m-j-1}F & f_{2j+2-m} & \cdots & & & & & f_{l-1} & f_l \\ x^0G & g_{j+1} & \cdots & g_{m-1} & g_m & & & & \\ x^1G & g_j & \cdots & & g_{m-1} & g_m & & & \\ \vdots & & & & & & & & \\ x^{l-j-1}G & g_{2j+2-l} & \cdots & & & & & g_{m-1} & g_m \end{pmatrix},$$

with $j = \deg(P_i)$ or $j = \deg(P_{i-1}) - 1$.

The determinants of M_i, $i = 3, 4, \ldots, k$, are called *subresultants*. This name originates from that the determinant of (1.5) with $j = 0$ is Sylvester's determinant representing the resultant. Based on the subresultant theory, the above authors constructed efficient algorithms for calculating PRS over I.

In a previous paper,[5] the present authors introduced a concept of secondary-PRS and extended the subresultant theory. Using the PRS $\{P_1, P_2, \ldots, P_k\}$ and H, we can generate a polynomial remainder sequence $\{\tilde{P}_1, \tilde{P}_2, \ldots\}$ through formulas

$$(1.6)\qquad \begin{aligned} &\tilde{P}_1 = H, \\ &\tilde{\beta}_i \tilde{P}_i = \tilde{\alpha}_i \tilde{P}_{i-1} - \tilde{Q}_i P_i, \ \deg(\tilde{P}_i) < \deg(P_i), \\ &\quad i = 2, 3, \ldots, k \text{ if } \deg(P_k) > 0, \ i = 2, 3, \ldots, k-1 \text{ if } \deg(P_k) = 0, \end{aligned}$$

where $\tilde{\alpha}_i$, $\tilde{\beta}_i \in I$. In deriving the sequence $\{\tilde{P}_1, \tilde{P}_2, \ldots\}$, the PRS $\{P_1, P_2, \ldots\}$ is used as a set of divisor polynomials and it is called *main-PRS*. On the other hand, the sequence $\{\tilde{P}_1, \tilde{P}_2, \ldots\}$ is obtained as a by-product of the main-PRS. Hence, the sequence was named *secondary-PRS*. For each polynomial $\tilde{P}_i$ in the secondary-PRS, there exists a matrix $\tilde{M}_i$ satisfying $\tilde{P}_i \sim |\tilde{M}_i|$. In fact, for $l \geqq n$, such an $\tilde{M}_i$

is given by

$$\tilde{M}_i = \begin{pmatrix} x^0F & f_j & \cdot & \cdot & \cdot & \cdot & f_{l-1} & f_l & & & \\ x^1F & f_{j-1} & \cdot & \cdot & \cdot & \cdot & \cdot & f_{l-1} & f_l & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ x^{m-j-1}F & f_{2j+1-m} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & f_{l-1} & f_l & \\ x^0G & g_j & \cdot & \cdot & \cdot & g_{m-1} & g_m & & & & \\ x^1G & g_{j-1} & \cdot & \cdot & \cdot & \cdot & g_{m-1} & g_m & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ x^{l-j-1}G & g_{2j+1-l} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & g_{m-1} & g_m & \\ x^0H & h_j & \cdot & \cdot & h_{n-1} & h_n & & & & & \end{pmatrix}, \tag{1.7}$$

with $j=\deg(P_i)$.

This paper generalizes the concepts of PRS and secondary-PRS to multi-PRS and extends the subresultant theory further. Suppose we have a set of m polynomials

$$\{P_0^{(1)}(x),\ P_0^{(2)}(x),\ \ldots,\ P_0^{(m)}(x)\},\quad m\geqq 2, \tag{1.8}$$

with coefficients in I. Treating these polynomials as starting polynomials, we can generate a sequence of sets of remainders

$$\{P_i^{(1)}(x),\ P_i^{(2)}(x),\ \ldots,\ P_i^{(m)}(x)\},\quad i=1,\ 2,\ \ldots,\ i_{\max}, \tag{1.9}$$

through the following formulas:

$$\begin{cases} \nu_i\in\{1,\ 2,\ \ldots,\ m\}, \\ \beta_i^{(\mu)}P_{i+1}^{(\mu)}=\alpha_i^{(\mu)}P_i^{(\mu)}-Q_i^{(\mu)}P_i^{(\nu_i)},\ \deg(P_{i+1}^{(\mu)})<\deg(P_i^{(\nu_i)}), \\ \qquad \text{for } \mu \text{ such that } \deg(P_i^{(\mu)})\geqq\deg(P_i^{(\nu_i)}),\quad \mu\neq\nu_i, \\ \beta_i^{(\mu)}P_{i+1}^{(\mu)}=\alpha_i^{(\mu)}P_i^{(\mu)} \\ \qquad \text{for } \mu \text{ such that } \deg(P_i^{(\mu)})<\deg(P_i^{(\nu_i)}), \\ \alpha_i^{(\mu)},\ \beta_i^{(\mu)}\in I, \\ P_{i+1}^{(\nu_i)}=P_i^{(\nu_i)} \text{ or } \alpha_i^{(\nu_i)}=\beta_i^{(\nu_i)}=1. \end{cases} \tag{1.10}$$

That is, the $(i+1)$st set of remainders $\{P_{i+1}^{(1)},\ P_{i+1}^{(2)},\ \ldots,\ P_{i+1}^{(m)}\}$ is generated by choosing the divisor polynomial $P_i^{(\nu_i)}$ arbitrarily. It is easy to see that the conventional PRS can be formulated as a special case of multi-PRS with starting polynomials $\{F,\ G\}$. Furthermore, the secondary-PRS is also a special case of three-PRS with $\nu_i\in\{1,\ 2\}$.

As a generalization of matrices M_i and $\tilde{M}_i$, we prove the existence of matrices $M_{i,j}^{(\mu)}$, $\mu=1,\ 2,\ \ldots,\ m$, $j=0,\ 1,\ \ldots,\ i-1$, such that

(1.11) $$P_i^{(\mu)} \sim |M_{i,j}^{(\mu)}| \quad \text{or} \quad P_i^{(\mu)} = \lambda_{i,j}^{(\mu)} |M_{i,j}^{(\mu)}|,$$

where $M_{i,j}^{(\mu)}$ is composed of $P_j^{(k)}(x)$, $k=1, 2, \ldots, m$, and their coefficients, just as M_i and $\tilde{M}_i$ are composed of F, G, H, and their coefficients. Furthermore, we derive several algorithms for calculating multi-PRS over I.

§ 2. PRS-Matrix

In this section, we define terminology, introduce notations, and specify main properties of the matrix $M_{i,j}^{(\mu)}$ which we call a *PRS-matrix*.

The coefficient of the highest degree term of a polynomial $P(x)$ is called *leading coefficient* and abbreviated to $\mathrm{lc}(P)$. For example, $\mathrm{lc}(F)=f_l$. The sets of starting polynomials and ith remainders in multi-PRS are denoted by $\{P_0^{(1)}(x), P_0^{(2)}(x), \ldots, P_0^{(m)}(x)\}$ and $\{P_i^{(1)}(x), P_i^{(2)}(x), \ldots, P_i^{(m)}(x)\}$, respectively, as in §1. The degree and the leading coefficient of the ith remainder $P_i^{(\mu)}$ are denoted by $n_i^{(\mu)}$ and $c_i^{(\mu)}$, respectively:

(2.1) $$n_i^{(\mu)} = \deg(P_i^{(\mu)}),$$

(2.2) $$c_i^{(\mu)} = \mathrm{lc}(P_i^{(\mu)}).$$

The divisor polynomial in the calculation of the $(i+1)$ st remainders is denoted by $P_i^{(\nu_i)}$, as in §1. The sequence $(P_0^{(\mu)}, P_1^{(\mu)}, \ldots, P_{i_{\max}}^{(\mu)})$ is *normal* if

(2.3) $$n_{i+1}^{(\mu)} = n_i^{(\nu_i)} - 1 \quad \text{for } i=0, 1, \ldots, i_{\max}-1,$$

otherwise the sequence is *abnormal*. The degree difference between $P_i^{(\mu)}$ and $P_i^{(\nu_i)}$ is denoted by $d_i^{(\mu)}$:

(2.4) $$d_i^{(\mu)} = \deg(P_i^{(\mu)}) - \deg(P_i^{(\nu_i)}).$$

When the polynomial remainder is calculated by the conventional division, the remainder is in general not in $I[x]$ but in $(I/I)[x]$. In order to make the remainder be in $I[x]$, we perform the pseudo-division instead of the division. (The pseudo-division of F and G is the division of $\mathrm{lc}(G)^{\deg(F)-\deg(G)+1} \cdot F$ and G.) The resulting remainder is called *pseudo-remainder* and abbreviated to *prem*. The coefficient of the term of degree k in $P_i(x)$ is denoted by $P_{i,k}$:

$$P_i(x) = P_{i,n}x^n + P_{i,n-1}x^{n-1} + \ldots + P_{i,0}.$$

We introduce notation "[ ]" to describe equations in (1.10) concisely:

$$[P_i^{(\mu)},\ P_i^{(\nu_i)}] \equiv \alpha_i^{(\mu)} P_i^{(\mu)} - Q_i^{(\mu)} P_i^{(\nu_i)},\quad \mu = 1,\ 2,\ \ldots,\ m, \tag{2.5}$$
$$(\text{if } n_i^{(\mu)} < n_i^{(\nu_i)} \text{ then } Q_i^{(\mu)} = 0).$$

Thus, if $\alpha = \mathrm{lc}(G)^{\deg(F)-\deg(G)+1}$ then $[F,\ G] = \mathrm{prem}(F,\ G)$. The coefficient of the term of degree k in $[F,\ G]$ is denoted by $[F,\ G]_k$.

Now, let us specify the PRS-matrix $M_{i,j}^{(\mu)}$ by defining terminology for the PRS-matrices.

Property 1. Each row of $M_{i,j}^{(\mu)}$ is composed of one of the polynomials $P_j^{(k)}$, $k = 1,\ 2,\ \ldots,\ m$, and its coefficients.

Type of a row: A row composed of $P_j^{(k)}$ and its coefficients is called of type $P_j^{(k)}$, or of type k in short.

Property 2. The leftmost element of a row of type $P_j^{(k)}$ in $M_{i,j}^{(\mu)}$ is either 0 or $x^l P_j^{(k)}$ with l a nonnegative integer. Each of the other elements of the row is either 0 or a coefficient of $P_j^{(k)}$.

Property 3. All rows of the same type are arranged sequentially.

We can visually understand the above properties by observing matrix M_i or $\tilde{M}_i$ given in §1. In discussing PRS-matrices in general, we are necessary to introduce a concept of block.

C-block: Except for the leftmost column, all other columns of $M_{i,j}^{(\mu)}$ are divided into nonoverlapping blocks called C-blocks. Each C-block is composed of a set of sequential columns (see Fig. 1).

R-block: All rows of $M_{i,j}^{(\mu)}$ are divided into nonoverlapping blocks called R-blocks. Each R-block is composed of a set of sequential rows of the same type (see Fig. 1).

Block: The largest submatrix contained in both a C-block and an R-block is called a block (see Fig. 1).

Type of a block/R-block: A block or R-block composed of rows of type k is called of type k.

According to the above definitions, all the elements that are in the second to the last columns of $M_{i,j}^{(\mu)}$ are divided into nonoverlapping blocks. We specify the blocks further.

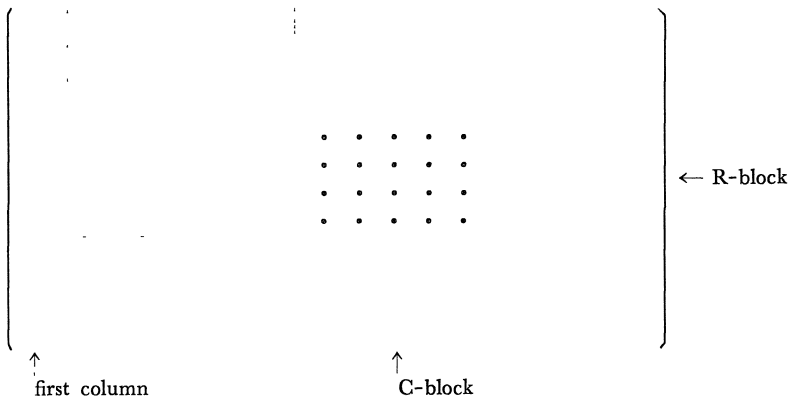


Fig. 1. Blocking of a matrix.
The dotted area shows a block.

Predecessor block: Among blocks in each R-block, the nonnull leftmost block is called a predecessor block (see Fig. 3).

Successor block: In each R-block, blocks which are at the right of the predecessor block are called successor blocks (see Fig. 3).

Property 4. An element in the leftmost column is nonzero only if the element is in an R-block which contains a predecessor block in the first C-block.

Property 5. Each block is either a null matrix or a matrix of the form illustrated by Fig. 2. Any predecessor block contains only nonnull rows.

Note that the nonzero rightmost element in any row is the leading coefficient.

Index of a nonnull row in a block: Let the leftmost element of the row be the coefficient of a term of degree k. (If there is no such term, we virtually assume the existence of the term.) Then, the row is called of index k. (For example, the rows in Fig. 2 are of indices $\bar{l}, \bar{l}-1, \ldots, \check{l}$.)

Normal rows, abnormal rows: There are two kinds of rows, normal and abnormal. In each block containing both normal and abnormal rows, the index of any abnormal row is greater than those of normal rows. (Abnormal rows can appear only when some PRSs are abnormal.) Detailed definitions of these terms are given in §3.

Index of a nonnull block: Among the normal rows in the block, let the nonnull topmost row be of index k. If the block contains no normal row, then let the nonnull bottommost abnormal row be of

$$\begin{pmatrix} f_{\bar{l}} & f_{\bar{l}+1} & \cdots & f_l & & & 0 & \cdots & 0 \\ f_{\bar{l}-1} & f_{\bar{l}} & \cdots & \cdots & f_l & & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{\bar{l}} & f_{\bar{l}+1} & \cdots & \cdots & \cdots & f_l & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & & & & & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & \cdots & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & & & 0 & \cdots & 0 \\ f_l & & & 0 & \cdots & 0 \\ \cdots & \cdots & & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{\bar{l}} & \cdots & f_l & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \cdots & 0 \\ \cdots & & & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

Fig. 2. Structure of a nonnull block.

A row composed of only 0 elements is called null. A block composed of only null rows is called null. The bottommost null rows and rightmost null columns may be vacuous. The topmost row is null only when the index of the row exceeds the degree (i. e. l in this figure). Any predecessor block does not contain null row.

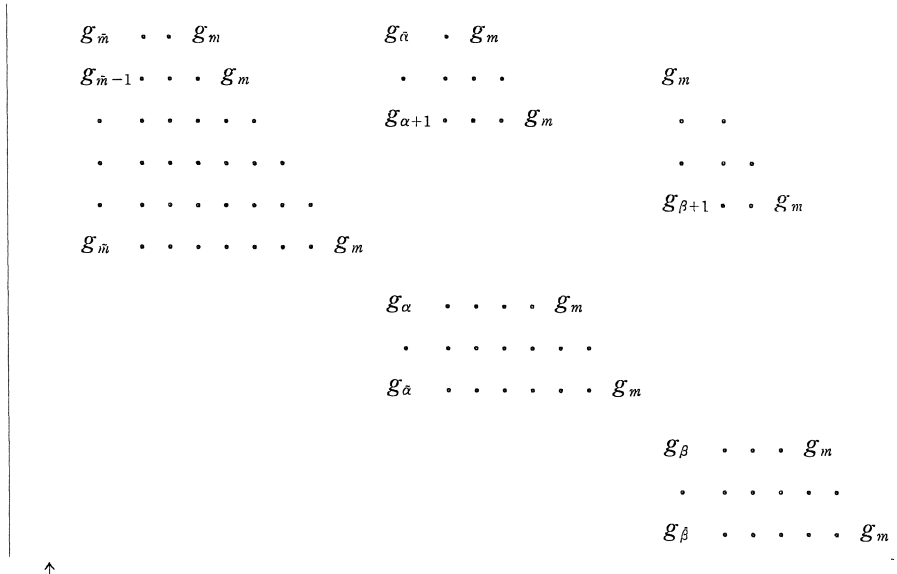


Fig. 3. Structure of R-blocks of the same type.

Three R-blocks are shown which contain three predecessor blocks (diagonal blocks) and two successor blocks (off-diagonal blocks). Note that, in each C-block, the indices of rows decrease continuously from the successor block to the predecessor bock.

index $k+1$. Then the block is called of index k.

Property 6. In each C-block, all predecessor blocks are of the same index while their types are different from each other.

Property 7. In each C-block, the index of the nonnull bottommost row in any successor block is the same as that in other successor block, and the index is one larger than the index of predecessor blocks in the C-block. (That is, combining a successor block and a predecessor block of the same type in a C-block, we obtain a larger block of the form illustrated by Fig. 3.)

Figure 3 illustrates the structure of R-blocks of the same type.

We define quantities specifying the $M_{i,j}^{(\mu)}$:

$L(\mu, i, j)$: The number of C-blocks in $M_{i,j}^{(\mu)}$. In §5, $L(\mu, i+1, j+1)$ and $L(\mu, i+1, j)$ are represented simply as L and L', respectively.

$N[l]_{i,j}^{(\mu)}(k)$: The number of normal rows in the predecessor block of type k in the lth C-block in $M_{i,j}^{(\mu)}$.

$A[l]_{i,j}^{(\mu)}(k)$: The number of abnormal rows in the predecessor block of type k in the lth C-block in $M_{i,j}^{(\mu)}$.

$N_{i,j}^{(\mu)}$: The order of matrix $M_{i,j}^{(\mu)}$.

By definition of predecessor blocks and property 6, we have

$$N_{i,j}^{(\mu)} = \sum_{k=1}^{m} \sum_{l=1}^{L(\mu,i,j)} \{N[l]_{i,j}^{(\mu)}(k) + A[l]_{i,j}^{(\mu)}(k)\}. \tag{2.6}$$

§ 3. Inverse-Reduction of PRS-Matrix

The inverse-reduction is an inverse operation of the well-known procedure of reducing determinants, and it is crucial for analyzing multi-PRS. This section explains the inverse-reduction of PRS-matrix by examples and define the procedure.

We first explain the reduction of PRS-matrix by considering the matrix M_i given in (1.5). Suppose that polynomials defined by (1.1), (1.2) and (1.3) satisfy the relation $H=F-QG$, $\deg(H) < \deg(G) \leqq \deg(F)$. Then, applying a procedure described in ref. 3 or 5, we can rewrite (1.5) as

$$(3.1)\qquad |M_i| = \begin{vmatrix} x^0H & h_{j+1} & \cdot & \cdot & h_{n-1} & h_n & & & & & & \\ x^1H & h_j & \cdot & \cdot & \cdot & h_{n-1} & h_n & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & \\ x^{m-j-1}H & h_{2j+2-m} & \cdot & \cdot & \cdot & \cdot & h_{n-1} & h_n & 0 & \cdot & 0 & \\ x^0G & g_{j+1} & \cdot & \cdot & \cdot & g_{m-1} & g_m & & & & & \\ x^1G & g_j & \cdot & \cdot & \cdot & \cdot & g_{m-1} & g_m & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ x^{l-j-1}G & g_{2j+2-l} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & g_{m-1} & g_m \end{vmatrix}.$$

When $j<n$, we can reduce the above matrix as

$$(3.1')\qquad |M_i| = g_m^{l-n} \begin{vmatrix} x^0H & h_{j+1} & \cdot & \cdot & h_{n-1} & h_n & & & & & \\ x^1H & h_j & \cdot & \cdot & \cdot & h_{n-1} & h_n & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ x^{m-j-1}H & h_{2j+2-m} & \cdot & \cdot & \cdot & \cdot & \cdot & h_{n-1} & h_n & \\ x^0G & g_{j+1} & \cdot & \cdot & \cdot & g_{m-1} & g_m & & & \\ x^1G & g_j & \cdot & \cdot & \cdot & \cdot & g_{m-1} & g_m & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ x^{n-j-1}G & g_{2j+2-n} & \cdot & \cdot & \cdot & \cdot & \cdot & g_{m-1} & g_m \end{vmatrix}.$$

Denoting the matrix in (3. 1′) by $M_{i,1}$, we see that $M_{i,1}$ is a PRS-matrix satisfying $P_i \sim |M_i| \sim |M_{i,1}|$. Compared with M_i, the order of $M_{i,1}$ is reduced by $l-n$. Hence, we call the above procedure the reduction of a PRS-matrix. Note that the reduction is nothing but a successive application of Gaussian elimination.

In the above reduction, the number of rows of type G is reduced. Conversely, if we add suitable rows of type G to $M_{i,1}$, we can transform the matrix $M_{i,1}$ to M_i, i. e., to another PRS-matrix of higher order. We call this procedure the inverse-reduction of PRS-matrix. We use this term not only for a PRS-matrix but also for a row in a PRS-matrix. Considering the reduction procedure, we may specify the inverse-reduction by the following rules:

Rule 1. *The inverse-reduction of a PRS-matrix* $M_{i,j+1}^{(\mu)}$ *to* $M_{i,j}^{(\mu)}$ *adds only rows of type* $P_j^{(\nu_j)}$ *to* $M_{i,j+1}^{(\mu)}$, *and it does not change the numbers of rows of other types.*

Rule 2. *The inverse-reduction does not change the indices of all rows contained in* $M^{(\mu)}_{i,j+1}$.

Rule 3. *Let* F, G, H *be polynomials defined by* (1.1)—(1.3), *with* $l \geqq m > n$, *and let* $H=[F, G]$. *Then, inverse-reduction of* $(h_{\bar{m}}, \ldots, h_n, 0, \ldots, 0)$, *a row of length* $\eta+1$, *to* $(f_{\bar{m}}, \ldots, f_n, \ldots, f_{\bar{m}+\eta}, \ldots, f_l)$ *requires* $l-(\bar{m}+\eta)$ *rows of type* G *and of indices* $m-\eta-1$, $m-\eta-2$, $\ldots$, $\bar{m}-l+m$. (See Fig. 4.)

It should be noted that, in Fig. 4, only rows of type G and of indices $\bar{m}$, $\bar{m}-1, \ldots, \bar{m}-l+m$ are necessary to reduce the row of type F to that of type H. The other rows of type G, i. e., rows of indices $m-\eta-1$, $m-\eta-2, \ldots, \bar{m}+1$ are used to reduce the number of zero elements in the reduced row of type H. Thus, we have two kinds of rows which we call normal and abnormal:

Normal rows and abnormal rows. The PRS-matrices $M^{(\mu)}_{i+1,i}$, $\mu=1, 2, \ldots, m$, $i=0, 1, \ldots, i_{\max}-1$, contain only normal rows. The rows which are necessary to reduce only the size of PRS-matrix without elimination of its element or to inverse-reduce only abnormal rows are abnormal.

InFig. 4, rows of type G and of indices $m-\eta-1$, $m-\eta-2, \ldots, \bar{m}+1$ are abnormal. The abnormal rows do not appear frequently in the PRS-matrices; they can appear only when more than one sequence of multi-PRS is abnormal (see §4).

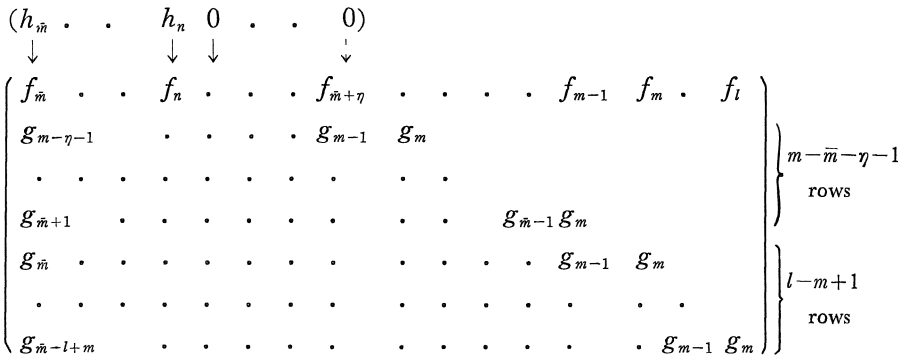


Fig. 4. Illustration of the inverse-reduction.

The row $(h_{\bar{m}} \ldots h_n\ 0 \ldots 0)$ of horizontal size $\eta+1$ is inverse-reduced to $(f_{\bar{m}} \ldots f_n \ldots f_{\bar{m}+\eta} \ldots f_l)$ by adding rows of type G, where $H=[F, G]$. It should be noted that the upper $m-\bar{m}-\eta-1$ rows of type G are used to reduce the number of 0 elements of the row of type H and they are not used to eliminate elements of the row of type F.

Matrices M_i, $M_{i,1}$, or $\tilde{M}_i$ are composed of only predecessor C-blocks and they contain no successor block. In order to show the necessity of successor blocks, we present an example of multi-PRS, where we set $[A, B]=\mathrm{prem}(A, B)$ and

$$(3.2)\qquad \{P_0^{(1)}, P_0^{(2)}, P_0^{(3)}\}\equiv\{F_0=F,\ G_0=G,\ H_0=H\},\quad \deg(F_0)=l=n+1,\ \deg(G_0)=m=n.$$

Choosing G_0 as the first divisor, we have

$$(3.3)\qquad F_1\equiv\mathrm{prem}(F_0, G_0)=\begin{vmatrix} F & f_n & f_{n+1} \\ G & g_n & \\ xG & g_{n-1} & g_n \end{vmatrix},\quad \deg(F_1)=n-1,$$

$$(3.4)\qquad G_1\equiv G_0,\ \deg(G_1)=n,$$

$$(3.5)\qquad H_1\equiv\mathrm{prem}(H_0, G_0)=\begin{vmatrix} H & h_n \\ G & g_n \end{vmatrix},\quad \deg(H_1)=n-1.$$

Choosing F_1 as the second divisor, we obtain

$$(3.6)\qquad F_2\equiv F_1,\ \deg(F_2)=n-1,$$

$$(3.7)\qquad G_2\equiv\mathrm{prem}(G_1, F_1)/\mathrm{lc}(G_0)^2=\begin{vmatrix} F & f_{n-1} & f_n & f_{n+1} & \\ xF & f_{n-2} & f_{n-1} & f_n & f_{n+1} \\ G & g_{n-1} & g_n & & \\ xG & g_{n-2} & g_{n-1} & g_n & \\ x^2G & g_{n-3} & g_{n-2} & g_{n-1} & g_n \end{vmatrix},\quad \deg(G_2)=n-2,$$

$$(3.8)\qquad H_2\equiv\mathrm{prem}(H_1, F_1)/\mathrm{lc}(G_0)=\begin{vmatrix} F & f_{n-1} & f_n & f_{n+1} \\ G & g_{n-1} & g_n & \\ xG & g_{n-2} & g_{n-1} & g_n \\ H & h_{n-1} & h_n & \end{vmatrix},\quad \deg(H_2)=n-2,$$

Choosing H_2 as the next divisor, we can calculate G_3 easily as

$$(3.9)\qquad G_3\equiv\mathrm{prem}(G_2, H_2)/\mathrm{lc}(F_1)=\begin{vmatrix} F & f_{n-2} & f_{n-1} & f_n & f_{n+1} & \\ xF & f_{n-3} & f_{n-2} & f_{n-1} & f_n & f_{n+1} \\ G & g_{n-2} & g_{n-1} & g_n & & \\ xG & g_{n-3} & g_{n-2} & g_{n-1} & g_n & \\ x^2G & g_{n-4} & g_{n-3} & g_{n-2} & g_{n-1} & g_n \\ H & h_{n-2} & h_{n-1} & h_n & & \end{vmatrix}.$$

In order to represent F_3 by a PRS-matrix, we are necessary to introduce successor blocks as

(3.10) $F_3 \equiv \mathrm{prem}(F_2, H_2)/\mathrm{lc}(F_1)$

$$= \begin{vmatrix} F & f_{n-2} & f_{n-1} & f_n & f_{n+1} & & f_n & f_{n+1} \\ xF & f_{n-3} & f_{n-2} & f_{n-1} & f_n & f_{n+1} & & \\ G & g_{n-2} & g_{n-1} & g_n & & & g_n & \\ xG & g_{n-3} & g_{n-2} & g_{n-1} & g_n & & & \\ x^2G & g_{n-4} & g_{n-3} & g_{n-2} & g_{n-1} & g_n & & \\ 0 & & & & & & g_{n-1} & g_n \\ H & h_{n-2} & h_{n-1} & h_n & & & h_n & \\ xH & h_{n-3} & h_{n-2} & h_{n-1} & h_n & & & \end{vmatrix}.$$

This matrix contains three successor blocks. The rows of type G are divided into two R-blocks, each of them contains a predecessor block. We can check that all Properties 1—7 presented in §2 are satisfied by the above matrix.

The matrix in (3.10) is quite complicated. However, such a complicated PRS-matrix can be derived rather easily by the inverse-reduction. In the inverse-reduction, F_3, for example, is represented first by a PRS-matrix composed of F_2 and H_2. Next, the matrix is transformed so that its elements are represented in terms of F_1 and H_1. Finally, we derive a PRS-matrix composed of F_0, G_0, and H_0. We trace this procedure explicitly.

Since the degrees of F_2 and H_2 are $n-1$ and $n-2$, respectively, $\tilde{F}_3 \equiv \mathrm{prem}(F_2, H_2)$ can be written as

(3.11) $$\tilde{F}_3 = \begin{vmatrix} F_2 & F_{2,n-2} & F_{2,n-1} \\ H_2 & H_{2,n-2} & \\ xH_2 & H_{2,n-3} & H_{2,n-2} \end{vmatrix}.$$

Using (3.6) and (3.8), we can rewrite (3.11) as

(3.12) $$\tilde{F}_3 = \frac{1}{\mathrm{lc}(G_0)^2} \begin{vmatrix} F_1 & F_{1,n-2} & F_{1,n-1} \\ [H_1, F_1] & [H_1, F_1]_{n-2} & \\ x[H_1, F_1] & [H_1, F_1]_{n-3} & [H_1, F_1]_{n-2} \end{vmatrix}.$$

Since $\deg(H_1) = \deg(F_1) = n-1$, we add one row of type F to the above matrix:

(3.13) $\tilde{F}_3 = \{1/\mathrm{lc}(G_0)^2 \mathrm{lc}(F_1)\}$

$$\times \begin{vmatrix} F_1 & F_{1,n-2} & F_{1,n-1} & \\ xF_1 & F_{1,n-3} & F_{1,n-2} & F_{1,n-1} \\ [H_1, F_1] & [H_1, F_1]_{n-2} & & \\ x[H_1, F_1] & [H_1, F_1]_{n-3} & [H_1, F_1]_{n-2} & \end{vmatrix}.$$

This form of matrix is ready to inverse-reduce to give

$$\text{(3.14)} \quad \tilde{F}_3 = \frac{\mathrm{lc}(F_1)}{\mathrm{lc}(G_0)^2} \begin{vmatrix} F_1 & F_{1,n-2} & F_{1,n-1} & \\ xF_1 & F_{1,n-3} & F_{1,n-2} & F_{1,n-1} \\ H_1 & H_{1,n-2} & H_{1,n-1} & \\ xH_1 & H_{1,n-3} & H_{1,n-2} & H_{1,n-1} \end{vmatrix}.$$

We continue the inverse-reduction. Using (3.3) and (3.5), we can rewrite (3.14) as

$$\text{(3.15)} \quad \tilde{F}_3 = \{\mathrm{lc}(F_1)/\mathrm{lc}(G_0)^2\} \times \begin{vmatrix} [F_0, G_0] & [F_0, G_0]_{n-2} & [F_0, G_0]_{n-1} & \\ x[F_0, G_0] & [F_0, G_0]_{n-3} & [F_0, G_0]_{n-2} & [F_0, G_0]_{n-1} \\ [H_0, G_0] & [H_0, G_0]_{n-2} & [H_0, G_0]_{n-1} & \\ x[H_0, G_0] & [H_0, G_0]_{n-3} & [H_0, G_0]_{n-2} & [H_0, G_0]_{n-1} \end{vmatrix}.$$

Since $\deg(F_0) = n+1$ and $\deg(G_0) = \deg(H_0) = n$, we must add the following three rows of type G_0 to the above matrix:

$$\begin{bmatrix} G_0 & G_{0,n-2} & G_{0,n-1} & G_{0,n} & & & G_{0,n} \\ xG_0 & G_{0,n-3} & G_{0,n-2} & G_{0,n-1} & G_{0,n} & & \\ x^2G_0 & G_{0,n-4} & G_{0,n-3} & G_{0,n-2} & G_{0,n-1} & G_{0,n} & \end{bmatrix} / (G_{0,n})^3.$$

Note that the first row of this matrix contains two $G_{0,n}$ elements. The reason is as follows: The order of the matrix in (3.15) is 4, and three rows are added. Hence, the order of resulting matrix is 7 and each row to be added must contain $G_{0,n}$ in one of the 5th to 7th columns. With the addition of three rows of type G_0, (3.15) can be transformed to

$$\text{(3.16)} \quad \tilde{F}_3 = \mathrm{lc}(F_1) g_n \times \begin{vmatrix} F & f_{n-2} & f_{n-1} & f_n & f_{n+1} & & f'_n \\ xF & f_{n-3} & f_{n-2} & f_{n-1} & f_n & f_{n+1} & \\ G & g_{n-2} & g_{n-1} & g_n & & & g_n \\ xG & g_{n-3} & g_{n-2} & g_{n-1} & g_n & & \\ x^2G & g_{n-4} & g_{n-3} & g_{n-2} & g_{n-1} & g_n & \\ H & h_{n-2} & h_{n-1} & h_n & & & h_n \\ xH & h_{n-3} & h_{n-2} & h_{n-1} & h_n & & \end{vmatrix},$$

with

$$f'_n = \begin{vmatrix} f_n & f_{n+1} \\ g_{n-1} & g_n \end{vmatrix} / g_n.$$

The matrix in (3.16) is not a PRS-matrix because it contains an element which is not linear in the coefficients of F and G. Linearizing the above matrix by introducing a row which has nonzero elements only in the second C-block, and dividing (3.16) by the factor $\mathrm{lc}(F_1)$, we obtain (3.10).

Eqs. (3.7)—(3.10) show that calculation of multi-PRS by pseudo-division introduces extraneous factors to the remainder polynomials. The extraneous factors are leading coefficients of divisor polynomials, and by eliminating them, we can calculate multi-PRS efficiently. Analysis of the extraneous factors is one of the main purposes of this paper.

In the following, we describe an outline of the inverse-reduction procedure algorithmically. The details of the algorithm as well as the proof of existence of PRS-matrices satisfying Properties 1—7 are given in the next section.

Procedure INVERSE-REDUCTION (*outline*)

Input : A set of polynomials $\{P_0^{(1)}(x), \ldots, P_0^{(m)}(x)\}$;

Output : PRS-matrices $\{M_{i,0}^{(1)}, \ldots, M_{i,0}^{(m)}\}$, $i=1, 2, \ldots, i_{\max}$;

For $i \leftarrow 0$ to $i_{\max}-1$ do [iteration on $i \geqq 0$]

For $\mu \leftarrow 1$ to m with $\mu \neq \nu_i$ do begin

Step 1: Represent $\tilde{P}_{i+1}^{(\mu)} \equiv \beta_i^{(\mu)} P_{i+1}^{(\mu)} \equiv [P_i^{(\mu)}, P_i^{(\nu_i)}]$ in the determinant form as (3.11) and let the determinant be $|M_{i+1,i}^{(\mu)}|$;

Step 2: [Iteration on $j \geqq 0$]

For $j \leftarrow i-1$ to 0 step -1 do begin

Step 2.1: [Here, $\tilde{P}_{i+1}^{(\mu)}$ is represented by $M_{i+1,j+1}^{(\mu)}$.]

For every $k \neq \nu_j$ and $r=0, 1, 2, \ldots$, replace $P_{j+1}^{(k)}$ and $P_{j+1,r}^{(k)}$ in $M_{i+1,j+1}^{(\mu)}$ by $[P_j^{(k)}, P_j^{(\nu_j)}]$ and $[P_j^{(k)}, P_j^{(\nu_j)}]_r$, respectively;

Step 2.2: Add normal rows of type $P_j^{(\nu_j)}$ to the matrix obtained in Step 2.1 so that all the normal rows may be inverse-reduced; [New C-blocks and R-blocks may be created.]

Step 2.3: Add abnormal rows of type $P_j^{(\nu_j)}$ to the matrix obtained in Step 2.2, similarly; [New R-blocks may be created.]

Step 2.4: Represent the matrix in terms of $P_j^{(k)}$ and $P_{j,r}^{(k)}$; [The elements $[P_j^{(k)}, P_j^{(\nu_j)}]$ and $[P_j^{(k)}, P_j^{(\nu_j)}]_r$ in the matrix are replaced by $P_j^{(k)}$ and $P_{j,r}^{(k)}$, respectively.]

Step 2.5: If the matrix obtained in Step 2.4 contains elements which are nonlinear in the coefficients of $P_j^{(k)}$, linearize the matrix by adding rows of type $P_j^{(\nu_j)}$; [Here, we have $M_{i+1,j}^{(\mu)}$.]

end;

Step 3: $P_{i+1}^{(\mu)} \leftarrow \tilde{P}_{i+1}^{(\mu)} / \beta_i^{(\mu)}$;

end;

§ 4. Existence of PRS-Matrix

Although we have stated much about the matrix $M_{i,j}^{(\mu)}$, we have not proved even the existence of $M_{i,j}^{(\mu)}$ yet. This section gives a constructive proof of the following theorem:

Theorem 1. *For any multi-PRS* $\{P_i^{(1)}, \ldots, P_i^{(m)}\}$, $i=1, 2, \ldots, i_{\max}$, *there exist PRS-matrices* $M_{i,j}^{(\mu)}$ *satisfying* (1.11) *and Properties* 1—7.

Proof. The proof goes parallelly with a detailed analysis of each step of the inverse-reduction procedure presented in §3.

Step 1. We recall the well-known determinant representation for the pseudo-remainder:

$$\text{(4.1)}\qquad \operatorname{prem}(F, G) = \begin{vmatrix} x^0F & f_m & f_{m+1} & \cdot & \cdot & \cdot & f_l \\ x^0G & g_m & & & & & \\ x^1G & g_{m-1} & g_m & & & & \\ \cdot & \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ x^{l-m}G & g_{2m-l} & \cdot & \cdot & \cdot & g_{m-1}\, g_m & \end{vmatrix},$$

where F and G are defined by (1.1) and (1.2), respectively, with $l \geqq m$. Using (4.1), we can easily perform the Step 1. As the first

step of iteration on i, let the matrix representing $\mathrm{prem}(P_0^{(\mu)}, P_0^{(\nu_0)})$ be $M_{1,0}^{(\mu)}$. Note that, if $n_0^{(\mu)} < n_0^{(\nu_0)}$, $M_{1,0}^{(\mu)}$ is a matrix of order 1, i. e., $M_{1,0}^{(\mu)} = (P_0^{(\mu)})$. When $n_0^{(\mu)} \geqq n_0^{(\nu_0)}$, the $M_{1,0}^{(\mu)}$ contains only one C-block and two R-blocks, and all blocks contained in $M_{1,0}^{(\mu)}$ are predecessor blocks. The $M_{1,0}^{(\mu)}$ satisfies Properties 1—7 obviously, and

$$L(\mu,\ 1,\ 0) = 1, \tag{4.2}$$

$$N[1]_{1,0}^{(\mu)}(k) = \begin{cases} 1 & \text{if } k = \mu, \\ n_0^{(\mu)} - n_0^{(\nu_0)} + 1 & \text{if } k = \nu_0 \text{ and } n_0^{(\mu)} \geqq n_0^{(\nu_0)}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.3}$$

$$A[1]_{1,0}^{(\mu)}(k) = 0, \quad k = 1,\ 2,\ \ldots,\ m. \tag{4.4}$$

As the assumption for iteration on $i \geqq 2$, assume that we have determined $P_{i'}^{(\mu)}$ and $M_{i',j}^{(\mu)}$, $\mu = 1, 2, \ldots, m$, $j' = i' - 1, i' - 2, \ldots, 0$, $i' = 1, 2, \ldots, i$, which satisfy Properties 1—7. Then, we have the values of $L(\mu, i', j')$, $N[l]_{i',j'}^{(\mu)}(k)$, $A[l]_{i',j'}^{(\mu)}(k)$, $k = 1, 2, \ldots, m$, $l = 1, \ldots, L(\mu, i', j')$. Upon this assumption, we will construct $M_{i+1,j}^{(\mu)}$, $j = i, i-1, \ldots, 0$, successively.

We first represent $\tilde{P}_{i+1}^{(\mu)} \equiv [P_i^{(\mu)}, P_i^{(\nu_i)}]$ by a determinant using (4.1). Let the matrix representing $\mathrm{prem}(P_i^{(\mu)}, P_i^{(\nu_i)})$ be $M_{i+1,i}^{(\mu)}$. Then, $M_{i+1,i}^{(\mu)}$ is a PRS-matrix. Similarly to $M_{1,0}^{(\mu)}$, the $M_{i+1,i}^{(\mu)}$ is specified as

$$L(\mu,\ i+1,\ i) = 1, \tag{4.5}$$

$$N[1]_{i+1,i}^{(\mu)}(k) = \begin{cases} 1 & \text{if } k = \mu, \\ n_i^{(\mu)} - n_i^{(\nu_i)} + 1 & \text{if } k = \nu_i \text{ and } n_i^{(\mu)} \geqq n_i^{(\nu_i)}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.6}$$

$$A[1]_{i+1,i}^{(\mu)}(k) = 0, \quad k = 1,\ 2,\ \ldots,\ m. \tag{4.7}$$

Step 2. As the assumption for iteration on j, assume that we have determined $M_{i+1,j'}^{(\mu)}$ $\mu = 1, 2, \ldots, m$, $j' = i, i-1, \ldots, j+1$, which satisfy Properties 1—7. Then, we have the values of $L(\mu, i+1, j')$, $N[l]_{i+1,j'}^{(\mu)}(k)$, $A[l]_{i+1,j'}^{(\mu)}(k)$, $k = 1, 2, \ldots, m$, $l = 1, \ldots, L(\mu, i+1, j')$.

Step 2. 1. The $M_{i+1,j+1}^{(\mu)}$ is composed of $P_{j+1}^{(k)}$, $k = 1, 2, \ldots, m$, and their coefficients. By the assumption for iteration on i, we have $P_{j+1}^{(k)}$, $P_j^{(k)}$, $P_j^{(\nu_j)}$ and $\beta_j^{(k)}$ such that

$$P_{j+1}^{(k)} = [P_j^{(k)}, P_j^{(\nu_j)}] / \beta_j^{(k)}, \quad k \neq \nu_j, \tag{4.8}$$

$$P_{j+1}^{(\nu_j)} = P_j^{(\nu_j)}. \tag{4.9}$$

Hence, it is trivial to replace $P_{j+1}^{(k)}$ and $P_{j+1}^{(\nu_j)}$ in the matrix $M_{i+1,j+1}^{(\mu)}$ by

(4. 8) and (4. 9), respectively.

Step 2. 2. We first consider the inverse-reduction of all nonnull blocks in the first C-block. These nonnull blocks are predecessor blocks, and $M^{(\mu)}_{i+1,j+1}$ contains $N[1]^{(\mu)}_{i+1,j+1}(k)$ normal rows of type k in the first C-block. Since only rows of type ν_j are added by the inverse-reduction from $M^{(\mu)}_{i+1,j+1}$ to $M^{(\mu)}_{i+1,j}$, we have

$$N[1]^{(\mu)}_{i+1,j}(k)=N[1]^{(\mu)}_{i+1,j+1}(k),\quad k\neq\nu_j. \tag{4. 10}$$

Addition of normal rows to the first C-block is necessary only when the $M^{(\mu)}_{i+1,j+1}$ contains rows of type k such that $n_j^{(k)}\geqq n_j^{(\nu_j)}$. According to Property 6, the predecessor blocks in the first C-block are of the same index, say $\bar{n}$. If $N[1]^{(\mu)}_{i+1,j+1}(\nu_j)\neq 0$, we add rows of type ν_j to the existing predecessor block in such a way that Property 5 is satisfied. If $N[1]^{(\mu)}_{i+1,j+1}(\nu_j)=0$, we create a new predecessor block of type ν_j and of index $\bar{n}$ in the first C-block. Anyway, according to Rule 3 in §2 (see also Fig. 5), inverse-reduction of the normal rows of type k in the first C-block requires $N[1]^{(\mu)}_{i+1,j+1}(k)+n_j^{(k)}-n_j^{(\nu_j)}$ normal rows of type ν_j and of indices $\bar{n}$, $\bar{n}-1,\ldots$. Hence,

$$\begin{aligned}N[1]^{(\mu)}_{i+1,j}(\nu_j)=\max_k\{&N[1]^{(\mu)}_{i+1,j+1}(k)+n_j^{(k)}-n_j^{(\nu_j)}\mid\\ &N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0,\ n_j^{(k)}\geqq n_j^{(\nu_j)},\ k\neq\nu_j\}.\end{aligned} \tag{4. 11}$$

As a result, every column in the first C-block contains at least one coefficient of $P_j^{(\nu_j)}$, and the horizontal size of the first C-block in $M^{(\mu)}_{i+1,j}$ is given by

$$N[1]^{(\mu)}_{i+1,j}(\nu_j)+n_j^{(\nu_j)}-\bar{n}.$$

For such k that $N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0$ and $n_j^{(k)}<n_j^{(\nu_j)}$, we have $n_{j+1}^{(k)}=n_j^{(k)}$, and

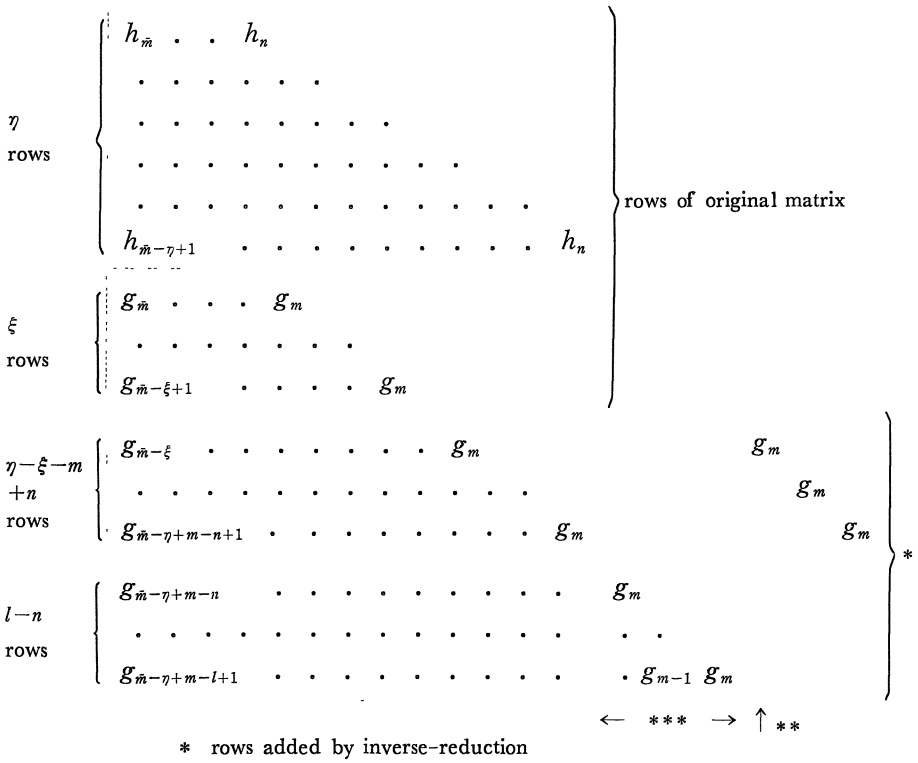
$$\begin{aligned}N[1]^{(\mu)}_{i+1,j+1}(k)+n_j^{(k)}-\bar{n}&=N[1]^{(\mu)}_{i+1,j+1}(k)+n_{j+1}^{(k)}-\bar{n}\\ &\leqq(\text{horizontal size of the first C-block in } M^{(\mu)}_{i+1,j+1})\\ &\leqq(\text{horizontal size of the first C-block in } M^{(\mu)}_{i+1,j})\\ &=N[1]^{(\mu)}_{i+1,j}(\nu_j)+n_j^{(\nu_j)}-\bar{n}.\end{aligned}$$

Therefore, we can delete the condition $n_j^{(k)}\geqq n_j^{(\nu_j)}$ in (4. 11). Furthermore, since $N[1]^{(\mu)}_{i+1,j}(\nu_j)\geqq N[1]^{(\mu)}_{i+1,j+1}(\nu_j)$, we may delete the condition $k\neq\nu_j$ in (4. 11). Thus, we can rewrite (4. 11) as

$$\begin{aligned}&N[1]^{(\mu)}_{i+1,j}(\nu_j)\\ &\quad=\max_k\{N[1]^{(\mu)}_{i+1,j+1}(k)+d_j^{(k)}\mid N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0\}.\end{aligned} \tag{4. 11′}$$

Eqs. (4. 10) and (4. 11′) are recurrence formulas for $N[1]^{(\mu)}_{i+1,j}(k)$, $k=1, \ldots, m$.

Corresponding to the addition of rows, we add $x^k P_j^{(\nu_j)}$, $k=N[1]^{(\mu)}_{i+1,j+1}(\nu_j), \ldots, N[1]^{(\mu)}_{i+1,j}(\nu_j)-1$, to the first column of the matrix so that Property 4 may be satisfied.



* rows added by inverse-reduction
** each column constitutes a new C-block
*** horizontal size of C-block is increased by $l-n$

Fig. 5. Addition of normal rows.
In order to inverse-reduce η rows of type H to those of type F, we are necessary to add $\eta-\xi+l-m$ rows of type G (rows marked with *). Among these, $l-n$ rows are used to increase the horizontal size of the C-block (columns marked with ***). Hence, if $\eta-\xi-m+l>l-n$, the other $\eta-\xi-m+n$ rows create new C-blocks (columns marked with **).

We consider the addition of normal rows in details by referring to Fig. 5. The increase of horizontal size of the first C-block by the inverse-reduction from $M^{(\mu)}_{i+1,j+1}$ to $M^{(\mu)}_{i+1,j}$ is given by

$$N[1]^{(\mu)}_{i+1,j}(\nu_j)+n_j^{(\nu_j)} - \max_k \{N[1]^{(\mu)}_{i+1,j+1}(k)+n^{(k)}_{j+1} \mid N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0\} \tag{4. 12}$$

$$(4.12') \qquad = N[1]^{(\mu)}_{i+1,j}(\nu_j) + n_j^{(\nu_j)} - N[1]^{(\mu)}_{i+1,j+1}(\nu_{j+1}) - n_{j+1}^{(\nu_{j+1})}$$
if $M^{(\mu)}_{i+1,j+1}$ contains rows of type ν_{j+1}.

On the other hand, the number of normal rows to be added by the inverse-reduction of the first C-block is

$$(4.13) \qquad N[1]^{(\mu)}_{i+1,j}(\nu_j) - N[1]^{(\mu)}_{i+1,j+1}(\nu_j).$$

If (4.13) is greater than (4.12), we must create new C-blocks as illustrated by Fig. 5. The number of C-blocks to be created by the inverse-reduction of the first C-block is given by

$$(4.14) \qquad \delta L[1](\mu,\ i+1,\ j) \equiv (4.13) - (4.12)$$
$$= \max_k \{N[1]^{(\mu)}_{i+1,j+1}(k) + n^{(k)}_{j+1} \mid N[1]^{(\mu)}_{i+1,j+1}(k) \neq 0\}$$
$$- \{N[1]^{(\mu)}_{i+1,j+1}(\nu_j) + n_j^{(\nu_j)}\}$$

$$(4.14') \qquad = N[1]^{(\mu)}_{i+1,j+1}(\nu_{j+1}) - N[1]^{(\mu)}_{i+1,j+1}(\nu_j) - d^{(\nu_j)}_{j+1}$$
if $M^{(\mu)}_{i+1,j+1}$ contains rows of type ν_{j+1},

where we have used the relation $n_j^{(\nu_j)} = n^{(\nu_j)}_{j+1}$.

Suppose we have added necessary normal rows to the 1st, 2nd, ..., $(l-1)$th C-blocks, and next consider the inverse-reduction of the normal rows in the lth C-block. Similarly to (4.10), we have

$$(4.15) \qquad N[l]^{(\mu)}_{i+1,j}(k) = N[l]^{(\mu)}_{i+1,j+1}(k),\ \ k \neq \nu_j.$$

Note that all the predecessor blocks in the lth C-block are of the same index, say $\bar{n}$, and these blocks are irrelevant to the inverse-reduction of the 1st, ..., $(l-1)$th C-blocks. Hence, similarly to (4.11), the number of normal rows in the predecessor block of type ν_j in $M^{(\mu)}_{i+1,j}$ is given by

$$(4.16) \qquad N[l]^{(\mu)}_{i+1,j}(\nu_j)$$
$$= \max_k \{N[l]^{(\mu)}_{i+1,j+1}(k) + d^{(k)}_j \mid N[1]^{(\mu)}_{i+1,j+1}(k) \neq 0\}.$$

Note the condition on k in this formula. Even if the lth C-block of $M^{(\mu)}_{i+1,j+1}$ contains no predecessor block, i.e., if $N[l]^{(\mu)}_{i+1,j+1}(k) = 0$ for every k, we must create a predecessor block of type ν_j in $M^{(\mu)}_{i+1,j}$ if $M^{(\mu)}_{i+1,j+1}$ contains rows of type k such that $d^{(k)}_j = n^{(k)}_j - n_j^{(\nu_j)} > 0$. This is to inverse-reduce the rows in successor blocks. That is, the index k in (4.16) runs over all values such that $N[1]^{(\mu)}_{i+1,j+1}(k) \neq 0$.

Eqs. (4.15) and (4.16) are recurrence formulas for $N[l]^{(\mu)}_{i+1,j}(\nu_j)$. We see that (4.10) and (4.11') are included in (4.15) and (4.16), respectively.

The rows added above are of indices $\bar{n}$, $\bar{n}-1, \ldots$, and these rows are not enough to inverse-reduce all successor blocks in the lth C-block. According to Properties 6 and 7, the nonnull bottommost rows in these successor blocks are of the same index $\bar{n}+1$. Hence, the inverse-reduction of all the successor blocks in the lth C-block requires normal rows of indices $\bar{n}+1$, $\bar{n}+2, \ldots$, as well. Thus, if successor blocks of type ν_j are null, we add normal rows of indices $\bar{n}+1$, $\bar{n}+2, \ldots$ to the successor blocks in such a way that Property 7 is satisfied (cf. Fig. 6).

Similarly to (4.14), we define $\delta L[l](\mu, i+1, j)$ as follows:

$$\begin{aligned}(4.17)\qquad &\delta L[l](\mu, i+1, j)\\ &\equiv \max_k \{N[l]^{(\mu)}_{i+1,j+1}(k)+n^{(k)}_{j+1} \mid N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0\}\\ &\qquad -\{N[l]^{(\mu)}_{i+1,j+1}(\nu_j)+n^{(\nu_j)}_{j}\}\end{aligned}$$

$$\begin{aligned}(4.17')\qquad &= N[l]^{(\mu)}_{i+1,j+1}(\nu_{j+1})-N[l]^{(\mu)}_{i+1,j+1}(\nu_j)-d^{(\nu_j)}_{j+1}\\ &\qquad \text{if } M^{(\mu)}_{i+1,j+1} \text{ contains rows of type } \nu_{j+1}.\end{aligned}$$

If $\delta L[l](\mu, i+1, j)>0$, new C-blocks are created by the inverse-reduction of normal rows of the lth C-block in $M^{(\mu)}_{i+1,j+1}$.

Step 2. 3. We have seen above that, if $\delta L[l](\mu, i+1, j)>0$, we must create new C-blocks. On the other hand, if $\delta L[l](\mu, i+1, j)<0$, we must add abnormal rows as illustrated by Fig. 4. Let us first investigate the condition

$$(4.18)\qquad \delta L[l](\mu, i+1, j)<0.$$

Since $n^{(\nu_j)}_{j}=n^{(\nu_j)}_{j+1}$, (4.17) tells us that the above inequality never holds if $N[1]^{(\mu)}_{i+1,j+1}(\nu_j)\neq 0$. That is, abnormal rows can appear only when $M^{(\mu)}_{i+1,j+1}$ does not contain rows of type ν_j. Suppose $M^{(\mu)}_{i+1,j+1}$ contains no row of type ν_j, i.e., $N[l]^{(\mu)}_{i+1,j+1}(\nu_j)=0$, then (4.18) can be written as

$$\begin{aligned}(4.19)\qquad &n^{(\nu_j)}_{j}=n^{(\nu_j)}_{j+1}>\max_k \{N[l]^{(\mu)}_{i+1,j+1}(k)+n^{(k)}_{j+1} \mid N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0\}\\ &\qquad \geqq \max_k \{n^{(k)}_{j+1} \mid N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0\}+1.\end{aligned}$$

Therefore, abnormal rows can appear only when all PRSs contained in $M^{(\mu)}_{i+1,j+1}$ are abnormal.

By definition, $M^{(\mu)}_{i+1,i}$ contains no abnormal rows. Suppose that $M^{(\mu)}_{i+1,k}$, $k=i, \ldots, j'+1$, do not contain abnormal row while $M^{(\mu)}_{i+1,j'}$ does in the lth C-block. Then, the abnormal rows in $M^{(\mu)}_{i+1,j'}$ are of type $\nu_{j'}$ and

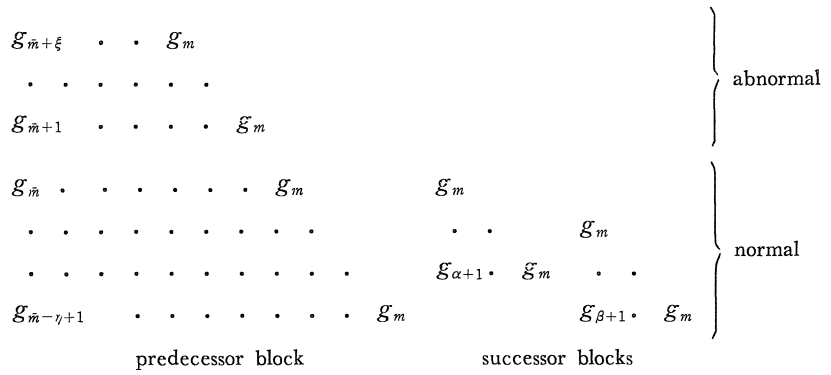


Fig. 6. Addition of abnormal rows.
Abnormal rows are added to the predecessor block of type G satisfying Property 5. Note that, when successor blocks are inverse-reduced as illustrated by Fig. 7, abnormal rows may appear in successor blocks.

$$A[l]^{(\mu)}_{i+1,j'}(k)=\begin{cases}-\delta L[l](\mu,\ i+1,\ j') & \text{if } k=\nu_{j'},\\ 0 & \text{otherwise.}\end{cases} \tag{4.20}$$

As we have seen above, $M^{(\mu)}_{i+1,j'+1}$ does not contain rows of type $\nu_{j'}$. Hence, we can add abnormal rows to the newly created predecessor block satisfying Property 5. Figure 6 illustrates the addition of abnormal rows.

Next, consider the case of $j<j'$, where $M^{(\mu)}_{i+1,j+1}$ contains abnormal rows in the lth C-block. In order to inverse-reduce $A[l]^{(\mu)}_{i+1,j+1}(k)$ abnormal rows of type k, we need the same number of abnormal rows and $n_j^{(k)}-n_j^{(\nu_j)}$ normal rows of type ν_i. The normal rows are already added in Step 2. 2. Hence, in order to inverse-reduce all abnormal rows in the lth C-block, we need

$$A[l]^{(\mu)}_{i+1,j}(\nu_j)=\max_k\{-\delta L[l](\mu,\ i+1,\ j),\ A[l]^{(\mu)}_{i+1,j+1}(k)\} \tag{4.21}$$

abnormal rows of type ν_j. We have added $-\delta L[l](\mu,\ i+1,\ j)$ term to (4.21) so that (4.21) includes (4.20) as a special case. On the other hand, the numbers of abnormal rows of types $k\neq\nu_j$ are unchanged:

$$A[l]^{(\mu)}_{i+1,j}(k)=A[l]^{(\mu)}_{i+1,j+1}(k),\quad k\neq\nu_j. \tag{4.22}$$

Eqs. (4.21) and (4.22) are recurrence formulas for $A[l]^{(\mu)}_{i+1,j}(k)$.

Step 2. 4. Now, we are ready to rewrite the matrix in terms of $P_j^{(k)}$ and $P_{j,r}^{(k)}$. For the blocks which are contained in $M^{(\mu)}_{i+1,j+1}$, the rewriting is easy: Figure 7 illustrates the rewriting. The rewriting is,

however, complicated in the C-blocks which were newly created in Step 2. 2. We explain the rewriting by taking up rows of type H in Fig. 5. We define the following quantities:

$$
(4.23)\quad \begin{cases} f'_{l-1} = \begin{vmatrix} f_{l-1} & f_l \\ g_{m-1} & g_m \end{vmatrix} / g_m, \\ f'_{l-2} = \begin{vmatrix} f_{l-2} & f_{l-1} & f_l \\ g_{m-1} & g_m & \\ g_{m-2} & g_{m-1} & g_m \end{vmatrix} / g_m^2, \\ \quad \vdots \\ f'_m = \begin{vmatrix} f_m & f_{m+1} & \cdots & f_l \\ g_{m-1} & g_m & & \\ \vdots & \vdots & & \\ g_{2m-l} & \cdots & \cdots & g_m \end{vmatrix} / g_m^{(l-m)}. \end{cases}
$$

Note that $g_m f'_{l-1}$, $g_m^2 f'_{l-2}, \ldots, g_m^{(l-m)} f'_m$ are the leading coefficients of polynomials which are obtained by eliminating, successively, lth, $(l-1)$th, ..., $(m+1)$st degree terms of F and G. For example,

$$g_m f'_{l-1} = \mathrm{lc}(g_m F - x^{l-m} f_l G).$$

Furthermore, we define

$$(4.23') \qquad f'_l = f_l, \quad f'_{l+1} = f'_{l+2} = \cdots = 0.$$

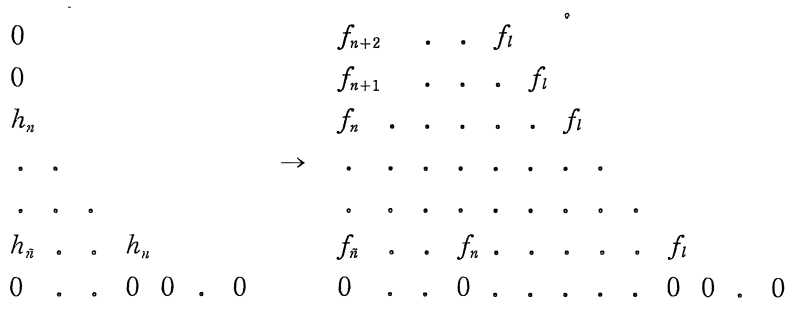


Fig. 7. Inverse-reduction of a successor block.
Rows of type H in a successor block are inverse-reduced to those of type F. (Some null block may become nonnull by the inverse-reduction.) The predecessor blocks of types other than ν_j are inverse-reduced similarly.

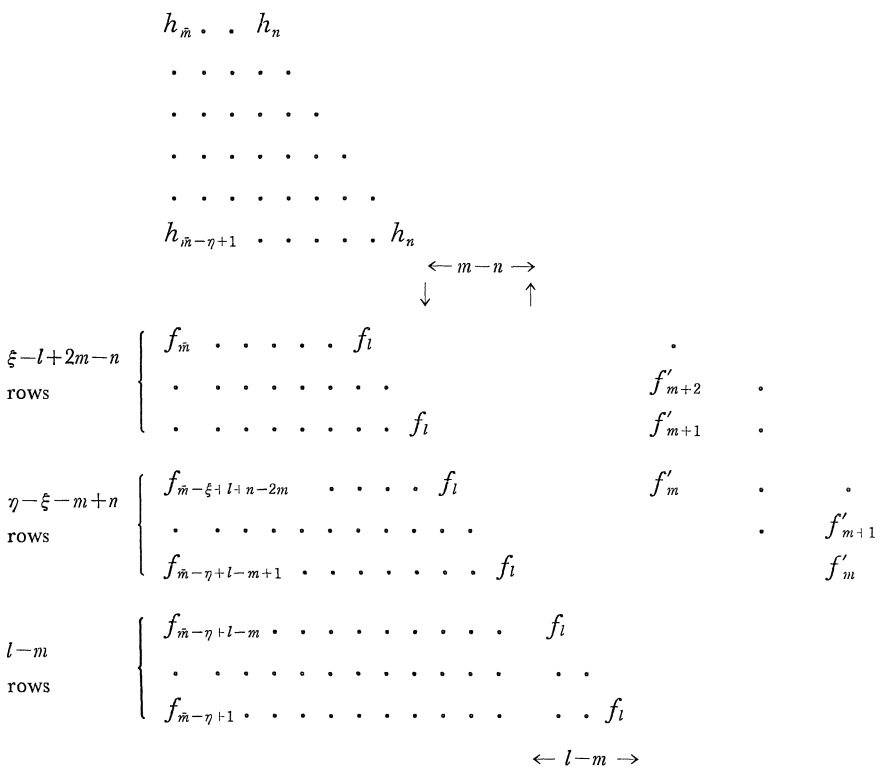


Fig. 8. Illustration of Step 2.4.
The rows of type H in Fig. 5 are replaced by rows of type F, where $H=[F, G]$. Note that nonlinear elements may appear in newly created C-blocks.

The rewriting of rows of type H in Fig. 5 is performed by adding elements f'_m, $f'_{m+1}, \ldots, f'_l$ to the newly created C-blocks as shown by Fig. 8.

Step 2.5. If $l=m$, the rightmost column, for example, of Fig. 8 contains only $f'_l=f_l$. If $l>m$, however, columns in Fig. 8 contains nonlinear elements and we have to linearize them. The linearization is performed by adding R-blocks of type G as shown by Fig. 9. Note that successor blocks of type F in Fig. 9 satisfy Property 5. After the linearization, the lth C-block, $L(\mu, i+1, j+1)<l\leqq L(\mu, i+1, j)$, in $M^{(\mu)}_{i+1,j}$ is characterized by

$$N[l]^{(\mu)}_{i+1,j}(\nu_j)=\max_k\{n^{(k)}_j-n^{(\nu_j)}_j \mid N[1]^{(\mu)}_{i+1,j+1}(k)\neq 0\}, \tag{4.24}$$

$$N[l]^{(\mu)}_{i+1,j}(k)=0, \quad k\neq\nu_j. \tag{4.25}$$

Eqs. (4.24) and (4.25) define the numbers of rows in the predecessor

blocks contained in the newly created C-blocks.

Now, in order to prove Theorem 1, we have only to show that the matrix $M^{(\mu)}_{i+1,j}$ obtained by the inverse-reduction procedure is a PRS-matrix, i.e., it satisfies the Properties 1—7. Properties 1—4 are obviously satisfied by $M^{(\mu)}_{i+1,j}$. Remembering the addition of normal rows to both predecessor blocks (see Fig. 5) and successor blocks (cf. Figs. 6 and 7), the addition of abnormal rows (see Fig. 6), and the process of linearization (see Fig. 9), we see that $M^{(\mu)}_{i+1,j}$ satisfies

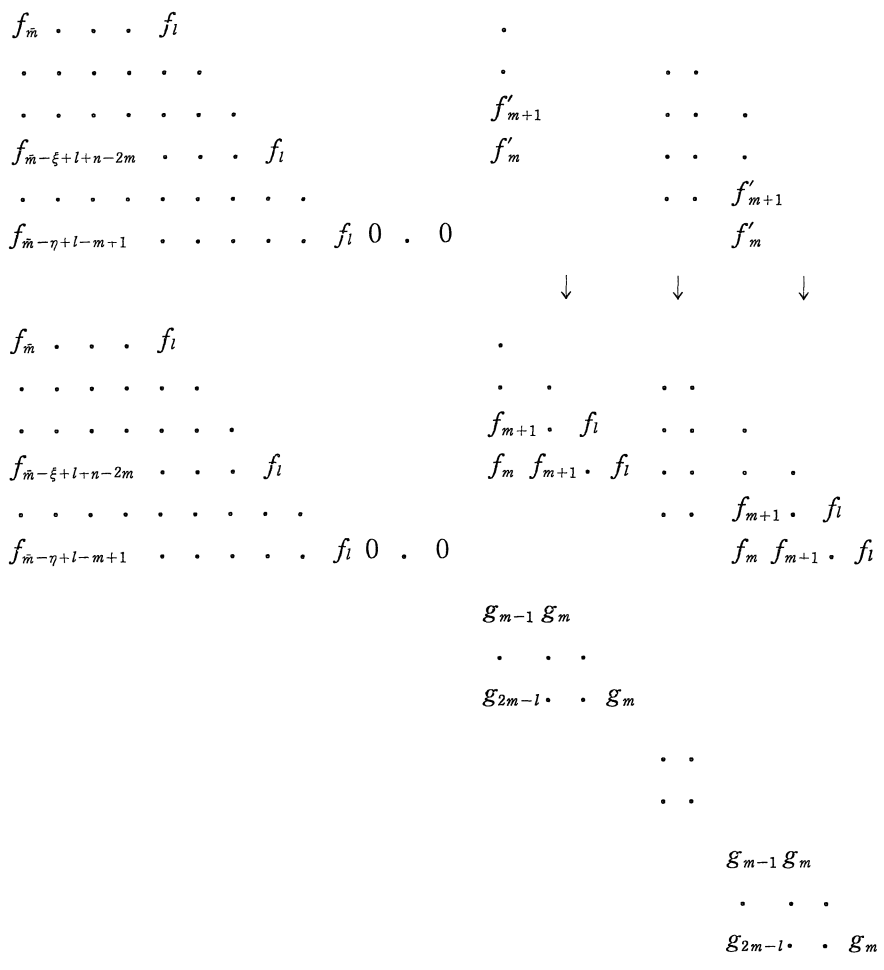


Fig. 9. Illustration of linearization.
The nonlinear elements of type F in Fig. 8 are linearized by adding predecessor blocks of type G. Note that each block satisfies Property 5. Note further that blocks of type G satisfy Property 7.

Property 5. In the inverse-reduction procedure, Steps 2. 2, 2. 3 and 2. 5 may create new predecessor blocks. Steps 2. 2 and 2. 3 can create a predecessor block in the lth C-block of $M^{(\mu)}_{i+1,j+1}$ only when the C-block contains no predecessor blocks of type ν_j. Step 2. 5 creats predecessor blocks in newly created C-blocks which contains only successor blocks. As we have explained, rows in these predecessor blocks are added so that Properties 6 and 7 are satisfied. Furthermore, successor blocks are inverse-reduced without in contradiction to Properties 6 and 7. Therefore, $M^{(\mu)}_{i+1,j}$ is a PRS-matrix.//

§ 5. Multi-PRS Algorithms

This section calculates the factor $\lambda^{(\mu)}_{i,0}$ defined in (1. 11) and derives several algorithms for calculating multi-PRS over I. Calculation of the factor $\lambda^{(\mu)}_{i,0}$ is performed easily by tracing the inverse-reduction procedure given in §3. We first calculate the factor which is introduced into $\lambda^{(\mu)}_{i+1,0}$ by the inverse-reduction from $M^{(\mu)}_{i+1,j+1}$ to $M^{(\mu)}_{i+1,j}$.

Step 1. Considering the definition of notation $[A, B]$ and the relation (4. 1), we obtain*)

$$\beta^{(\mu)}_i P^{(\mu)}_{i+1} = \{\alpha^{(\mu)}_i / (c_i^{(\nu_i)} \uparrow (d^{(\mu)}_i + 1))\} \cdot |M^{(\mu)}_{i+1,i}|. \tag{5. 1}$$

for such μ that $n^{(\mu)}_i \geqq n_i^{(\nu_i)}$ and $\mu \neq \nu_i$,

$$\beta^{(\mu)}_i P^{(\mu)}_{i+1} = \alpha^{(\mu)}_i P^{(\mu)}_i \equiv \alpha^{(\mu)}_i \cdot |M^{(\mu)}_{i+1,i}| \tag{5. 2}$$

for such μ that $n^{(\mu)}_i < n_i^{(\nu_i)}$.

Step 2. 1. Since $P^{(k)}_{j+1} = [P^{(k)}_j, P_j^{(\nu_j)}]/\beta^{(k)}_j$ for every $k \neq \nu_j$, and since $M^{(\mu)}_{i+1,j+1}$ contains $N[l]^{(\mu)}_{i+1,j+1}(k) + A[l]^{(\mu)}_{i+1,j+1}(k)$ rows of type k in the lth C-block, this step introduces the factor

$$\prod_{k=1}^{m} (1/\beta^{(k)}_j) \uparrow \sum_{l=1}^{L} \{N[l]^{(\mu)}_{i+1,j+1}(k) + A[l]^{(\mu)}_{i+1,j+1}(k)\}, \tag{5. 3}$$

with $L \equiv L(\mu, i+1, j+1)$,

into the r. h. s. of (5. 1) or (5. 2). Note that we have included the factor of $k = \nu_j$ to the product in (5. 3) because $\beta_j^{(\nu_j)} = 1$.

Step 2. 2. In this step, $N[l]^{(\mu)}_{i+1,j}(\nu_j) - N[l]^{(\mu)}_{i+1,j+1}(\nu_j)$ rows of type ν_j are added to the lth C-block of $M^{(\mu)}_{i+1,j+1}$. By adding a row of type ν_j, we must multiply the factor $1/c_j^{(\nu_j)}$. Hence, this step introduces the factor

*) For convenience of typography, we write $a \uparrow b$ instead of a^b in the following formulas.

$$(5.4)\qquad (1/c_j^{(\nu_j)}) \uparrow \sum_{l=1}^{L}\{N[l]^{(\mu)}_{i+1,j}(\nu_j) - N[l]^{(\mu)}_{i+1,j+1}(\nu_j)\}.$$

Step 2. 3. Similarly to Step 2. 2, this step introduces the factor

$$(5.5)\qquad (1/c_j^{(\nu_j)}) \uparrow \sum_{l=1}^{L}\{A[l]^{(\mu)}_{i+1,j}(\nu_j) - A[l]^{(\mu)}_{i+1,j+1}(\nu_j)\}.$$

Step 2. 4. By replacing $[P_j^{(k)}, P_j^{(\nu_j)}]$ in a row by $P_j^{(k)}$, we must multiply the factor $\alpha_j^{(k)}$ to the matrix. Hence, this step introduces the factor

$$(5.6)\qquad \prod_{k=1}^{m}(\alpha_j^{(k)}) \uparrow \sum_{l=1}^{L}\{N[l]^{(\mu)}_{i+1,j+1}(k) + A[l]^{(\mu)}_{i+1,j+1}(k)\},$$

where we have included the factor of $k=\nu_j$ to (5. 6) because $\alpha_j^{(\nu_j)}=1$.

Step 2. 5. The linearization step adds $N[l]^{(\mu)}_{i+1,j}(\nu_j)$ rows of type ν_j to the lth C-block for $l>L(\mu,\ i+1,\ j+1)$. Hence, this step introduces the factor

$$(5.7)\qquad (1/c_j^{(\nu_j)}) \uparrow \sum_{l=L+1}^{L'} N[l]^{(\mu)}_{i+1,j}(\nu_j),\ \text{with}\ L'\equiv L(\mu,\ i+1,\ j).$$

Summarizing the above results, the $j+1\to j$ iteration step introduces the factor

$$(5.8)\qquad [(1/c_j^{(\nu_j)}) \uparrow \sum_{l=1}^{L'}\{\delta N[l]^{(\mu)}_{i+1,j} + \delta A[l]^{(\mu)}_{i+1,j}\}]$$
$$\times \prod_{k=1}^{m}(\alpha_j^{(k)}/\beta_j^{(k)}) \uparrow \sum_{l=1}^{L}\{N[l]^{(\mu)}_{i+1,j+1}(k) + A[l]^{(\mu)}_{i+1,j+1}(k)\}$$

into the r. h. s. of (5. 1) or (5. 2), where

$$(5.9)\qquad \delta N[l]^{(\mu)}_{i+1,j} \equiv N[l]^{(\mu)}_{i+1,j}(\nu_j) - N[l]^{(\mu)}_{i+1,j+1}(\nu_j),$$

$$(5.10)\qquad \delta A[l]^{(\mu)}_{i+1,j} \equiv A[l]^{(\mu)}_{i+1,j}(\nu_j) - A[l]^{(\mu)}_{i+1,j+1}(\nu_j).$$

Note that, for such l that $L<l\leqq L'$, $N[l]^{(\mu)}_{i+1,j+1}(\nu_j)=0$ and $\delta A[l]^{(\mu)}_{i+1,j}=0$.

The above results give the following theorem.

Theorem 2. *Let* $n^{(\mu)}_{i+1}=n^{(\mu)}_{i'+1}$ *and* $n^{(\mu)}_{i'}\geqq n^{(\nu_{i'})}_{i'}$ *for* $i'\leqq i$, *i.e.*, $P^{(\mu)}_{i+1}\sim\cdots\sim P^{(\mu)}_{i'+1}\nsim P^{(\mu)}_{i'}$. *Then, when the PRS-matrix* $M^{(\mu)}_{i+1,j}$ *is constructed by the way described in* §4, *the* $\lambda^{(\mu)}_{i+1,j}$, $i\geqq 1$, *is given as*

$$(5.11)\qquad \lambda^{(\mu)}_{i+1,j} = \sigma\cdot\{\prod_{j'=i'+1}^{i}(\alpha^{(\mu)}_{j'}/\beta^{(\mu)}_{j'})\}\cdot(\beta^{(\mu)}_{i'})^{-1}\cdot\alpha^{(\mu)}_{i'}/((c_{i'}^{(\nu_{i'})}) \uparrow (d^{(\mu)}_{i'}+1))$$
$$\times \prod_{j'=i'-1}^{j}\Big\{(1/c_{j'}^{(\nu_{j'})}) \uparrow \sum_{l=1}^{L(\mu,i'+1,j')}\{\delta N[l]^{(\mu)}_{i'+1,j'} + \delta A^{(\mu)}_{i'+1,j'}\}$$
$$\times \prod_{k=1}^{m}(\alpha_{j'}^{(k)}/\beta_{j'}^{(k)}) \uparrow \sum_{l=1}^{L(\mu,i'+1,j'+1)}\{N[l]^{(\mu)}_{i'+1,j'+1}(k) + A[l]^{(\mu)}_{i'+1,j'+1}(k)\}\Big\},$$

where σ *is the sign factor, i.e.,*

(5. 12) $$\sigma=1 \text{ or } -1.$$

Proof. Representing P_{i+1} in terms of $M^{(\mu)}_{i'+1,i'}$ by using (5. 1) and (5. 2), and multiplying (5. 8) with $i=i'$ and $j=i'-1,\ i'-2,\ \ldots,\ i-1$ to the result, we obtain (5. 11) immediately. (Note that, even if $n_j^{(\mu)}<n_j^{(\nu_j)}$ for some $j<i'$, we must multiply (5. 8).)//

It should be commented that the number of PRS-matrices which are similar to $P_i^{(\mu)}$ is more than one in general. Such a case happens, for example, in an abnormal PRS (see (1. 5)).

Let us consider (5. 11) in the simplest case that

(5. 13) $$n_0^{(1)}\geqq n_0^{(2)},\quad \nu_{2j}=2 \text{ and } \nu_{2j+1}=1,\quad j=0,\ 1,\ 2,\ \ldots$$

Then, the sequence $(P_0^{(1)},\ P_0^{(2)},\ P_1^{(1)},\ P_2^{(2)},\ P_3^{(1)},\ P_4^{(2)},\ \ldots)$ constitutes a PRS and $(P_0^{(\mu)},\ P_1^{(\mu)},\ \ldots)$, with $\mu\geqq 3$, is a secondary-PRS. In this case, we can easily calculate $N[1]^{(\mu)}_{i+1,j}(k)$ from (4. 6), (4. 10) and (4. 11′). Let $\bar{\nu}_k=3-\nu_k$, $k=0,\ 1,\ \ldots$, that is, $\bar{\nu}_k=1$ if $\nu_k=2$ and $\bar{\nu}_k=2$ if $\nu_k=1$. Then $N[1]^{(\mu)}_{i+1,j}(k)$, $j\leqq i-1$, is given as

(5. 14) $$N[1]^{(\mu)}_{i+1,j}(k)=\begin{cases} d_i^{(\mu)}+d_{i-1}^{(\bar{\nu}_{i-1})}+\ldots+d_{j+1}^{(\bar{\nu}_{j+1})}+d_j^{(2)}+1, & k=1,\\ d_i^{(\mu)}+d_{i-1}^{(\bar{\nu}_{i-1})}+\ldots+d_{j+1}^{(\bar{\nu}_{j+1})}+d_j^{(1)}+1, & k=2,\\ 1, & k=\mu \text{ and } \mu\neq 1,\ 2,\\ 0, & \text{otherwise,}\end{cases}$$

where we have assumed that $n_i^{(\mu)}\geqq n_i^{(\nu_i)}$. (Note that $d_j^{(\nu_j)}=0$.) For example, when i is an even integer, or $\nu_i=2$ and $\nu_{i+1}=1$, we have

$$N[1]^{(1)}_{i+1,i}(k)=\begin{cases} 1, & k=1,\\ d_i^{(1)}+1, & k=2,\\ 0, & \text{otherwise,}\end{cases}$$

$$N[1]^{(1)}_{i+1,i-1}(k)=\begin{cases} d_i^{(1)}+d_{i-1}^{(2)}+1, & k=1,\\ d_i^{(1)}+1, & k=2,\\ 0, & \text{otherwise,}\end{cases}$$

$$N[1]^{(1)}_{i+1,i-2}(k)=\begin{cases} d_i^{(1)}+d_{i-1}^{(2)}+1, & k=1,\\ d_i^{(1)}+d_{i-1}^{(2)}+d_{i-2}^{(1)}+1, & k=2,\\ 0, & \text{otherwise.}\end{cases}$$

From (5. 14), we readily obtain (see (4. 17′) and note that $d_j^{(\nu_j)}=0$)

(5. 15) $$\delta L[1](\mu,\ i+1,\ j)=0,\quad \mu=1,\ 2,\ \ldots,\ m.$$

That is, the number of C-blocks in $M_{i+1,j}^{(\mu)}$ is one and we have neither successor block nor abnormal row in this case. Furthermore (5.9) gives us

$$\delta N[1]_{i+1,j}^{(\mu)} = d_{j+1}^{(\bar{\nu}_{j+1})} + d_j^{(\bar{\nu}_j)}. \tag{5.16}$$

Thus, remembering the relation $\alpha_j^{(\nu_j)} = \beta_j^{(\nu_j)} = 1$ (see (1.10)), we can rewrite (5.11) with $i \geqq 1$ and $\mu = \bar{\nu}_i = 1$ or 2 as

$$\begin{aligned}\lambda_{i+1,0}^{(\mu=\bar{\nu}_i)} &= \sigma \cdot (\beta_i^{(\bar{\nu}_i)})^{-1} \cdot \alpha_i^{(\bar{\nu}_i)} / ((c_i^{(\nu_i)}) \uparrow (d_i^{(\bar{\nu}_i)} + 1)) \\ &\times \prod_{j=i-1}^{0} \{[(1/c_j^{(\nu_j)}) \uparrow (d_{j+1}^{(\bar{\nu}_{j+1})} + d_j^{(\bar{\nu}_j)})] \cdot [(\alpha_j^{(\bar{\nu}_j)} / \beta_j^{(\bar{\nu}_j)}) \uparrow (n_j^{(\bar{\nu}_j)} - n_i^{(\nu_i)} + 1)]\}.\end{aligned} \tag{5.17}$$

This formula is the same as one of the fundamental formulas on PRS (see Eq. (29) in Ref. 3), which produces the reduced-PRS and the subresultant-PRS algorithms.

Similarly, for μ such that $\mu \geqq 3$ and $n_i^{(\mu)} \geqq n_i^{(\nu_i)}$, we obtain

$$\begin{aligned}\lambda_{i+1,0}^{(\mu \geqq 3)} &= \sigma \cdot (\beta_i^{(\mu)})^{-1} \cdot \alpha_i^{(\mu)} / ((c_i^{(\nu_i)}) \uparrow (d_i^{(\mu)} + 1)) \cdot \prod_{j=i-1}^{0} (\alpha_j^{(\mu)} / \beta_j^{(\mu)}) \\ &\times \prod_{j=i-1}^{0} \{[(1/c_j^{(\nu_j)}) \uparrow (d_{j+1}^{(\bar{\nu}_{j+1})} + d_j^{(\bar{\nu}_j)})] \\ &\qquad \cdot [(\alpha_j^{(\bar{\nu}_j)} / \beta_j^{(\bar{\nu}_j)}) \uparrow (n_j^{(\bar{\nu}_j)} - n_{i-1}^{(\nu_{i-1})} + d_i^{(\mu)} + 1)]\}.\end{aligned} \tag{5.18}$$

When the secondary-PRS $(P_0^{(\mu)}, P_1^{(\mu)}, \ldots)$ is normal, $n_i^{(\mu)} = n_{i-1}^{(\nu_{i-1})} - 1$ hence $n_j^{(\bar{\nu}_j)} - n_{i-1}^{(\nu_{i-1})} + d_i^{(\mu)} + 1 = n_j^{(\bar{\nu}_j)} - n_i^{(\nu_i)}$. Therefore, (5.18) is the same as a formula which the present authors obtained in Ref. 5 (Eq. (4.3)). However, in the case of abnormal secondary-PRS, (5.18) is different from Eq. (4.3) in Ref. 5. That is, the PRS-matrix obtained by the procedure described in §4 is different in general from the PRS-matrix for secondary-PRS presented in Ref. 5.

Now, let us return to (5.11) and rewrite it with $i' = i$ by assuming

$$\beta_0^{(k)} = 1, \quad k = 1, 2, \ldots, m. \tag{5.19}$$

This assumption is reasonable because the first remainder $P_1^{(k)}$ is not proportional to $\mathrm{lc}(P_0^{(\nu_0)})$ in general. Eqs. (4.15) and (4.16), (4.21) and (4.22), (4.24) and (4.25), (5.9) and (5.10) yield (note that $L' \geqq L$)

$$\begin{aligned}&\prod_{j=i-2}^{0} \prod_{k=1}^{m} (\alpha_j^{(k)}) \uparrow \textstyle\sum_{l=1}^{L} \{N[l]_{i+1,j+1}^{(\mu)}(k) + A[l]_{i+1,j+1}^{(\mu)}(k)\} \\ &= \prod_{j=i-1}^{1} \prod_{k=1}^{m} (\alpha_{j-1}^{(k)}) \uparrow \textstyle\sum_{l=1}^{L'} \{N[l]_{i+1,j}^{(\mu)}(k) + A[l]_{i+1,j}^{(\mu)}(k)\} \\ &= \left\{ \prod_{j=i-1}^{1} \prod_{k=1}^{m} (a_{j-1}^{(k)}) \uparrow \textstyle\sum_{l=1}^{L} \{N[l]_{i+1,j+1}^{(\mu)}(k) + A[l]_{i+1,j+1}^{(\mu)}(k)\} \right\}\end{aligned}$$

$$\times \prod_{j=i-2}^{0} (\alpha_j^{(\nu_{j+1})}) \uparrow \sum_{l=1}^{L} \{\delta N[l]_{i+1,j+1}^{(\mu)} + \delta A[l]_{i+1,j+1}^{(\mu)}\}.$$

Furthermore, (4.5)—(4.7) yield

$$\prod_{k=1}^{m} (\alpha_{i-1}^{(k)}) \uparrow \sum_{l=1}^{L} \{N[l]_{i+1,i}^{(\mu)}(k) + A[l]_{i+1,i}^{(\mu)}(k)\} = \alpha_{i-1}^{(\mu)} \cdot (\alpha_{i-1}^{(\nu_i)}) \uparrow (d_i^{(\mu)}+1).$$

Hence, extending (5.9) and (5.10) to the case of $j=i$ and defining as

$$\delta N[1]_{i+1,i}^{(\mu)} = d_i^{(\mu)} + 1, \tag{5.20}$$

$$\delta A[1]_{i+1,i}^{(\mu)} = 0, \tag{5.21}$$

we can rewrite (5.11) with $i'=i$, $j=0$, and $\mu \neq \nu_i$ as

$$\begin{aligned} \lambda_{i+1,0}^{(\mu \neq \nu_i)} = {} & \sigma \cdot (\alpha_{i-1}^{(\mu)} / \beta_i^{(\mu)}) \cdot \alpha_i^{(\mu)} / ((c_i^{(\nu_i)}) \uparrow (d_i^{(\mu)}+1)) \\ & \times \prod_{j=i-1}^{0} \Big\{ (1/c_j^{(\nu_j)}) \uparrow \sum_{l=1}^{L'} \{\delta N[l]_{i+1,j}^{(\mu)} + \delta A[l]_{i+1,j}^{(\mu)}\} \\ & \qquad \times (\alpha_j^{(\nu_{j+1})}) \uparrow \sum_{l=1}^{L} \{\delta N[l]_{i+1,j+1}^{(\mu)} + \delta A[l]_{i+1,j+1}^{(\mu)}\} \Big\} \\ & \times \prod_{j=i-1}^{1} \prod_{k=1}^{m} (\alpha_{j-1}^{(k)} / \beta_j^{(k)}) \uparrow \sum_{l=1}^{L} \{N[l]_{i+1,j+1}^{(\mu)}(k) + A[l]_{i+1,j+1}^{(\mu)}(k)\}. \end{aligned} \tag{5.22}$$

At the first glance, this formula seems to suggest the choice

$$\alpha_i^{(\mu)} = \beta_{i+1}^{(\mu)} = (c_i^{(\nu_i)}) \uparrow (d_i^{(\mu)}+1), \tag{5.23}$$

as a multi-PRS algorithm. This choice is the simplest generalization of Collins' reduced-PRS algorithm and it makes the formula (5.22) very simple. This choice, however, does not guarantee that $\lambda_{i+1,0}^{(\mu)} \in I$, because

$$\begin{aligned} & \sum_{l=1}^{L'} \{\delta N[l]_{i+1,j}^{(\mu)} + \delta A[l]_{i+1,j}^{(\mu)}\} \\ & \quad > \text{or} \leqq (d_j^{(\nu_{j+1})}+1) \cdot \sum_{l=1}^{L} \{\delta N[l]_{i+1,j+1}^{(\mu)} + \delta A[l]_{i+1,j+1}^{(\mu)}\}. \end{aligned}$$

We convince ourselves of this by the example we have presented in §3: we set $\alpha_1^{(G)} = (\mathrm{lc}(F_1))^2$ in the calculation of G_2, while $\mathrm{prem}(G_2, H_2) = \mathrm{lc}(F_1) \cdot G_3$ or $\beta_2^{(G)} = \alpha_1^{(G)} / \mathrm{lc}(F_1)$. In the following, we present three algorithms for calculating multi-PRS over I.

Algorithm 1. *We choose* $\alpha_i^{(\mu)}$ *and* $\beta_i^{(\mu)}$ *as*

$$\alpha_i^{(\mu)} = \begin{cases} (c_i^{(\nu_i)}) \uparrow (d_i^{(\mu)}+1) \cdot \tilde{\alpha}_i^{(\mu)}, & \text{if } n_i^{(\mu)} \geqq n_i^{(\nu_i)}, \\ 1, & \text{otherwise}, \end{cases} \tag{5.24}$$

$$\beta_i^{(\mu)} = \alpha_{i-1}^{(\mu)}, \quad i \geqq 1, \tag{5.25}$$

$$\tilde{\alpha}_0^{(\mu)} = \beta_0^{(\mu)} = 1, \quad \mu = 1, 2, \ldots, m, \tag{5.26}$$

where $\tilde{\alpha}_i^{(\mu)} \in I$ *is determined as small as possible.*

Suppose we have determined $\alpha_j^{(\mu)}$, $j=1,\ldots,i-1$, $\mu=1,\ldots,m$, in the calculation of $P_{j+1}^{(\mu)}$. Then, formulas (4.5)—(4.7), (4.15)—(4.17), (4.21) and (4.22), (4.24) and (4.25) allow us to calculate $L(\mu, i+1, j)$, $N[l]_{i+1,j}^{(\mu)}(k)$ and $A[l]_{i+1,j}^{(\mu)}(k)$, $k=1,\ldots,m$, $l=1,\ldots,L(\mu, i+1, j)$, $\mu=1,\ldots,m$, $j=0,\ldots,i$. Therefore, we can calculate the product factors in $\lambda_{i+1,0}^{(\mu)}$. The product factors in (5.22) can be written as

$$\begin{aligned}(5.27)\quad &\prod_{j=i-1}^{0}\Big\{(1/c_j^{(\nu_j)})\uparrow\sum_{l=1}^{L'}\{\delta N[l]_{i+1,j}^{(\mu)}+\delta A[l]_{i+1,j}^{(\mu)}\}\\ &\qquad\times(\alpha_j^{(\nu_{j+1})})\uparrow\sum_{l=1}^{L}\{\delta N[l]_{i+1,j+1}^{(\mu)}+\delta A[l]_{i+1,j+1}^{(\mu)}\}\Big\}\\ &\qquad\equiv\prod_{j=i-1}^{0}(c_j^{(\nu_j)})^{e(\mu,i+1,j)},\quad e(\mu,i+1,j)\text{ is an integer.}\end{aligned}$$

Hence, we determine $\tilde{\alpha}_i^{(\mu)}$ as

$$(5.28)\qquad \tilde{\alpha}_i^{(\mu)}=\prod_{j=i-1}^{0}(c_j^{(\nu_j)})^{\max\{0,-e(\mu,i+1,j)\}},$$

which makes $\lambda_{i+1,0}^{(\mu)}$ to be

$$(5.29)\qquad |\lambda_{i+1,0}^{(\mu)}|=\prod_{j=i-1}^{0}(c_j^{(\nu_j)})^{\max\{0,e(\mu,i+1,j)\}}.$$

After calculating $P_{i+1}^{(\mu)}$ by the formulas (1.10) and (5.24)—(5.28), we divide $P_{i+1}^{(\mu)}$ by (5.29) to get polynomial identical to $|M_{i+1,0}^{(\mu)}|$ up to the sign factor. Note that, in this algorithm, we need not calculate the product factors in (5.22) explicitly. We have only to calculate $e(\mu, i+1, j)$, $j=0,\ldots,i-1$, and $\tilde{\alpha}_i^{(\mu)}$. Elimination of the factor (5.29) from $P_{i+1}^{(\mu)}$ is done by removing each factor $(c_j^{(\nu_j)})^{\max\{0,e(\mu,i+1,j)\}}$ in (5.29) successively.

Algorithm 2. *We choose* $\alpha_i^{(\mu)}$ *as*

$$(5.30)\qquad \alpha_i^{(\mu)}=\begin{cases}(c_i^{(\nu_i)})\uparrow(d_i^{(\mu)}+1), & \text{if } n_i^{(\mu)}\geqq n_i^{(\nu_i)},\\ 1, & \text{otherwise,}\end{cases}$$

$\beta_i^{(\mu)}$ is determined so that $P_{i+1}^{(\mu)}=\sigma|M_{i+1,0}^{(\mu)}|$, *with*

$$(5.31)\qquad \beta_0^{(\mu)}=1,\quad \mu=1,\ldots,m.$$

Suppose we have determined $\beta_j^{(\mu)}$, $j=1,\ldots,i-1$, $\mu=1,\ldots,m$, in the calculation of $P_{j+1}^{(\mu)}$. Then, formulas (4.5)—(4.7), (4.15)—(4.17), (4.20)—(4.22), (4.24) and (4.25) allow us to calculate $L(\mu, i+1, j)$, $N[l]_{i+1,j}^{(\mu)}(k)$ and $A[l]_{i+1,j}^{(\mu)}(k)$, $k=1,\ldots,m$, $l=1,\ldots,L(\mu, i+1, j)$, $\mu=1,\ldots,m$, $j=0,\ldots,i$. That is, by representing (5.22) as

$$(5.32)\qquad \lambda_{i+1,0}^{(\mu)}=\sigma\cdot(\alpha_{i-1}^{(\mu)}/\beta_i^{(\mu)})\prod_{j=i-1}^{0}(c_j^{(\nu_j)})^{e(\mu,i+1,j)},$$

we can calculate $e(\mu, i+1, j)$, $j=0, \ldots, i-1$, $\mu=1, \ldots, m$. Therefore, we determine $\beta_i^{(\mu)}$ as

$$\beta_i^{(\mu)}=\alpha_{i-1}^{(\mu)} \prod_{j=i-1}^{0} (c_j^{(\nu_j)})^{e(\mu, i+1, j)}. \tag{5.33}$$

This choice makes $\lambda_{i+1,0}^{(\mu)}$ a sign factor, or

$$P_{i+1}^{(\mu)}=\sigma \cdot |M_{i+1,0}^{(\mu)}|. \tag{5.34}$$

Algorithm 3. In this algorithm, we are along with Hearn's trial division algorithm for GCD.[6] Algorithm for PRS, secondary-PRS, and multi-PRS in general are to calculate $[P_{i-1}^{(\mu)}, P_i^{(\nu_i)}]$ and then divide it by a factor of the form $\Pi_{j=0}^{i-1}(c_j^{(\nu_j)})^{e_j}$. Contrary to Algorithms 1 and 2, where the exponents e_j in the divisor factor are calculated by the iteration formulas on $L(\mu, i+1, j)$, $N[l]_{i+1,j}^{(\mu)}(k)$ and $A[l]_{i+1,j}^{(\mu)}(k)$, Algorithm 3 performs trial division to determine whether or not $c_j^{(\nu_j)}$ is a factor of $P_{i+1}^{(\mu)}$. We describe the algorithm explicitly.

Algorithm TRIAL-DIVISION MULTI-PRS.

Input: A set of polynomials $\{P_0^{(1)}, \ldots, P_0^{(m)}\}$
and a sequence $\{\nu_0, \nu_1, \ldots, \nu_{i_{\max}-1}\}$.

Output: Multi-PRS $\{P_i^{(1)}, \ldots, P_i^{(m)}\}$, $i=1, \ldots, i_{\max}$.

```
P_1^(ν0) ← P_0^(ν0);
For μ←1 to m with μ≠ν0 do
    P_1^(μ) ←prem(P_0^(μ), P_0^(ν0));
For i←2 to i_max do begin
    P_i^(νi-1) ← P_{i-1}^(νi-1);
    For μ←1 to m with μ≠νi-1 do
        if n_{i-1}^(μ) ≤ n_{i-1}^(νi-1) then P_i^(μ) ← P_{i-1}^(μ)
          else begin
              P_i^(μ) ←prem(P_{i-1}^(μ), P_{i-1}^(νi-1));
              For j←i-2 to 0 step -1 do
                  while c_j^(νj) divides P_i^(μ) do
                      P_i^(μ) ← P_i^(μ)/c_j^(νj);
              end;
    end;
```

§ 6. Concluding Remarks

Algorithms 1 and 2 are, respectively, generalizations of the reduced-PRS and the subresultant-PRS algorithms. Algorithm 1 is simpler than Algorithm 2 but the latter is more efficient than the former. We have not tested the efficiency of Algorithm 3. If, however, high efficiency of the trial-division algorithm in PRS calculation can be extended to our multi-PRS, Algorithm 3 will be efficient practically.

Selection of divisor polynomials $\{P_0^{(\nu_0)}, P_1^{(\nu_1)}, \dots\}$ is quite important in actual computation. As the example of multi-PRS presented in §3 shows, when the divisor polynomials are chosen arbitrarily, successor blocks and abnormal rows appear in PRS-matrix quite commonly, making the orders of PRS-matrices large. Generally speaking, the larger the orders of PRS-matrices are, the more time the calculation of the multi-PRS requires. Therefore, we had better calculate multi-PRS as a set of secondary-PRSs. Then, we encounter neither successor blocks nor abnormal rows in the PRS-matrices (see, below Theorem 2 in §5).

So far we have defined multi-PRS by (1.10). The formulas in (1.10) do not define the most general multi-PRS, because they suffer from a restriction that the number of divisor polynomials in the calculation of the $(i+1)$st remainders is one. By removing this restriction, we can define the most general multi-PRS. That is, setting $P_i^{(\nu_{ik})}$, $k=1, \dots, n$, as divisor polynomials, we generate the $(i+1)$st remainders $\{P_{i+1}^{(1)}, \dots, P_{i+1}^{(m)}\}$ through formulas

$$\nu_{ik} \in \{1, 2, \dots, m\},$$
$$\nu(\mu, i) \in \{\nu_{i1}, \dots, \nu_{in}\},$$
$$\beta_i^{(\mu)} P_{i+1}^{(\mu)} = \alpha_i^{(\mu)} P_i^{(\mu)} - Q_i^{(\mu)} P_i^{(\nu(\mu,i))},$$
$$\deg(P_{i+1}^{(\mu)}) < \deg(P_i^{(\nu(\mu,i))}), \quad \alpha_i^{(\mu)}, \beta_i^{(\mu)} \in I,$$
$$P_{i+1}^{(\nu_{ik})} = P_i^{(\nu_{ik})}, \quad k=1, \dots, n.$$

Let us divide the set of $(i+1)$st remainders into groups such that each polynomial in the kth group is generated by the divisor polynomial $P_i^{(\nu_{ik})}$, $1 \leqq k \leqq n$. Furthermore, let the kth group contain $P_{i+1}^{(\nu_{ik})}$. Then, we can inverse-reduce the PRS-matrix by adding rows of types $P_i^{(\nu_{i1})}, \dots, P_i^{(\nu_{in})}$ successively, in such a way that the rows of type $P_i^{(\nu_{ik})}$ are added only to inverse-reduce all the rows which are

grouped into the kth set. Then, the procedure of inverse-reduction presented in §3 and analyzed in §4 is applicable also to the generalized multi-PRS. Therefore, Theorem 1 stated in §4 is still valid for the generalized multi-PRS.

References

[1] Collins, G. E., Polynomial remainder sequences and determinants, *Amer. Math. Mon.* **73**, (1966), 708.

[2] ———, Subresultants and reduced polynomial remainder sequences, *J. ACM* **14**, (1967), 128.

[3] Brown, W. S. and Traub, J. F., On Euclid's algorithm and the theory of subresultants, *J. ACM* **18**, (1971), 505.

[4] Brown, W. S., The subresultant PRS algorithm, *ACM Trans. Math. Soft.* **4**, (1978), 237.

[5] Sasaki, T. and Furukawa, A., Secondary polynomial remainder sequence and an extension of subresultant theory, *J. Inform. Proces.* (to appear).

[6] Hearn, A. C., Non-modular computation of polynomial GCDs using trial division, *Proc. EUROSAM 79, Lecture Notes in Comp. Sci.*, **72**, Springer-Verlag, (1979), 228.