数理解析研究所講究録
第 685 巻 1989 年 1-14

On Sturm Sequence with Floating-point Number Coefficients

Masayuki Suzuki and Tateaki Sasaki
(鈴木正幸) (佐々木建昭)

The Institute of Physical and Chemical Research
Hirosawa, Wako-shi, Saitama 351-01, Japan

Abstract

Let $(P_1(x), P_2 = dP_1/dx, P_3, \ldots)$ be a Sturm sequence with coefficients of floating-point numbers. If P_1 contains "close" roots the accuracy of coefficients of P_k decreases rapidly as k increases. Furthermore, the leading coefficient of some element may become abnormally small. Hence, the sequence must be treated carefully. In this paper, we first describe how to handle the polynomials with floating-point number coefficients. In particular, the polynomial division is carefully defined. Then, we analyze the "abnormal" sequence and show the usefulness of approximate Sturm sequence under some conditions. In order to attain the desired accuracy, we present an algorithm for increasing the accuracy of coefficients of P_k. By expanding P_k as $P_k = P_{k1} + \varepsilon P_{k2} + \varepsilon^2 P_{k3} + \ldots$, with ε a small positive number, say $\varepsilon = 10^{-7}$, the algorithm increases the accuracy of P_k from relative error $\mathrm{O}(\varepsilon^j)$ to $\mathrm{O}(\varepsilon^{j+1})$ iteratively, without increasing the accuracy of $P_3, \ldots, P_{k-1}$. The algorithm has a similarity to Hensel lifting of integers, with some important differences. Performance of the algorithm is explained by examples.

1 Introduction

The Sturm sequence has been used for long years to calculate the real roots of algebraic equations accurately, see [2] for example. If we generate Sturm sequence by using the integer arithmetic or the rational number arithmetic, as in [3], we often meet tremendously large coefficients. This suggests us to use the floating-point arithmetic [4]. With the floating-point arithmetic, however, the accuracy of coefficients of Sturm sequence often decreases largely by the cancellation of almost equal numbers, see example in **3**. This phenomenon happens always if the given polynomial has "close" roots, and the relationship between the decrease of accuracy and the distance of mutually close roots is almost clarified by [5] and [6]. Furthermore, the Sturm sequence may be "abnormal", i.e., the leading coefficient of some element of the sequence is very small compared with other coefficients of the elements.

Three points are important in handling Sturm sequence with floating-point number coefficients: the first is how to detect the decrease of accuracy, the second is how to treat the abnormal sequence, and the third is how to calculate the Sturm sequence to a given accuracy. As for the first point, Pinkert [7] proposed to use the interval arithmetic. In this paper, we describe another simple method which detects the amount of accuracy decreasing by the reduction of magnitude of the coefficients. As for the second and third points, it seems that no comprehensive study has been made so far. Note that these points are never trivial, even if we adopt the interval arithmetic, because the accuracy of the sequence may decrease as the computation proceeds and we cannot know the accuracy of the result in advance. In particular, the abnormal sequence must be treated carefully because neglect of a coefficient of very small magnitude may change the property of Sturm sequence significantly. When the accuracy of answer is not enough, we usually repeat the same computation by increasing the precision of numbers, which is wasteful. A better method is to increase the accuracy iteratively by utilizing expressions already computed. Although this method can be formulated easily and simply in a general form, we show in this paper that we can increase the accuracy by a method similar to Hensel lifting (see [8], for example) of integers.

After defining necessary notions in **2**, we describe how to handle Sturm sequence with floating-point number coefficients in **3**. Usefulness of approximate Sturm sequence is shown in **4**. The algorithm for increasing the accuracy of coefficients, which is similar to Hensel lifting, is given in **5** and the performance of the algorithm is explained in **6** by examples.

2 Definitions on approximate polynomials

In this paper, by approximate polynomials, we mean polynomials with approximate numeric coefficients. Following ref. [5], we give some definitions for treating approximate polynomials.

Let $P(x)$ be a polynomial in variable x with floating-point number coefficients:

$$P(x) = a_l x^l + a_{l-1}x^{l-1} + \cdots + a_0, \quad a_l \neq 0. \tag{1}$$

The l, a_l, and $a_l x^l$ are called degree, leading coefficient, and leading term, respectively, of P and written as $\deg(P)$, $\mathrm{lc}(P)$, and $\mathrm{lt}(P)$.

Definition 1 [maximum magnitude coefficient]. *The absolute value of the maximum magnitude coefficient of $P(x)$ is written as $\mathrm{mmc}(P)$:*

$$\mathrm{mmc}(P) = \max\{|a_l|, \cdots, |a_0|\}. \tag{2}$$

The $\mathrm{mmc}(P)$ is nothing but the infinite "norm" of P, i.e., $\mathrm{mmc}(P) = \| P \|_\infty$.

Definition 2 [numbers of similar magnitudes]. *Let f and g be numbers (may be complex) with $g \neq 0$. By $f = \mathrm{O}(g)$, we mean that $1/c \le |f/g| \le c$, where c is a positive number not much different from 1. (Usually "O" denotes Landau's notation, and we are using "O" in some different meaning.)*

It is not easy to specify the value of c precisely. For example, $c \sim 3$ or 4 in some case but $c \sim 10$ or 20 in another case. The discussions in [5] and [6] were developed under the condition that if polynomials F, G, and H are such that $F = GH$ then $\mathrm{mmc}(F) = \mathrm{O}(\mathrm{mmc}(G) \times \mathrm{mmc}(H))$, by assuming that $\deg(F)$ is not so large. In this paper also, we use "O" in the same sense as in [5]. An apparent condition on c is that $1/c \gg \varepsilon$, where ε is a small positive number we introduce below.

Definition 3 [polynomial with small magnitude coefficients]. *Let ε be a small positive number, $0 < \varepsilon \ll 1$. By $\mathrm{O}(\varepsilon(x))$, we mean a polynomial such that $\mathrm{mmc}(\mathrm{O}(\varepsilon(x))) = \mathrm{O}(\varepsilon)$.*

Definition 4 [regular polynomial]. *The $P(x)$, defined in (2), is called regular if*

$$|a_l| = \mathrm{O}(1) \ \textit{and} \ \max\{|a_{l-1}|, \cdots, |a_0|\} = \ \textit{either} \ \mathrm{O}(1) \ \textit{or} \ 0. \tag{3}$$

(Note). Any univariate polynomial $P(x)$ can be made regular by the scaling transformation $P(x) \to \xi P(\eta x)$, where ξ and η are suitably chosen numbers. Q_t

Let $P(x)$ be regular and $P(x) \neq \mathrm{ht}(P(x))$. Let the roots of $P(x)$ be $\alpha_1, \cdots, \alpha_l$, then it is well-known that $\max\{|\alpha_1|, \cdots, |\alpha_l|\} = \mathrm{O}(1)$. This fact allows us to define the close roots.

Definition 5 [close roots]. *Let $P(x)$ be a regular polynomial. If α_i and α_j are roots of $P(x)$ such that $0 < |\alpha_i - \alpha_j| \ll 1$ then α_i and α_j are (mutually) close roots.*

Definition 6 [accuracy of floating-point numbers]. *Let f be a floating-point number containing an error Δf, then we define the accuracy of f as*

$$\mathrm{acc}(f) = \log_2 |f/\Delta f|. \tag{4}$$

The accuracy of f is nothing but the number of bits representing the correct part of f. Suppose M bits are used to represent the mantissa of f and only the leading M' bits are correct then $\mathrm{acc}(f) = M'$.

3 Approximate Sturm sequence

In this paper, by approximate Sturm sequence we mean the Sturm sequence with coefficients computed approximately. Conversely, mathematically correct sequence is called exact Sturm sequence. On the basis of definitions in **2**, let us discuss how to calculate the approximate Sturm sequence. As we will see below, this is fundamentally important when the floating-point arithmetic is used.

Let $F(x)$ and $G(x)$ be polynomials in single variable x with $\deg(F) \geq \deg(G)$. The Sturm sequence is a polynomial remainder sequence $(P_1, P_2, P_3, \ldots)$ calculated iteratively as

$$\begin{cases} P_1 = F(x), \quad P_2 = G(x), \\ -c_i P_{i+1} = \mathrm{remainder}(P_{i-1}, P_i), \quad i = 2, 3, \cdots, \end{cases} \tag{5}$$

where c_i is a positive number to be specified below. In particular, the case $G(x) \propto dF(x)/dx$ is very important practically. Since we are handling polynomials with floating-point number coefficients, we must calculate the remainder sequence carefully. The remainder calculation, or the division operation, is a successive application of leading term elimination, and we impose the following rules for the leading term elimination.

Rule 1 [leading term elimination]. *Let $F(x)$ and $G(x)$ be*

$$\begin{cases} F(x) = f_l x^l + \cdots + f_0, & f_l \neq 0, \\ G(x) = g_m x^m + \cdots + g_0, & g_m \neq 0, \quad l \geq m. \end{cases} \tag{6}$$

We eliminate the leading term (x^l term) as

$$\begin{aligned} \tilde{F}(x) &= [F(x) - \mathrm{ht}(F(x))] - x^{l-m}(f_l/g_m)[G(x) - \mathrm{ht}(G(x))] \\ &= \textstyle\sum_{i=1}^{l} [f_{l-i} - (f_l/g_m) g_{m-i}] x^{l-i}. \end{aligned} \tag{7}$$

Rule 2 **[zero coefficient].** *Let M bits be used to represent the floating-point number in the system. If x^{l-i} term of (7) satisfies the following condition, then we discard the term as a zero coefficient term (i.e., we cutoff the small number at $\mathrm{O}(2^{-M})$).*

$$|f_{l-i} - (f_l/g_m)g_{m-i}| \le \mathrm{O}(2^{-M}). \tag{8}$$

With Rule 1, we are free from error in $f_l - (f_l/g_m)g_m$ which must be 0 theoretically but may not be 0 in the approximate arithmetic. If $|g_m| = \mathrm{O}(2^{-M}) \neq 0$, which may happen in the approximate arithmetic, then the elimination is meaningless ($\tilde{F}$ in (7) is almost proportional to G). Rule 2 is imposed to avoid such hazardous situation.

One very important point in the calculation of approximate Sturm sequence (and approximate algebraic expressions in general) is that the accuracy of coefficients must be determined easily; if we cannot know the accuracy we can never rely on the result obtained. We accomplish this point by suitably choosing the normalization constant c_i in (5) as follows.

Rule 3 **[normalization of Sturm sequence].** *We choose c_i in (5) as*

$$\begin{cases} Q_i \leftarrow \mathrm{quo}(P_{i-1}, P_i), \\ -P_{i+1} \leftarrow \mathrm{rem}(P_{i-1}, P_i)/\max\{1, \mathrm{mmc}(Q_i)\}, \end{cases} \tag{9}$$

where quo *and* rem *denote the quotient and the remainder, respectively.*

Lemma 1 *Let P_{i-1}, P_i and P_{i+1} satisfy (9). Let the upper bound of the errors in the coefficients of P_j be $\mathrm{O}(\varepsilon_j)$, $j = i-1, i, i+1$. If $|\mathrm{lc}(P_{i-1})| \gg \varepsilon_{i-1}$, $|\mathrm{lc}(P_i)| \gg \varepsilon_i$, and $\varepsilon_{i-1} \ge \varepsilon_i$ then ε_{i+1} is given by ε_{i-1} and ε_i as*

$$\varepsilon_{i+1} \cong \varepsilon_i \cdot \mathrm{mmc}(P_i)/|\mathrm{lc}(P_i)|. \tag{10}$$

Proof: For convenience, we denote P_{i-1}, P_i, ε_{i-1}, ε_i by F, G, ε_F, ε_G, respectively, with F and G given by (6). Since the division is a successive application of leading term elimination, let us consider (7). Let ΔF and ΔG be errors in f_l and g_m, respectively, then

$$g_{m-i}(f_l + \Delta f)/(g_m + \Delta g) \cong (f_l/g_m)\{g_{m-i} + \Delta f(g_{m-i}/f_l) - \Delta g(g_{m-i}/g_m)\}. \tag{11}$$

Note that $|\Delta f| \le \varepsilon_F$ and $|\Delta g| \le \varepsilon_G$. If $|f_l/g_m| \equiv q \ge 1$ then (11) gives

$$\begin{aligned} &\mathrm{error}[f_{l-i} - (f_l/g_m)g_{m-i}]/\max\{1, |f_l/g_m|\}) \\ &\le \max\{\varepsilon_F/q, \varepsilon_G, \varepsilon_F \cdot \mathrm{mmc}(G)/|f_l|, \varepsilon_G \cdot \mathrm{mmc}(G)/|g_m|\} \\ &= \mathrm{mmc}(G)/|g_m| \times \max\{\varepsilon_F/q, \varepsilon_G\}. \end{aligned}$$

Similarly, if $|f_l/g_m| \equiv q < 1$ then the error bound is

$$\begin{aligned} &\max\{\varepsilon_F, \varepsilon_G q, \varepsilon_F q \cdot \mathrm{mmc}(G)/|f_l|, \varepsilon_G q \cdot \mathrm{mmc}(G)/|g_m|\} \\ &= \mathrm{mmc}(G)/|g_m| \times \max\{\varepsilon_F, \varepsilon_G q\}. \end{aligned}$$

Here, we have neglected the statistical accumulation of errors. Note that $\max\{1, |f_l|/|g_m|\} = \max\{1, |\mathrm{lc}(Q_i)|\}$. Elimination of x^l term of F and G gives

$$\tilde{F}(x) = [f_{l-1} - (f_l/g_m)g_{m-1}]x^{l-1} + \cdots.$$

The error in the coefficients of $\tilde{F}$ can be estimated by replacing f_{l-1} and Δf in (11) by $f_{l-i} - (f_l/g_m)g_{m-i}$, $i = 0, 1, \cdots$, and ε_G, respectively, because $\varepsilon_G \geq \varepsilon_F$. After a calculation similar to the above, we find

$$error \leq \varepsilon_G \times \mathrm{mmc}(G)/|g_m|.$$

Continuing this estimation, we obtain (10). □

Theorem 1 *Let P_1 and P_2 be polynomials such that* $\mathrm{mmc}(P_1) = \mathrm{O}(1)$ *and* $\mathrm{mmc}(P_2) = \mathrm{O}(1)$, *with errors less than* 2^{-M} *in their coefficients. Then, we have*

$$\begin{aligned} &\mathrm{acc}(\textit{each coefficient of } P_k) \geq \mathrm{O}(\log_2[r_2 \cdots r_{k-1} \mathrm{mmc}(P_k) \times 2^M)), \\ &r_i = |\mathrm{lc}(P_i)/\mathrm{mmc}(P_i)| \leq 1. \end{aligned} \tag{12}$$

Proof: Putting $\varepsilon_1 = \varepsilon_2 = 2^{-M}$ in Lemma 1 and using (4), we obtain (12) easily. □

(Note). We see that the decrease of accuracy in the coefficients is easily determined by the reduction of the leading coefficients and the maximum magnitude coefficients.

Theorem 1 is applicable to the sequences calculated with Rules 1, 2, and 3. Actually, there may happen that the leading coefficient of some element of the sequence is extremely small if calculated exactly, hence the term is erased by Rule 2. Analysis of such sequence is given in the next section.

Definition 7 [abnormal sequence]. *Sturm sequence $(P_1, P_2, P_3, \cdots)$ is called abnormal if the following relation holds.*

$$\deg(P_i) > \deg(P_{i+1}) + 1 \ \textit{or}\ |\mathrm{lc}(P_i)| \ll \mathrm{mmc}(P_i) \ \ \textit{for some } i. \tag{13}$$

If $|\mathrm{lc}(P_i)| \ll \mathrm{mmc}(P_i)$ and $|\mathrm{lc}(P_{i-1})| = \mathrm{O}(\mathrm{mmc}(P_{i-1}))$ then $\mathrm{mmc}(\mathrm{rem}(P_{i-1}, P_i))$ becomes much larger than $\mathrm{mmc}(P_i)$. Hence, if we choose $c_i = 1$ in (5), then $\mathrm{mmc}(P_i)$ will fluctuate largely as i increases for abnormal Sturm sequence, leading to numerical unstability of the computation. With Rule 3, $\mathrm{mmc}(P_i)$ changes gently as i increases and it decreases steadily if $F(x)$ and $G(x)$ have mutually close roots, see an example below. This is another important consequence of Rule 3.

Let us show an example of Sturm sequence calcuated by formula (9). We see a strong magnitude reduction of the coefficients.

Example 1. Sturm sequence of P_1 and $P_2 = [dP_1(x)/dx]/\deg(P_1)$.

$$P_1 = (X+1)(X-2)(X-.5)(X-.501)(X-.503)$$

$$P_2 = (dP_1/dX)/5$$

$$P_3 = .90000136X^3 - .135432204E^1X^2 + .679323541X - .113581429$$

$$P_4 = -.121499582E^1X^2 + .121823582E^1X - .305370171$$

$$P_5 = .349999695E^{-5}X - .175299848E^{-5}$$

$$P_6 = -.192857883E^{-11}$$

Here, we had better comment on Schönhage's method of computing "quasi-GCD" [9]. Given polynomials P_1 and P_2, Schönhage generates a sequence $(P_3, P_4, \cdots)$ by the formula

$$P_{i-1} - (x - \alpha_i)P_i = (x - \beta_i)^2 P_{i+1}, \quad i = 2, 3, \cdots, \tag{14}$$

where α_i and β_i are numbers so determined as not to generate abnormal sequence. The polynomial sequence calculated by (12) is not the polynomial remainder sequence, but it is free from numerical unstability and it allows us to calculate an approximate GCD. Schönhage analized the time complexity of his algorithm but did not consider the accuracy decreasing of coefficients. As we have pointed out in **1**, one very important point in the approximate Sturm sequence is the analysis of accuracy of coefficients.

4 Usefulness of approximate Sturm sequence

Consider that an exact Sturm sequence is abnormal, i.e., $|\mathrm{lc}(P_i)| \ll \mathrm{mmc}(P_i)$ for some element P_i of the sequence. Then, $\mathrm{lt}(P_i)$ may vanish in the approximate Sturm sequence. Since the leading term plays an essential role in the division, one may be afraid that the approximate Sturm sequence is much different from the exact sequence if it is abnormal. In fact, the length of such approximate sequence is not the same as that of exact sequence. In this section, we show that such approximate sequences are still useful under some conditions.

We first note that the leading term may be cutoff during the division process. This cutoff does not cause any problem unless $|\mathrm{lc}(\mathrm{divisor})| \ll \mathrm{mmc}(\mathrm{divisor})$, as the following lemma shows.

Lemma 2 *Let ε be a small positive number, $0 < \varepsilon \ll 1$, and $F(x)$ and $G(x)$ be polynomials, with $|\mathrm{lc}(F)| \gg \varepsilon$ and $|\mathrm{lc}(G)| \gg \varepsilon$. Let*

$$\begin{cases} R(x) = \mathrm{rem}(F(x), G(x))/\gamma, \\ R'(x) = \mathrm{rem}(F(x), G(x))/\gamma \quad \textit{with coefficient cuttoff at } \mathrm{O}(\varepsilon), \\ \gamma = \max\{1, \mathrm{mmc}(\mathrm{quo}(F, G))\}. \end{cases} \tag{15}$$

Then, we have

$$\begin{cases} R(x) = R'(x) + \Delta R(x)/\gamma, \\ \mathrm{mmc}(\Delta R(x)) \leq \mathrm{O}(\varepsilon) \times \mathrm{mmc}(G)/|\mathrm{lc}(G)|. \end{cases} \tag{16}$$

Proof: Let $\deg(F) = l \geq m = \deg(G)$. Suppose that, after eliminating terms of degrees greater than m', $m' \geq m$, of F by G, we obtain

$$H(x) = h_{m'}x^{m'} + \cdots + h_m x^m + H'(x), \ \deg(H') < m,$$
$$|h_{m'}|, \cdots, |h_m| < \varepsilon.$$

Then, $R'(x) = H'(x)/\gamma$. In order to get $R(x)$, we must eliminate terms of degrees $m', \cdots, m$ further. This elimination is performed by multiplying numbers of $\mathrm{O}(\varepsilon)$ or less to $G/\mathrm{lc}(G)$. Hence, we obtain (16). □

Next, we consider the case that $R = \mathrm{rem}(F, G)/\gamma$ is such that $|\mathrm{lc}(R)| < \varepsilon$ if calculated exactly; thus, $\mathrm{lt}(R)$ vanishes in the approximate sequence.

Lemma 3 *Let ε be such that $0 < \varepsilon \ll 1$. Let $(P_1, P_2, P_3, \cdots)$ be an exact Sturm sequence and $(P'_1 \cong P_1, P'_2 \cong P_2, P'_3, \cdots)$ be an approximate Sturm sequence, with coefficient cutoff at $\mathrm{O}(\varepsilon)$, generated by (9). (Hence, $|\mathrm{lc}(P'_i)| > \varepsilon$ for every i). Let $k1+1 < k\lambda$ and*

$$\begin{cases} \deg(P_{k1}) = \deg(P'_k) = l, \\ \deg(P_{k1+1}) = m, \quad n < m < l, \\ \deg(P_{k\lambda}) = \deg(P'_{k+1}) = n. \end{cases}$$

(That is, terms of degrees greater than n in P'_{k+1} are cutoff, hence the approximate sequence does not contain elements corresponding to $P_{k1+1}, \cdots, P_{k\lambda-1}$.) If $\mathrm{lc}(P'_k) \gg \varepsilon$ and $\mathrm{lc}(P'_{k+1}) \gg \varepsilon$ then we have the following relations, where

$$r_i \equiv |\mathrm{lc}(P'_i)|/\mathrm{mmc}(P'_i), \quad i = 1, 2, \cdots. \tag{17}$$

When $k1+1 \le i \le k\lambda$,

$$\begin{cases} P_i/\mathrm{mmc}(P_i) = \pm[P'_{k+1} + \mathrm{O}(\varepsilon'(x)) + \mathrm{O}(\eta'(x))]/\mathrm{mmc}(P'_{k+1}), \\ \varepsilon' = \varepsilon/(r_2 \cdots r_k), \quad \eta' = \varepsilon/\min\{r_k, r_{k+1}\}. \end{cases} \tag{18}$$

When $i = k\lambda + 1$,

$$\begin{cases} P_i/\mathrm{mmc}(P_i) = \pm[P'_{k+2} + \mathrm{O}(\varepsilon''(x)) + \mathrm{O}(\eta''(x))]/\mathrm{mmc}(P'_{k+2}), \\ \varepsilon'' = \varepsilon/(r_2 \cdots r_k r_{k+1}), \quad \eta'' = \varepsilon/(r_k r_{k+1}) \times \mathrm{mmc}(P'_{k+2})/\mathrm{mmc}(P'_{k+1}). \end{cases} \tag{19}$$

Here, $\pm$ sign means either $+$ or $-$ sign.

Proof: Let P_{k1} and P_{k1+1} in normalized form be

$$P_{k1}/\mathrm{mmc}(P_{k1}) \equiv F = a_l x^l + \cdots + a_0, \; a_l \neq 0,$$
$$P_{k1+1}/\mathrm{mmc}(P_{k1+1}) \equiv G = b_m x^m + \cdots + b_0, \; b_m \neq 0.$$

By assumption, $G \cong P'_{k+1}/\mathrm{mmc}(P'_{k+1})$ and

$$\eta \equiv \max\{|b_m|, \cdots, |b_{n+1}|\} \le \mathrm{O}(\varepsilon)/\mathrm{mmc}(P'_{k+1}), \tag{20}$$
$$P'_{k+1}/\mathrm{mmc}(P'_{k+1}) \equiv G' = b_n x^n + \cdots + b_0 + \Delta H(x). \tag{21}$$

Lemma 1 and Lemma 2 tell that

$$\mathrm{mmc}(\Delta H) \le \mathrm{O}(\varepsilon)/[r_2 \cdots r_k \times \mathrm{mmc}(P'_{k+1})]. \tag{22}$$

According to the subresultant theory (see [10], for example), the element P_i, $i \ge k1+2$, of the exact sequence can be represented by P_{k1} and P_{k1+1} as

$$P_i \propto \begin{vmatrix} a_l & a_{l-1} & \cdots & \cdots & \cdots & a_{2\nu+2-m} & Fx^{m-\nu-1} \\ & a_l & \cdots & \cdots & \cdots & a_{2\nu+3-m} & Fx^{m-\nu-2} \\ & & \ddots & \cdots & \cdots & \cdots & \cdots \\ & & & a_l & \cdots & a_{\nu+1} & Fx^0 \\ b_m & b_{m-1} & \cdots & \cdots & \cdots & b_{2\nu+2-l} & Gx^{l-\nu-1} \\ & b_m & \cdots & \cdots & \cdots & b_{2\nu+3-l} & Gx^{l-\nu-2} \\ & & \ddots & \cdots & \cdots & \cdots & \cdots \\ & & & b_m & \cdots & b_{\nu+1} & Gx^0 \end{vmatrix} \tag{23}$$

where $\nu = \deg(P_{i-1}) - 1$ and $a_j = b_j = 0$ if $j < 0$.

Since $|b_m|, \cdots, |b_{n+1}| \ll 1$, while $\mathrm{mmc}(F) = \mathrm{mmc}(G) = 1$, we can evaluate the above determinant by expanding it w.r.t. the first, second, $\cdots$ columns successively.

When $n \le \nu < m$. In this case, we have

$$P_i \propto D + [\text{ terms smaller by } \mathrm{O}(\eta/|a_l|)],$$

$$D = a_l^{m-\nu} \begin{vmatrix} b_\nu & \cdots & b_{2\nu+2-l} & Gx^{l-\nu-1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & b_{\nu+1} & Gx^0 \end{vmatrix}.$$

Expansion of D gives $D \propto G + [\text{ terms smaller by } \mathrm{O}(\eta/|b_n|)]$. Eqs. (20) and (21) tell that $G = G' - \Delta H(x) + \mathrm{O}(\eta(x))$. Hence, noting that $|a_l| = r_k$ and $|b_n| = r_{k+1}$, we obtain (18).

When $\nu < n$. In this case, we have

$$P_i \propto D + [\text{ terms smaller by } \mathrm{O}(\eta/|a_l|)],$$

$$D = \begin{vmatrix} a_l & a_{l-1} & \cdots & \cdots & \cdots & a_{2\nu+2-n} & Fx^{n-\nu-1} \\ & a_l & \cdots & \cdots & \cdots & a_{2\nu+3-n} & Fx^{n-\nu-2} \\ & & \ddots & \cdots & \cdots & \cdots & \cdots \\ & & & a_l & \cdots & a_{\nu+1} & Fx^0 \\ b_n & b_{n-1} & \cdots & \cdots & \cdots & b_{2\nu+2-l} & G'x^{l-\nu-1} \\ & b_n & \cdots & \cdots & \cdots & b_{2\nu+3-l} & G'x^{l-\nu-1} \\ & & \ddots & \cdots & \cdots & \cdots & \cdots \\ & & & b_n & \cdots & b_{\nu+1} & G'x^0 \end{vmatrix}$$

That is, D is a subresultant of F and G'. In particular, if $\nu = \deg(G') - 1 = n - 1$, we have $D \propto \mathrm{rem}(F, G')$. This division increases the error term by $\mathrm{mmc}(P'_{k+1})/|\mathrm{lc}(P'_{k+1})|$, as Lemma 1 asserts. Hence, we obtain (19) easily. □

Lemma 2 tells that, except for the $\pm$ sign in (18) and (19), both exact and approximate sequences contain nearly the same elements so long as $\varepsilon \ll 1$. However, the sign is very important in the Sturm sequence and the sign is dependent on the situation.

Example 2. Abnormal sequence

$$P_1 = (x^2 + \varepsilon x + \varepsilon')(x^3 - 1), \quad \varepsilon' = \mathrm{O}(\varepsilon), \quad 0 < \varepsilon \ll 1.$$

The exact sequence $(P_1, P_2 = (dP_1/dx)/5, P_3, \cdots)$ and approximate sequence $(P_1, P_2, P'_3, \cdots)$, with coefficient cutoff at $\mathrm{O}(\varepsilon)$, are as follows.

$$\begin{aligned} P_3 &= -(2/3)\varepsilon' x^3 + x^2 + (6/5)\varepsilon x + (5/3)\varepsilon' + \mathrm{O}(\varepsilon^2(x)), \\ P_4 &= -x^2 - (6/5)\varepsilon x - (5/3)\varepsilon' + \mathrm{O}(\varepsilon^2(x)), \\ &\cdots \\ P'_3 &= x^2, \\ P'_4 &= x, \\ P'_5 &= 0. \end{aligned}$$

The P_4 corresponds to P'_3, but we see $P'_3 = -P_4 + \mathrm{O}(\varepsilon(x))$.

Finally, let us consider the $\pm$ sign in Eqs. (18) and (19). As we have seen in Lemma 3 and Example 2, a small change in the coefficients of initial polynomials may change the sign in Eqs. (18) and (19), if the sequence is abnormal. According to the Sturm theorem, the sign change must be due to the existence of close roots, although the Sturm sequence may be abnormal even if there is no close root. Fortunately, we can determine the existence of mutually close roots by the approximate Sturm sequence, so long as P_1 and P_2 are regular.

Theorem 2 [Sasaki & Noda [5]] *Let ε be a small positive number, $0 < \varepsilon \ll 1$, and $F(x)$ and $G(x)$ be regular polynomials, in single variable x, such that*

$$\begin{cases} F(x) = D(x)\tilde{F}(x) + \mathrm{O}(\varepsilon(x)), \\ G(x) = D(x)\tilde{G}(x) + \mathrm{O}(\varepsilon(x)), \end{cases} \tag{24}$$

where $|\mathrm{lc}(D)| = 1$ and $\tilde{F}$ and $\tilde{G}$ have no mutually close roots. Let $(P'_1 \simeq F, P'_2 \simeq G, P'_3, \cdots)$ be an approximate polynomial remainder sequence, with coefficient cutoff at $\mathrm{O}(\varepsilon)$, generated by (9). Then some two successive elements, let them be P'_k and P'_{k+1}, are such that

$$\begin{cases} P'_k = \text{constant} \times D + \mathrm{O}(\varepsilon(x)), \ \deg(P'_k) = \deg(D), \\ P'_{k+1} = \mathrm{O}(\varepsilon(x)). \end{cases} \tag{25}$$

(Let δ be an average separation of mutually close roots, then $\varepsilon = \mathrm{O}(\delta)$ usually but $\varepsilon = \mathrm{O}(\delta^2)$ if $G \approx dF/dx$, etc.) □

According to the celebrated Sturm theorem, or its generalized versions, what we are interested in is not Sturm sequence itself but the following quantity:

$$N(a, b) = V(a) - V(b), \tag{26}$$

where a and b are real numbers and $V(c)$, $c \in \{a, b\}$, is the number of sign changes in $(P_1(c), P_2(c), P_3(c), \cdots)$ scanned from the left to right direction.

With this in mind, let us summarize the above results.

Theorem 3 *Let ε be a small positive number, $0 < \varepsilon \ll 1$, and F and G be regular polynomials, where $\deg(F) \geq \deg(G)$. Let $(P'_1 \simeq F,\ P'_2 \simeq G,\ P'_3,\ \cdots, P'_k)$ be an approximate Sturm sequence, with coefficient cutoff at $\mathrm{O}(\varepsilon)$, generated by formula (9). Furthermore, let a and b be real numbers, with $c \in \{a, b\}$, such that*

$$\begin{cases} |P'_i(c)| \gg \mathrm{O}(\varepsilon_i(c)) \ \textit{for every}\ i = 1, 2, \cdots, k, \\ \varepsilon_i = \varepsilon/(r_2 \cdots r_{i-1}), \quad r_j = |\mathrm{lc}(P'_j)|/\mathrm{mmc}(P'_j), \quad j = 2, \cdots, i-1. \end{cases} \tag{27}$$

(i) If P_1 and P_2 are regular and $P'_k =$ constant such that $|P'_k| \gg \varepsilon^{1/2}$ then we can calculate $N(a, b)$ correctly using approximate sequence, instead of exact sequence.

(ii) Let $P_2 = [dP_1/dx]/\deg(P_1)$. If we count the μ mutually close roots of root-separation $\leq \mathrm{O}(\varepsilon^{1/2})$ as μ multiple roots, then we can count the number of "different" real roots of P_1 by using approximate sequence.

Proof: We note that ε_i in (27) specifies the coefficient bound of the error term of $P'_i(x)$. Suppose P_1 and P_2 have mutually close roots of root-separation $\le \mathrm{O}(\delta)$, $0 < \delta \le 1$, and consider that these mutually close roots are moved to their respective center positions. This root-moving changes the coefficients of P'_i, $i = 1, 2, \cdots$, by $\mathrm{O}(\delta)$ or less, but we can increase the accuracy of approximate sequence to any precision. Hence, the claim *(ii)* is obtained. If $P'_k = constant$ and $|P'_k| \gg \varepsilon^{1/2}$, then F and G have no mutually close roots hence we have the claim *(i)*. □

The condition (27) tells that, if $\deg(P'_i) < \deg(P'_{i-1}) - 1$ for some i, we cannot set $a = -\infty$ or $b = \infty$ unless we know that no leading term of exact sequence vanishes by the cutoff at $\mathrm{O}(\varepsilon)$. This restriction is, however, not severe because we can bound the magnitude of roots easily.

5 Iteratively increasing the accuracy

The analysis in the previous section suggests that, even if we find that the Sturm sequence is abnormal, we proceed the calculation of approximate sequence. After that, we calculate P_k accurately when the error terms become significant. This section presents an algorithm which calculates P_k accurately without increasing the accuracy of $P_3, \cdots, P_{k-1}$ anymore.

Throughout the following, we assume that $\mathrm{mmc}(P_1) = \mathrm{O}(1)$, $\mathrm{mmc}(P_2) = \mathrm{O}(1)$.

As is well-known, the Sturm sequence $(P_1, P_2, P_3, \cdots)$ is associated with cofactor sequences $(A_1, A_2, A_3, \cdots)$ and $(B_1, B_2, B_3, \cdots)$ satisfying

$$\begin{cases} A_i P_1 + B_i P_2 = P_i, \quad i = 1, 2, 3, \cdots, \\ \deg(A_i) < \deg(P_2) - \deg(P_i), \\ \deg(B_i) < \deg(P_1) - \deg(P_i). \end{cases} \tag{28}$$

With formula (9), we can generate the cofactor sequences as

$$\begin{cases} A_1 = 1, \quad A_2 = 0, \quad -A_{i+1} = (A_{i-1} - Q_i A_i)/\gamma_i, \\ B_1 = 0, \quad B_2 = 1, \quad -B_{i+1} = (B_{i-1} - Q_i B_i)/\gamma_i, \\ \gamma_i = \max\{1, \mathrm{mmc}(Q_i)\}. \end{cases} \tag{29}$$

Let ε be a small positive number, say $\varepsilon = 10^{-7}$ or 10^{-10}. We consider that polynomial P_i, $\mathrm{mmc}(P_i) \le \mathrm{O}(1)$, is expanded as

$$\begin{cases} P_i = P_{i1} + \varepsilon P_{i2} + \cdots + \varepsilon^{j-1} P_{ij} + \cdots, \\ \text{coefficients of } P_{ij} \text{ are cutoff at } \varepsilon, \\ \mathrm{mmc}(P_{ij}) \le \mathrm{O}(1), \quad j = 1, 2, \cdots. \end{cases} \tag{30}$$

For simplicity, we denote

$$P_i^{(j)} = P_{i1} + \varepsilon P_{i2} + \cdots + \varepsilon^{j-1} P_{ij}. \tag{31}$$

Then, we have

$$P_i(x) = P_i^{(j)}(x) + \mathrm{O}(\varepsilon^j(x)). \tag{32}$$

We increase the accuracy of P_k as follows.

[Initial setup].

We calculate approximate Sturm and cofactor sequences satisfying

$$A_i^{(1)}P_1^{(1)} + B_i^{(1)}P_2^{(1)} = P_i^{(1)} + \mathrm{O}(\varepsilon(x)),\ i = 3,4,\cdots. \tag{33}$$

This calculation can be done iteratively by using formulas (9) and (29) with fixed-precision floating-point arithmetic.

[Iteration on j].

For $k \geq 3$, suppose we have $P_k^{(j)}$, $A_k^{(j)}$ and $B_k^{(j)}$, $j \geq 1$, satisfying

$$A_k^{(j)}P_1^{(j)} + B_k^{(j)}P_2^{(j)} = P_k^{(j)} + \mathrm{O}(\varepsilon^j(x)). \tag{34}$$

Calculating this equation with cutoff at ε^{j+1}, we obtain a polynomial $D(x)$ satisfying

$$\left\{\begin{array}{l} A_k^{(j)}P_1^{(j+1)} + B_k^{(j)}P_2^{(j+1)} = P_k^{(j)} + \varepsilon^j D(x) + \mathrm{O}(\varepsilon^{j+1}(x)), \\ \deg(D) \leq \deg(P_1) + \deg(P_2) - \deg(P_{k-1}), \quad \mathrm{mmc}(D) \leq \mathrm{O}(1). \end{array}\right. \tag{35}$$

Putting $P_k^{(j+1)}$, $A_k^{(j+1)}$, $B_k^{(j+1)}$, as

$$P_k^{(j+1)} = P_k^{(j)} + \varepsilon^j\tilde{P},\ A_k^{(j+1)} = A_k^{(j)} + \varepsilon^j\tilde{A},\ B_k^{(j+1)} = B_k^{(j)} + \varepsilon^j\tilde{B}, \tag{36}$$

we determine $\tilde{P}$, $\tilde{A}$ and $\tilde{B}$ so as to satisfy

$$A_k^{(j+1)}P_1^{(j+1)} + B_k^{(j+1)}P_2^{(j+1)} = P_k^{(j+1)} + \mathrm{O}(\varepsilon^{j+1}(x)). \tag{37}$$

Substituting (36) into (37), and using (35), we obtain

$$\tilde{A}P_1 + \tilde{B}P_2 = \tilde{P} - D(x) + \mathrm{O}(\varepsilon(x)). \tag{38}$$

Therefore, we have only to solve (38) with conditions

$$\left\{\begin{array}{l} \deg(\tilde{P}) < \deg(P_{k-1}^{(1)}), \\ \deg(\tilde{A}) \leq \deg(P_2) - \deg(P_{k-1}^{(1)}), \\ \deg(\tilde{B}) \leq \deg(P_1) - \deg(P_{k-1}^{(1)}). \end{array}\right. \tag{39}$$

[Solving Eq. (38) with conditions (39)].

We can solve (38) by using the theory of secondary polynomial remainder sequence, ref. [11]. Let $(\tilde{P}_1 = S, \tilde{P}_2, \cdots)$ be the secondary sequence and $(\tilde{A}_1, \tilde{A}_2, \cdots)$, $(\tilde{B}_1, \tilde{B}_2, \cdots)$ and $(\tilde{C}_1, \tilde{C}_2, \cdots)$ be its cofactor sequences. The secondary sequence is calculated from S and polynomial remainder sequence $(P_1,\ P_2,\ P_3,\ \cdots)$ by the following iteration formula.

$$\begin{array}{l} \tilde{P}_1 = S, \\ \tilde{Q}_i \leftarrow \mathrm{quo}(\tilde{P}_{i-1}, P_i), \quad i = 2,3,\cdots, \\ \tilde{P}_i \leftarrow (\tilde{P}_{i-1} - \tilde{Q}_i P_i)/\tilde{\gamma}_i, \\ \tilde{\gamma}_i = \max\{1, \mathrm{mmc}(\tilde{Q}_i)\}. \end{array} \tag{40}$$

Similarly, the cofactor sequences are calculated as

$$\begin{array}{l} \tilde{A}_1 = \tilde{B}_1 = 0,\ \tilde{C}_1 = 1, \\ \tilde{A}_i \leftarrow (\tilde{A}_{i-1} - \tilde{Q}_i A_i)/\tilde{\gamma}_i, \\ \tilde{B}_i \leftarrow (\tilde{B}_{i-1} - \tilde{Q}_i B_i)/\tilde{\gamma}_i, \\ \tilde{C}_i \leftarrow \tilde{C}_{i-1}/\tilde{\gamma}_i, \quad i = 2,3,\cdots. \end{array} \tag{41}$$

where $(A_1, A_2, \cdots)$ and $(B_1, B_2, \cdots)$ are cofactor sequences of the main sequence $(P_1, P_2, \cdots)$. The $\tilde{A}_i$, $\tilde{B}_i$ and $\tilde{P}_i$ satisfy

$$\begin{cases} \tilde{A}_i P_1 + \tilde{B}_i P_2 + \tilde{C}_i S = \tilde{P}_i, \quad i = 1, 2, \cdots, \\ \tilde{C}_i \text{ is a number.} \end{cases} \tag{42}$$

Thus, the solution $(\tilde{A}, \tilde{B}, \tilde{P})$ of equation (38), with degree condition (39), is obtained by putting $S = D$ and calculating the secondary polynomial remainder sequence and its cofactor sequences with fixed-precision floating-point number arithmetic; if i is such that $\deg(\tilde{P}_{i-1}) \geq \deg(P_{k-1}^{(1)})$ and $\deg(\tilde{P}_i) < \deg(P_{k-1}^{(1)})$ then we obtain

$$\tilde{A} = \tilde{A}_i / \tilde{C}_i, \ \tilde{B} = \tilde{B}_i / \tilde{C}_i, \ \tilde{P} = \tilde{P}_i / \tilde{C}_i. \tag{43}$$

Let us consider the above calculation method in detail.

On the expansion in (30)

We note that the expansion, $P_i = P_{i1} + \varepsilon P_{i2} + \cdots$, in (30) is not unique: for each P_{ij} in (30), the last several digits of its coefficients (corresponding to numbers of magnitude $\sim \varepsilon^j$) may be erroneous because of rounding. However, the errors are exactly corrected by the first several digits of the coefficients of $P_{i,j+1}$, see examples in the next section. That is, $P_{i,j+1}$ is such that $\mathrm{mmc}(\varepsilon^j P_{i,j+1}) \leq \mathrm{O}(\varepsilon^j)$ and not $\mathrm{mmc}(\varepsilon^j P_{i,j+1}) < \varepsilon^j$. This situation is quite different from Hensel lifting of integers: in the Hensel lifting, the numbers calculated with (mod p^j), with p a prime, is exact and not corrected by the calculation with (mod p^{j+1}).

On the necessary precision of numbers to solve Eq. (38)

One may think that we can solve Eq. (38) by approximating it as

$$\tilde{A} P_1^{(1)} + \tilde{B} P_2^{(1)} = \tilde{P} - D(x) + \mathrm{O}(\varepsilon(x)),$$

but this is not the case actually. This can be seen easily from the formulas in (40): the $\tilde{P}_i$ is generated by the division of $\tilde{P}_{i-1}$ and P_i, and $\mathrm{mmc}(P_i)$ (hence the accuracy of P_i) decreases almost steadily as i increases, see Example 1 shows. The magnitude reduction of the coefficients in P_i makes $\tilde{C}_i$ and coefficients of $\tilde{P}_i$ in (42) small in such a way that $\mathrm{mmc}(\tilde{P}_i)$, $\mathrm{mmc}(P_i) \leq \mathrm{O}(\tilde{C}_i)$. The condition $\mathrm{mmc}(\tilde{P}) \leq \mathrm{O}(1)$ is then satisfied by the relation $\tilde{P} = \tilde{P}_i / \tilde{C}_i$ in (43). Therefore, we must solve Eq. (38) with an extra accuracy λ. The value of λ is

$$\lambda \approx -\log_2 |\mathrm{lc}(P_{k-1})|.$$

On abnormal sequence

Suppose $d \equiv \deg(P_k^{(j)}) < \deg(P_{k-1}^{(j)}) - 1$. Then, in the iteration step of calculating $P_{k,j+1}$, $P_k = P_k^{(j)} + \varepsilon^j P_{k,j+1} + \mathrm{O}(\varepsilon^{j+1}(x))$, we may find that $\tilde{P}_i$, the the solution of Eq. (38), satisfies $d < \deg(\tilde{P}_i) < \deg(P_{k-1}^{(1)})$. In such a case, we must split P_k into several polynomials $P_{k,1}$, $P_{k,2}$, $\cdots$, where

$$\deg(P_{k,1}) = d_1 = \deg(\tilde{P}_i), \quad d_1 > \deg(P_{k,2}) > \cdots.$$

The $P_{k,1}$ is nothing but $P_k^{(j+1)}$:

$$P_{k,1} \longleftarrow P_k^{(j+1)} = P_k^{(j)} + \varepsilon^j \tilde{P}. \tag{44}$$

Other polynomials $P_{k,2},\cdots$ are generated by division as

$$\begin{cases} P_{k,0} = P_{k-1}, \\ Q_{k,i} \leftarrow \mathrm{quo}(P_{k,i-1}, P_{k,i}), \quad i = 1,2,\cdots, \\ P_{k,i+1} \leftarrow (P_{k,i-1} - Q_{k,i}P_i)/\max\{1, \mathrm{mmc}(Q_{k,i})\}. \end{cases} \tag{45}$$

This iteration is stopped if we find $P_{k,j}$ such that $\deg(P_{k,j}) = \deg(P_{k+1})$. Then, we modify the signs of P_{k+1}, $P_{k+2},\cdots$ by comparing the sign of $P_{k,j}$ and P_{k+1}, so that the sign of P_{k+1} becomes the same as that of $P_{k,j}$.

6 Performance of algorithm

Let us show the performance of our algorithm by an example.

Example 3.

$$P_1 = (X+1)(X-2)(X-0.5)(X-0.501)(X-0.503)$$

This is the polynomial used in Example 1, where the Sturm sequence was calculated by double-precision floating-point arithmetic. Below, we calculate P_5 and P_6 accurately by using $(P_1, P_2 = [dP_1/dX]/5, P_3, P_4)$ calculated up to 10^{-14} precision. For comparison, we show $A_k^{(j)}P_1 + B_k^{(j)}P_2$ also.

$$P_5^{(1)} = .350E^{-5}X - .175E^{-5}$$
$$A_5^{(1)}P_1 + B_5^{(1)}P_2 = .1E^{-7}X^6 - .1E^{-7}X^5 - .1E^{-7}X^4 + .2E^{-7}X^3 + .349E^{-5}X - .175E^{-5}$$

$$P_5^{(2)} = .349,99969195E^{-5}X - .175,29984617E^{-5}$$
$$A_5^{(2)}P_1 + B_5^{(2)}P_2 = -.1E^{-15}X^3 + .349,99969196E^{-5}X - .175,29984617E^{-5}$$

$$P_5^{(3)} = .349,99969195,11529587E^{-5}X - .175,29984616,86797682E^{-5}$$
$$A_5^{(3)}P_1 + B_5^{(3)}P_2 = .349,99969195,11529586E^{-5}X - .175,29984616,86797682E^{-5}$$

$$P_5^{(4)} = .349,99969195,11529586,61936188E^{-5}X - .175,29984616,86797681,91827946E^{-5}$$
$$\begin{aligned} A_5^{(4)}P_1 + B_5^{(4)}P_2 = \; & -.2E^{-31}X^3 - .1E^{-31}X^2 \\ & +.349,99969195,11529586,61936190E^{-5}X \\ & -.175,29984616,86797681,91827946E^{-5} \end{aligned}$$

$$P_6^{(1)} = 0$$
$$A_6^{(1)}P_1 + B_6^{(1)}P_2 = -.1E^{-7}X^7 + .3E^{-7}X^5 - .3E^{-7}X^4 + .3E^{-7}X^2 - .1E^{-7}X$$

$$P_6^{(2)} = -.19286E^{-11}$$
$$A_6^{(2)}P_1 + B_6^{(2)}P_2 = -.1E^{-15}X^5D + .1E^{-15}X^4 - .2E^{-15}X^2 - .19286E^{-11}$$

$$P_6^{(3)} = -.19285,78751616E^{-11}$$
$$A_6^{(3)}P_1 + B_6^{(3)}P_2 = .1^{-23}X^3 - .1E^{-23}X^2 - .19285,78751617E^{-11}$$

$$P_6^{(4)} = -.19285,78751616,44705762E^{-11}$$
$$A_6^{(4)}P_1 + B_6^{(4)}P_2 = -.1E^{-31}X^5 + .1E^{-31}X^4 + .1E^{-31}X - .19285,78751616,44705762E^{-11}$$

14

References

[1] *Computer Algebra: Symbolic and Algebraic Computation*, B. Buchberger, G.E. Collins and R. Loos, editors, Springer-Verlag, 1982.

[2] G.E. Collins. Real zeros of polynomials. in [1], pages 83–94.

[3] L.E. Heindel. Integer arithmetic algorithms for polynomial real zero determination. *J.ACM*, **18**, 533–548, 1971.

[4] B.W. Char. Floating point isolation of zeros of a real polynomial via macsyma. In *Proc. MACSYMA User's Conference*, pages 53–54, 1977.

[5] T. Sasaki and M. Noda. Approximate square-free decomposition and root-finding of ill-conditioned algebraic equation. *J. Inf. Proces.*, to appear.

[6] T. Sasaki and M. Sasaki. Analysis of accuracy decreasing in polynomial remainder sequence with floating-point number coefficients. *preprint of IPCR*, Jan. 1989.

[7] J. Pinkert. Interval arithmetic applied to polynomial remainder sequences. In *Proc. 1976 Symp. on Symbolic and Algebraic Computation*, pages 214–218, 1976.

[8] M. Lauer. Computing by homomorphic images. In [1], pages 139–168.

[9] A.Schönhage. Quasi-gcd computations. *J.Complexity*, **1**, 118–137, 1985.

[10] R.Loos. Generalized polynomial remainder sequences. In [1], pages 115–138.

[11] T. Sasaki and A. Furukawa. Secondary polynomial remainder sequence and an extension of subresultant theory. *J. Inf. Proces.*, **7**, 175–184, 1984.