

An Algebraic Method for Separating Close-root Clusters and the Minimum Root Separation

Tateaki Sasaki and Fujio Kako

Keywords. close roots, close-root cluster, minimum root separation, separation of close roots.

Abstract. Given a univariate polynomial over \mathbf{C} , we discuss two issues, an algebraic method for separating a factor of mutually close roots from the polynomial, and a reasonable formula for the minimum root separation, by assuming that the close roots form well-separated clusters. The technique we use is very simple and effective; we move the origin near to the center of a close-root cluster, then we are able to treat the other roots collectively, reducing the problem to a very simple one. Following this idea, we present a very simple and stable algebraic method for separating the close-root cluster, derive two lower-bound formulas for the distance between two close roots, and obtain a fairly simple lower bound of the minimum root separation of polynomials over \mathbf{C} .

1. Introduction

In this paper, assuming that a given univariate polynomial contains well-separated clusters of close roots and that the coefficients of the given polynomial can be computed to any required accuracy, 1) we present a new algebraic method for separating the close-root clusters, and 2) we investigate the minimum root separation. Although these two issues are different, we discuss them in a single article because we employ the same approach.

Our technique of attacking the above issues is very simple and effective; it was devised in [TS00] first and used in [IS04] etc. If we move the origin near to the center of a close-root cluster, the coefficients of the shifted polynomial show a peculiar behavior. Using this behavior, we can treat the roots other than those in the cluster collectively, and the problem is reduced to a much simpler one. Furthermore, with this technique, we can usually obtain fairly accurate inequalities, where by *accurate*

inequality we mean that the quantities in the left hand side (l.h.s.) and the right hand side (r.h.s.) are not much different.

Computation of the roots of a univariate polynomial is a very old issue, but it is still posing problems to researchers. In 1990's, several semi-algebraic methods were proposed for factoring a univariate polynomial into two factors numerically hence approximately. Sakurai, Sugiura and Torii [SST92] proposed a method which is based on an Hermite interpolation. Pan [Pan95, Pan96, Pan01] proposed a method using Graeffe's technique and revealed a very good computational complexity of the method. Repeating this factorization recursively, we obtain linear factors hence the roots. The algorithms seem to be quite effective for many polynomials, but actually they become unstable if the given polynomial contains close roots.

In this paper, we consider ill-conditioned polynomials which contain well-separated clusters of close roots. In order to separate factors of close roots, Sasaki and Noda [SN89] proposed an algorithm of approximate square-free decomposition, and Hribernic and Stetter [HS97] presented a similar method. These authors used the polynomial remainder sequence (PRS) in their algorithms. In this paper, assuming that the PRS has been computed by a suitable method, we present a very simple and very stable algorithm for separating a factor containing only a cluster of mutually close roots. The algorithm presented is crucially based on the above-mentioned peculiar behavior of the shifted polynomial.

In computer algebra, there are several quantities for which the theoretical lower or upper bounds differ from the actual values by many orders of magnitudes. The minimum root separation is one of such quantities. Let $A(x)$ be a given square-free polynomial over \mathbf{C} or \mathbf{Z} , of degree $n \geq 3$, having the roots $\alpha_1, \dots, \alpha_n$, where $\alpha_i \neq \alpha_j$ ($\forall i \neq j$). The minimum root separation, or $\text{sep}(A)$ in short, is defined to be $\text{sep}(A) = \min\{|\alpha_i - \alpha_j| \mid 1 \leq i < j \leq n\}$.

So far, many formulas for the lower bound of $\text{sep}(A)$ were presented; see [Mig92]. For polynomials over \mathbf{Z} , Collins and Horowitz [CH74] derived the bound $\text{sep}(A) > \frac{1}{2} e^{-n/2} n^{-3n/2} \|A\|_\infty^{-n}$, where $\|A\|_p$ is the p -norm. A much better lower bound is given by Mignotte [Mig92]: $\text{sep}(A) > n^{-(n+2)/2} D^{1/2} \|A\|_2^{-(n-1)}$, where D denotes the discriminant of $A(x)$. Unfortunately, these theoretical bounds are extraordinary smaller than experimental values. In fact, after many experiments, Collins [Col01] conjectured that $\text{sep}(A) > n^{-n/4} \|A\|_\infty^{-n/2}$. In deriving the theoretical formulas, close roots are not considered so far. The minimum root separation is determined by the closest roots, hence, we are absolutely necessary to take the close roots into account.

In this paper, we will present a new approach to the minimum root separation. The approach is again based on the peculiar behavior of the shifted polynomial. It should be noted that the given polynomial must be treated as accurately as required (by high precision arithmetic in several steps of algorithm). In fact, if the coefficients are perturbed by relative magnitude ε , $0 < \varepsilon \ll 1$, then m multiple or very close roots may be moved as large as $O(\varepsilon^{1/m})$, hence the minimum root

separation will also be changed largely. On the other hand, many authors took an approach to compute multiple roots pretty accurately without using high precision arithmetic, see [Zen03] for example. In this approach, it is assumed (often implicitly) that the given polynomial has multiple roots and no close roots; in other words, a cluster of close roots of a polynomial with truncated coefficients are regarded as multiple roots. Without such an assumption, we cannot compute “multiple” roots by the fixed-precision arithmetic; in fact, the concept of multiple roots can never hold for polynomials with inexact coefficients (we should replace it by “approximately multiple” roots).

In **2**, we review two theorems for distinguishing close roots distributed near the origin from the other roots. We append two new theorems for the cluster of two close roots. The reader will see our technique from the proofs of these theorems. In **3**, we define a normalized PRS and explain characteristic behaviors of the sequence when the given polynomial has close roots. Then, we review a method for finding the locations of the clusters. Finally, we present a very simple and very stable method for separating a factor containing only the close roots in a cluster. In **4**, we derive two lower bounds for the distance between two close roots and obtain a fairly simple lower bound for the minimum root separation. In **5**, we point out open problems being concerned with this work.

2. Gap Theorems on the Roots

In this section, we review two theorems on a cluster of close roots of $A(x)$:

$$A(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x - \alpha_1) \cdots (x - \alpha_n). \quad (2.1)$$

Furthermore, we append two new theorems for special cases. First, we show a well-known lemma; see [Mig92] for the proof.

LEMMA 1. *Let a_n and a_0 be not zero and the roots be ordered as $|\alpha_1| \leq \cdots \leq |\alpha_n|$. Then, $|\alpha_1|$ and $|\alpha_n|$ are bounded as follows.*

$$\frac{|a_0|}{|a_0| + \max\{|a_1|, \dots, |a_n|\}} \leq |\alpha_1| \leq |\alpha_n| \leq \frac{|a_n| + \max\{|a_{n-1}|, \dots, |a_1|\}}{|a_n|}. \quad (2.2)$$

By using this lemma, the following theorems were proved; see [TS00] or [ST02] for the proof of Theorem 1 and [IS04] for the proof of Theorem 2.

THEOREM 1 (Sasaki and Terui). *Let $\bar{A}(x) \in \mathbb{C}[x]$ be*

$$\bar{A}(x) = \bar{a}_n x^n + \cdots + \bar{a}_{m+1} x^{m+1} + 1 \cdot x^m + \bar{e}_{m-1} x^{m-1} + \cdots + \bar{e}_0, \quad (2.3)$$

where the coefficients satisfy

$$\begin{cases} \max\{|\bar{a}_n|, \dots, |\bar{a}_{m+1}|\} = 1, \\ \bar{e} \stackrel{\text{def}}{=} \max\{|\bar{e}_{m-1}|^{1/1}, |\bar{e}_{m-2}|^{1/2}, \dots, |\bar{e}_0|^{1/m}\} \ll 1. \end{cases} \quad (2.4)$$

If $\bar{e} < 1/9$ then $\bar{A}(x)$ has m small roots inside a disc \bar{D}_{in} of radius \bar{R}_{in} and other $n-m$ roots outside a disc \bar{D}_{out} of radius \bar{R}_{out} , located at the origin, where

$$\bar{R}_{\text{in(out)}} = \frac{(1 + 3\bar{e}) - (+)\sqrt{(1 + 3\bar{e})^2 - 16\bar{e}}}{4}. \quad (2.5)$$

COROLLARY 1. Each root in the close-root cluster located at the origin, of $\bar{A}(x)$ is separated from other $n-m$ roots at least by $\bar{R}_{\text{out}} - \bar{R}_{\text{in}} = \frac{1}{2}\sqrt{(1+3\bar{e})^2 - 16\bar{e}}$.

THEOREM 2 (Inaba and Sasaki). Let $m = 1$ in (2.3) and put $\hat{e} = |\bar{e}_0|$. If $\hat{e} < 1/(3+2\sqrt{2})$ then $\bar{A}(x)$ has one small root inside a disc \hat{D}_{in} of radius \hat{R}_{in} and other $n-1$ roots outside a disc \hat{D}_{out} of radius \hat{R}_{out} , located at the origin, where

$$\hat{R}_{\text{in(out)}} = \frac{(1 + \hat{e}) - (+)\sqrt{(1 + \hat{e})^2 - 8\hat{e}}}{4}. \quad (2.6)$$

COROLLARY 2. For $m = 1$, the smallest root around the origin of $\bar{A}(x)$ is separated from other $n-1$ roots at least by $\hat{R}_{\text{out}} - \hat{R}_{\text{in}} = \frac{1}{2}\sqrt{(1+\hat{e})^2 - 8\hat{e}}$.

\bar{R}_{in} and \bar{R}_{out} (and \hat{R}_{in} and \hat{R}_{out} , too) are two roots of a quadratic polynomial. \hat{R}_{in} and \hat{R}_{out} were obtained first by Wang and Han in [WH90], in a study of Newton's method for computing a root of univariate polynomial. \bar{R}_{in} was obtained also by Yakoubsohn [Yak00] by a different approach, but he did not obtain \bar{R}_{out} . How accurately the formula (2.5) bounds the actual roots was investigated numerically by Sasaki and Terui [ST02], which revealed that the formula bounds the actual roots fairly well.

2.1. Special two cases of $m = 2$

In this paper, we are interested in the case that only two close roots form a cluster. In this subsection, we specialize the above theorems for the case of $m = 2$.

We first consider the case that the origin is very close to one of the two close roots. If we perform a scale transformation so that the cluster size becomes $O(1)$, the polynomial $A(x)$ will be transformed to the following regularized form.

$$\begin{cases} \bar{A}_2(x) = \bar{a}_n d^{n-2} x^n + \cdots + \bar{a}_3 d x^3 + \bar{a}_2 x^2 + x + \bar{e}_0, \\ 0 < d \ll 1, \quad 0 < |\bar{e}_0| \ll 1, \\ \max\{|\bar{a}_n|, \dots, |\bar{a}_3|\} = |\bar{a}_2| = 1. \end{cases} \quad (2.7)$$

We can transform $\bar{A}(x)$ in (2.3), with $m = 2$, to the polynomial $\bar{A}_2(x)$ in (2.7), as follows. If $|\bar{e}_1|^2 \gg |\bar{e}_0|$ then put $\bar{A}_2(x) = \bar{A}(\bar{e}_1 x)/\bar{e}_1^2$. Otherwise, compute $\bar{A}'(x) = \bar{A}(x + \alpha') \stackrel{\text{def}}{=} a'_n x^n + \cdots + a'_2 x^2 + a'_1 x + a'_0$, with $\alpha' = (-\bar{e}_1 + \sqrt{\bar{e}_1^2 - 4\bar{e}_0})/2$, and put $\bar{A}_2(x) = \bar{A}'(a'_1 x/a'_2) \cdot a'_2/(a'_1)^2$. Note that $|\alpha'| \ll 1$ because $\max\{|\bar{e}_1|, |\bar{e}_0|^{1/2}\} \ll 1$.

$\bar{A}_2(x)$ has one small root near the origin, let it be $\hat{\gamma}$. Let $\check{\gamma}$ be a root of $\bar{A}_2(x)$, other than $\hat{\gamma}$, then we have $|\check{\gamma}| \gtrsim 0.5$. For $\bar{A}_2(x)$, we can strengthen Theorem 2 as follows.

THEOREM 3. Put $\hat{e} = |\bar{e}_0|$ for simplicity. If $\hat{e} < 1/[(2+d) + 2\sqrt{1+d}]$ then $\bar{A}_2(x)$ has one small root inside a disc \hat{D}_{in} of radius \hat{R}_{in} and other $n-1$ roots outside a disc \hat{D}_{out} of radius \hat{R}_{out} , located at the origin, where

$$\hat{R}_{\text{in(out)}} = \frac{(1 + d\hat{e}) - (+)\sqrt{(1 + d\hat{e})^2 - 4(1 + d)\hat{e}}}{2(1 + d)}. \quad (2.8)$$

COROLLARY 3. The smallest root $\hat{\gamma}$ around the origin of $\bar{A}_2(x)$ is separated from other $n-1$ roots at least by $\sqrt{(1 + d\hat{e})^2 - 4(1 + d)\hat{e}}/(1 + d)$.

Proof Equality $\bar{A}_2(\hat{\gamma}) = 0$ gives us $\hat{\gamma} \cdot (\bar{a}_n d^{n-2} \hat{\gamma}^{n-1} + \dots + \bar{a}_3 d \hat{\gamma}^2 + \bar{a}_2 \hat{\gamma} + 1) = -\bar{e}_0$. Since $|\hat{\gamma}| \ll 1$, we obtain

$$\begin{aligned} |\hat{\gamma}| &= \hat{e} / |1 + \bar{a}_2 \hat{\gamma} + \bar{a}_3 d \hat{\gamma}^2 + \dots + \bar{a}_n d^{n-2} \hat{\gamma}^{n-1}| \\ &\leq \hat{e} / \{1 - |\hat{\gamma}| - d|\hat{\gamma}|^2 - \dots - d^{n-2} |\hat{\gamma}|^{n-1}\} \\ &< \hat{e} / \{1 - |\hat{\gamma}|/(1 - d|\hat{\gamma}|)\} \\ \implies (1 + d)|\hat{\gamma}|^2 - (1 + d\hat{e})|\hat{\gamma}| + \hat{e} &> 0. \end{aligned}$$

The last inequality holds only if $(1 + d\hat{e})^2 - 4(1 + d)\hat{e} > 0$, or $\hat{e} < 1/[(2+d) + 2\sqrt{1+d}]$. With this condition, the above last inequality gives us the bound \hat{R}_{in} for $|\hat{\gamma}|$.

Next, consider $d^2 \bar{A}_2(x/d) \stackrel{\text{def}}{=} \tilde{A}_2(x) = \bar{a}_n x^n + \dots + \bar{a}_2 x^2 + dx + d^2 \bar{e}_0$. $\tilde{A}_2(x)$ has a root $d\check{\gamma}$, and we put $\gamma = d\check{\gamma}$ for simplicity. Dividing $\tilde{A}_2(\gamma) = 0$ by γ , we obtain equality $\bar{a}_n \gamma^{n-1} + \dots + \bar{a}_2 \gamma + \bar{a}_1 = 0$, where $\bar{a}_1 = d(1 + d\bar{e}_0/\gamma)$. We see $|\bar{a}_1| \simeq d \ll 1$ because $|\check{\gamma}| \gtrsim 0.5$. We regard this equality as an equation in γ , of degree $n-1$ with the constant term \bar{a}_1 , and apply formula (2.2) to it. (We can state this situation as follows. Consider a set of polynomials $\{\bar{a}_n z^{n-1} + \dots + \bar{a}_2 z + \bar{a}_1 \mid |\bar{a}_1| \leq \bar{a}\}$, where \bar{a} is so chosen that the set contains a polynomial having the root γ . Since \bar{a}_1 is a number, we can apply formula (2.2) to every polynomial in the set.) Then, we obtain

$$\begin{aligned} |\gamma| &\geq \frac{1}{1 + 1/|\bar{a}_1|} \geq \frac{1}{1 + 1/(d - d^2 \hat{e}/|\gamma|)} \\ \implies (1 + d)|\gamma|^2 - d(1 + d\hat{e})|\gamma| + d^2 \hat{e} &\geq 0 \\ \text{or } (1 + d)|\check{\gamma}|^2 - (1 + d\hat{e})|\check{\gamma}| + \hat{e} &\geq 0. \end{aligned}$$

We have obtained the same polynomial for both $|\hat{\gamma}|$ and $|\check{\gamma}|$. Since $\check{\gamma}$ is not the smallest root, we obtain the bound \hat{R}_{out} for $|\check{\gamma}|$. The $\hat{\gamma}$ is separated from other $n-1$ roots by at least $\hat{R}_{\text{out}} - \hat{R}_{\text{in}}$, which proves the corollary. \square

Next, we consider the case that the origin is near to the center of close-root cluster. That is, instead of $\bar{A}_2(x)$ in (2.7), we consider $\bar{A}_2(x)$ regularized as follows.

$$\begin{cases} \bar{A}_2(x) = \bar{a}_n x^n + \dots + \bar{a}_3 x^3 + x^2 + \bar{e}_1 x + \bar{e}_0, & |\bar{e}_1| < |\bar{e}_0|, \\ \max\{|\bar{a}_n|, \dots, |\bar{a}_3|\} = 1, & \bar{e} \stackrel{\text{def}}{=} \max\{|\bar{e}_1|, |\bar{e}_0|^{1/2}\} \ll 1. \end{cases} \quad (2.9)$$

We can transform $\bar{A}(x)$ in (2.3), with $m = 2$, to the polynomial $\bar{A}_2(x)$ in (2.9), as follows. Compute $\bar{A}'(x) = \bar{A}(x - \bar{e}_1/2) \stackrel{\text{def}}{=} a'_n x^n + \cdots + a'_2 x^2 + a'_1 x + a'_0$, and put $\bar{A}_2(x) = \bar{A}'(x/\eta) \cdot \eta^2/a'_2$, where $\eta = \max\{|a'_3/a'_2|^{1/1}, |a'_4/a'_2|^{1/2}, \dots, |a'_n/a'_2|^{1/(n-2)}\}$.

$\bar{A}_2(x)$ has two small roots around the origin, let one of them be $\hat{\gamma}$, and any other root $\check{\gamma}$ of $\bar{A}_2(x)$ is such that $\check{\gamma} \gtrsim 0.5$.

THEOREM 4. *Let a polynomial $P_2(r)$ be defined as*

$$P_2(r) = 2r^3 - (1 + |\bar{e}_1|)r^2 + (|\bar{e}_1| - |\bar{e}_0|)r + |\bar{e}_0|. \quad (2.10)$$

If \bar{e}_1 and \bar{e}_0 in (2.9) are such that $P_2(r)$ has two real positive roots \bar{R}_{in} and \bar{R}_{out} , with $\bar{R}_{\text{in}} < \bar{R}_{\text{out}}$, then $\bar{A}_2(x)$ has two small roots inside a disc \bar{D}_{in} of radius \bar{R}_{in} and $n-2$ roots outside a disc \bar{D}_{out} of radius \bar{R}_{out} , located at the origin. The conditions for $P_2(r)$ having two real positive roots are

$$\begin{cases} \text{Condition 1 : } & |\bar{e}_1| < |\bar{e}_0|, \\ \text{Condition 2 : } & R < 0, \end{cases} \quad (2.11)$$

where $R = |\bar{e}_1|^4 - |\bar{e}_1|^3(6 - 2|\bar{e}_0|) + |\bar{e}_1|^2(1 - 4|\bar{e}_0| + |\bar{e}_0|^2) - |\bar{e}_1|(26|\bar{e}_0| - 14|\bar{e}_0|^2) + (4|\bar{e}_0| - 71|\bar{e}_0|^2 + 8|\bar{e}_1|^3)$.

COROLLARY 4. *The two small roots around the origin, of $\bar{A}_2(x)$ are separated from other $n-2$ roots at least by*

$$\bar{R}_{\text{out}} - \bar{R}_{\text{in}}. \quad (2.12)$$

Proof $\bar{A}_2(x)$ has a root $\check{\gamma}$. Denoting $\check{\gamma}$ by γ and dividing $\bar{A}_2(\gamma)$ by γ^2 , we obtain $0 = \bar{a}_n \gamma^{n-2} + \cdots + \bar{a}_3 \gamma + \bar{a}_2$, where $\bar{a}_2 = 1 + \bar{e}_1/\check{\gamma} + \bar{e}_0/\check{\gamma}^2$. We see $|\bar{a}_2| \simeq 1$ because $|\check{\gamma}| \gtrsim 0.5$. We regard the above r.h.s. expression as a polynomial in γ of degree $n-2$ with the constant term \bar{a}_2 , and apply formula (2.2) to it. Then, we obtain the following inequality for $\check{\gamma}$.

$$\begin{aligned} |\check{\gamma}| &\geq \frac{1}{1 + 1/|\bar{a}_2|} \geq \frac{1}{1 + 1/(1 - |\bar{e}_1|/|\check{\gamma}| - |\bar{e}_0|/|\check{\gamma}|^2)} \\ \implies & 2|\check{\gamma}|^3 - (1 + |\bar{e}_1|)|\check{\gamma}|^2 + (|\bar{e}_1| - |\bar{e}_0|)|\check{\gamma}| + |\bar{e}_0| \geq 0. \end{aligned}$$

Next, consider $\bar{A}_2(ex)/e^2 \stackrel{\text{def}}{=} \tilde{A}_2(x) = \bar{a}_n e^{n-2} x^n + \cdots + \bar{a}_3 e x^3 + x^2 + (\bar{e}_1/e)x + (\bar{e}_0/e^2)$, where $e = \bar{e}$. $\tilde{A}_2(x)$ has a root $\hat{\gamma}/e$. Putting $\gamma = \hat{\gamma}/e$, we have $\gamma^2 \cdot \{\bar{a}_n (e\gamma)^{n-2} + \cdots + \bar{a}_3 (e\gamma) + 1\} = -(\bar{e}_1/e)\gamma - (\bar{e}_0/e^2)$. Since we have $e|\gamma| = |\hat{\gamma}| \ll 1$, we obtain the following inequality for $\hat{\gamma}$.

$$\begin{aligned} (|\bar{e}_1|/e)|\gamma| + (|\bar{e}_0|/e^2) &\geq |\gamma|^2 \cdot (1 - |e\gamma| - \cdots - |e\gamma|^{n-2}) \\ &> |\gamma|^2 \cdot \{1 - e|\gamma|/(1 - e|\gamma|)\} \\ \implies & 2e^3|\gamma|^3 - (1 + |\bar{e}_1|)e^2|\gamma|^2 + (|\bar{e}_1| - |\bar{e}_0|)e|\gamma| + |\bar{e}_0| > 0 \\ \text{or } & 2|\hat{\gamma}|^3 - (1 + |\bar{e}_1|)|\hat{\gamma}|^2 + (|\bar{e}_1| - |\bar{e}_0|)|\hat{\gamma}| + |\bar{e}_0| > 0. \end{aligned}$$

We have obtained the same polynomial $P_2(r)$ for both $\hat{\gamma}$ and $\check{\gamma}$. Since $P_2(0) = |\bar{e}_0| > 0$, $P_2(r)$ has at least one negative root. Since $|\hat{\gamma}|$ and $|\check{\gamma}|$ must be two roots of $P_2(r)$, we have conditions in (2.11). \square

Condition 2 in (2.11) is complicated to obtain the general solution, so we estimate the values of \bar{e} and \bar{R}_{in} for the following three cases.

$$\begin{aligned} \text{Case 1 : } |\bar{e}_1| = 0 \text{ and } |\bar{e}_0| = \bar{e}^2 &\implies \bar{e} \approx 0.23812, \quad \bar{R}_{\text{in}} \approx 0.3596, \\ \text{Case 2 : } 5|\bar{e}_1| = |\bar{e}_0| = \bar{e}^2 &\implies \bar{e} \approx 0.23002, \quad \bar{R}_{\text{in}} \approx 0.3566, \\ \text{Case 3 : } 2|\bar{e}_1| = |\bar{e}_0| = \bar{e}^2 &\implies \bar{e} \approx 0.21938, \quad \bar{R}_{\text{in}} \approx 0.3527, \end{aligned}$$

The value of \bar{R}_{in} in Theorem 4 is much larger than those in Theorems 1 and 2. However, Theorem 4 is less useful practically than Theorems 1 and 2, because the first condition in (2.11) is quite restrictive.

3. Separating Clusters of Close Roots

In this section, by $\text{quo}(A, B)$, $\text{rem}(A, B)$ and $\text{lc}(A)$, we denote the quotient and remainder of A divided by B and the leading coefficient of A , respectively. By $\|P\|$ we denote the infinity norm of polynomial P .

First of all, we note that the theorems in **2** can be generalized directly to polynomials with inexact coefficients, so long as the error bound of each coefficient is known. Here, we state the generalization for Theorem 1 only.

PROPOSITION 1. *Let the coefficients $\bar{a}_n, \dots, \bar{a}_{m+1}, \bar{e}_{m-1}, \dots, \bar{e}_0$ of $\bar{A}(x)$ in Theorem 1 contain small errors which are bounded respectively by $\varepsilon_n, \dots, \varepsilon_{m+1}, \varepsilon_{m-1}, \dots, \varepsilon_0$. Theorem 1 is valid if we regularize $\bar{A}(x)$ as $\max\{|a_n| + \varepsilon_n, \dots, |a_{m+1}| + \varepsilon_{m+1}\} = 1$ and define \bar{e} as $\bar{e} = \max\{(|\bar{e}_{m-1}| + \varepsilon_{m-1})^{1/1}, (|\bar{e}_{m-2}| + \varepsilon_{m-2})^{1/2}, \dots, (|\bar{e}_0| + \varepsilon_0)^{1/m}\}$.*

We assume that $A(x)$ is monic and regularized as

$$a_n = \max\{|a_{n-1}|, \dots, |a_0|\} = 1. \quad (3.1)$$

With this regularization, Lemma 1 tells us that any root α of $A(x)$ is bounded as $|\alpha| \leq 2$. Therefore, if two different roots α_i and α_j of $A(x)$ are such that $|\alpha_i - \alpha_j| \ll 1/n$ then we can say that α_i and α_j are *mutually close roots of closeness* $|\alpha_i - \alpha_j|$. We consider the case that close roots of $A(x)$ form clusters of different sizes $O(\delta_1), \dots, O(\delta_\tau)$, with $1/n \gg \delta_1 \gg \dots \gg \delta_\tau$ (τ may be 1), and that each cluster of size $O(\delta_i)$ is separated from other roots by distance $\gg \delta_i$. Let the number of close roots of closeness $\leq O(\delta_i)$ be m_i ($i = 1, \dots, \tau$), and the close roots of closeness $O(\delta_i)$ be distributed among ℓ_i clusters ($i = 1, \dots, \tau$). A bigger cluster may contain several smaller clusters. We define the *center of the cluster* to be the average value of the close roots in the cluster.

3.1. Normalized PRS (polynomial remainder sequence)

Putting $P_1 = A(x)$, $P_2 = \frac{1}{n} dA/dx$, $S_1 = T_2 = 1$ and $S_2 = T_1 = 0$, we generate a PRS $(P_1, P_2, P_3, P_4, \dots)$ and cofactor sequences $(S_1, S_2, S_3, S_4, \dots)$ and

$(T_1, T_2, T_3, T_4, \dots)$, by the following formulas.

$$\begin{cases} q_j &:= \text{quo}(P_{j-1}, P_j), \\ P_{j+1} &:= (P_{j-1} - q_j P_j)/w_j, \\ S_{j+1} &:= (S_{j-1} - q_j S_j)/w_j, \\ T_{j+1} &:= (T_{j-1} - q_j T_j)/w_j, \end{cases} \quad (j = 2, 3, \dots), \quad (3.2)$$

where w_j is a number to be chosen to satisfy

$$\max\{\text{lc}(S_{j+1}), \text{lc}(T_{j+1})\} = 1 \quad (j = 2, 3, \dots). \quad (3.3)$$

We call the PRS generated by the formulas in (3.2) **normalized PRS**.

Remark 1 We call a quantity Q **shift-invariant** if $Q = Q'$, where Q' is the same quantity as Q but computed after shifting the origin arbitrarily. The l.h.s. quantity in (3.3) is shift-invariant, hence $\text{lc}(P_{j+1})$ ($j = 2, 3, \dots$) are shift-invariant. In [SS97] and [Sas03], the normalization formula $\max\{\|S_{j+1}\|, \|T_{j+1}\|\} = 1$ is used. If $A(x)$ is regularized, the PRS's normalized by both formulas are almost the same. \square

Let indices k_1, k_2, \dots, k_τ be such that

$$\deg(P_{k_i}) = m_i - \ell_i \quad (i = 1, 2, \dots, \tau). \quad (3.4)$$

$\deg(P_{k_i})$ is equal to the number of roots of dA/dx , of closeness $\leq O(\delta_i)$, distributed among ℓ_i clusters, and P_{k_i} is an approximate common divisor of $A(x)$ and dA/dx .

The normalized PRS behaves as follows, see [SS89] and [Sas03].

- 1): We have $\|P_j\| = O(\delta_1^0)$ for $j \leq k_1$ (i.e., $\|P_j\|$ does not decrease much until the remainder becomes an approximate GCD of A and dA/dx).
- 2): For each $i = 1, \dots, \tau$, we have $\|P_{k_i+1}\|/\|P_{k_i}\| = O(\delta_i^2)$ (i.e., P_{k_i} is an approximate common divisor of A and dA/dx , of tolerance $O(\delta_i^2)$).
- 3): If $A(x)$ contains only one cluster of size $O(\delta_1)$, we call the PRS **single-cluster type**. For $j > k_1$, the PRS of single-cluster type behaves as $\|P_{k_1+j}\| = O(\delta_1^{2j})$ for $j = 1, 2, \dots$ (until we encounter smaller clusters).
- 4): If $A(x)$ contains two or more clusters of size $O(\delta_1)$, we call the PRS **multiple-cluster type**. For $j > k_1$, the PRS of multiple-cluster type behaves as $\|P_{k_1+j+1}\|/\|P_{k_1+1}\| = O(\delta_1^0)$ for $1 \leq j < \ell_1$, $\|P_{k_1+\ell_1+1}\|/\|P_{k_1+1}\| = O(\delta_1^2)$, and so on. That is, ℓ successive remainder computations strip ℓ close roots from the ℓ clusters, one root from each cluster, without changing the norm of remainders much until the ℓ close roots are stripped. The PRS may become of single-cluster type after being stripped off all the close roots of closeness $O(\delta_1)$.

It should be emphasized that single- and multiple-cluster types are clearly distinguished from each other by the behavior of normalized PRS.

Remark 2 From the viewpoint of elimination, the elements of PRS are unique up to constant factors. From the viewpoint of computation, however, the accuracy of the result depends very much on the algorithm used; in fact, the conventional

Euclidean algorithm causes large cancellations errors if small leading coefficients appear during the computation. This instability can be removed largely (but not always) by performing the elimination carefully. For example, Ohsako et al. [OST97] utilized the Givens transformation which works nicely for removing the cancellation errors. One may compute an approximate GCD of $P_1(x)$ and $P_2(x)$ by a stable method such as proposed by Corless et al. [CWZ02]. \square

3.2. Finding the location of a cluster

Finding the location of clusters of close roots has already been discussed in [SN89] and [HS97]. Here, we briefly survey the method.

We first consider the single-cluster case. Assume that the normalized PRS for $A(x)$ is of single-cluster type (hence, $\ell_1 = 1$), and put $\delta_1 = \delta$, $k_1 = k$ and $m_1 = m$. Let the mutually close roots in the cluster be $\alpha_1, \dots, \alpha_m$ and α_c the cluster center: $\alpha_c = (\alpha_1 + \dots + \alpha_m)/m$. We express $P_k(x)$ and define α'_c as

$$\begin{cases} P_k(x) = p_{m-1}x^{m-1} + p_{m-2}x^{m-2} + \dots + p_0, \\ \alpha'_c \stackrel{\text{def}}{=} \frac{-1}{m-1} p_{m-2}/p_{m-1}. \end{cases} \quad (3.5)$$

We will show in **3.2** that $|\alpha'_c - \alpha_c| = O(\delta^2)$, hence α'_c is very close to the cluster center α_c . Furthermore, we can know the cluster size δ approximately by the ratio $\|P_{k+1}\|/\|P_k\| = O(\delta^2)$.

The fact $\|P_{k+1}\|/\|P_k\| = O(\delta^2)$ shows that the above mentioned method will work quite well for clusters of small sizes such as $\delta \lesssim 10^{-3}$ or 10^{-4} . So, in the example below, we check the method by a cluster of very large size $\sim 10^{-1}$.

Example 1 (single-cluster type) Let $A(x)$ be as follows.

$$A = (x^2 - 1)(x - 0.30)(x - 0.31)(x - 0.35)(x^2 - 0.60x + 0.0925).$$

$A(x)$ has five close roots of closeness ~ 0.05 at $x \sim 0.3$ ($\alpha_c = 0.312$), and the normalized PRS shows that $\|P_5\|/\|P_4\| \sim 0.0021 \approx (0.05)^2$. Determining α'_c by P_4 as described above, we obtain $\alpha'_c = 0.31139\dots$. Shifting the origin to α'_c , we obtain $A'(x) \stackrel{\text{def}}{=} A(x + \alpha'_c)$ and $P'_4 \stackrel{\text{def}}{=} P_4(x + \alpha'_c)$ as follows.

$$\begin{aligned} A'(x) &= x^7 + 0.61977\dots x^6 - 0.90334\dots x^5 + 0.00300\dots x^4 - 0.00010\dots x^3 \\ &\quad + 0.70895\dots \times 10^{-4}x^2 + 0.11466 \times 10^{-5}x - 0.14589\dots \times 10^{-8}, \\ P'_4 &= -0.15544\dots x^4 - 1.0000\dots \times 10^{-4}x^2 + \dots + 4.0545\dots \times 10^{-8}. \end{aligned}$$

Observe that the x^4 -term of $A'(x)$ is abnormally small ($\sim (0.05)^2$) and that x^i -terms ($i \leq 3$) of $A'(x)$ decrease steadily as i decreases. \square

We next consider the case of multiple clusters. Assume that $A(x)$ contains ℓ clusters of close roots of closeness $O(\delta)$, with $\ell > 1$, then $A(x)$ must be of the following form.

$$A(x) = \tilde{A}(x)(x - \alpha'_1)^{\mu_1} \dots (x - \alpha'_\ell)^{\mu_\ell} C(x) + O(\delta^2), \quad \mu_1 \geq \dots \geq \mu_\ell. \quad (3.6)$$

Here, α'_i is an approximate center of the i th cluster ($i=1, \dots, \ell$), $\tilde{A}(x)$ represents the factor of all the non-close roots, and $C(x)$ represents the factor of close roots of smaller closenesses.

Given $A(x)$, we generate the following normalized PRS for $i=1 \Rightarrow 2 \Rightarrow \dots \Rightarrow \mu_1$ successively, where $P^{(0)} = A(x)$.

$$\left\{ \begin{array}{l} (P_1^{(i)} = P^{(i-1)}, P_2^{(i)} = \frac{1}{\deg(P^{(i-1)})} dP^{(i-1)}/dx, \dots, P_{k_i}^{(i)} \stackrel{\text{def}}{=} P^{(i)}, P_{\text{last}}^{(i)}), \\ \|P_j^{(i)}\| = O(\delta^0) \quad (j \leq k_i), \quad \|P_{\text{last}}^{(i)}\| \leq O(\delta^2). \end{array} \right. \quad (3.7)$$

Note that $P^{(1)}, P^{(2)}, \dots$ are determined by large decreases of $\|P_{\text{last}}^{(1)}\|, \|P_{\text{last}}^{(2)}\|, \dots$. Then, for index $i < \mu_\ell$, we have $P^{(i)} \propto (x-\alpha'_1)^{\mu_1-i} \dots (x-\alpha'_\ell)^{\mu_\ell-i} C(x) + O(\delta^2)$. For index $\mu_\ell \leq i \leq \mu_1$, we have $P^{(i)} \propto (x-\alpha'_1)^{\mu_1-i} \dots (x-\alpha'_r)^{\mu_r-i} C(x) + O(\delta^2)$, where $1 < r < \ell$. Therefore, we can obtain square-free factors of the product $(x-\alpha'_1)^{\mu_1} \dots (x-\alpha'_\ell)^{\mu_\ell}$ by computing the quotients of $P^{(i-1)}$ by $P^{(i)}$ ($1 \leq i \leq \mu_1$) successively. For example, if $\mu_1 = \dots = \mu_r > \mu_{r+1} = \dots = \mu_\ell$ we will obtain the following polynomials.

$$\begin{aligned} P^{(\mu_\ell-1)} &\simeq C(x) \cdot [(x-\alpha'_1) \dots (x-\alpha'_r)]^{\mu_1-\mu_\ell+1} \cdot [(x-\alpha'_{r+1}) \dots (x-\alpha'_\ell)], \\ P^{(\mu_1-1)} &\simeq C(x) \cdot [(x-\alpha'_1) \dots (x-\alpha'_r)], \\ P^{(\mu_1)} &\simeq C(x). \end{aligned}$$

Thus, we have $\text{quo}(P^{(\mu_1-1)}, P^{(\mu_1)}) \approx (x-\alpha'_1) \dots (x-\alpha'_r)$ and $\text{quo}(P^{(\mu_\ell-1)}, P^{(\mu_\ell)}) \approx (x-\alpha'_1) \dots (x-\alpha'_\ell)$. Finally, computing the roots of approximately square-free factors $(x-\alpha'_1) \dots (x-\alpha'_r)$ and $(x-\alpha'_{r+1}) \dots (x-\alpha'_\ell)$, we can find the approximate locations of the clusters.

Remark 3 Separating the approximate factor $(x-\alpha'_1)^{\mu_1} \dots (x-\alpha'_\ell)^{\mu_\ell}$ in (3.6) to factors of the same “multiplicity” is the most unstable step of our method; this point was discussed to some extent in [SN89]. If close-root clusters are closer, the separation becomes more unstable. This fact forces us to assume that the close-root clusters are well separated each other. This instability will be reduced much if we adopt such “least square algorithms” as were used in [Zen03]. \square

3.3. A basic problem on PRS

Let $B(x)$ be a polynomial regularized as $A(x)$ in (3.1). If $A(x)$ and $B(x)$ have mutually close roots of closeness $O(\delta)$, the normalized PRS of $P_1 = A(x)$ and $P_2 = B(x)$ gives us $\|P_{k_1+1}\| = O(\delta)$ in general. In the case of $B(x) = \frac{1}{\deg(A)} dA/dx$, however, we have $\|P_{k_1+1}\| = O(\delta^2)$. This means that the normalized PRS gives us fairly accurate information on the close-root clusters. However, we have currently no answer to the following basic problem.

Problem: By using the PRS, determine fairly accurate upper bounds of the size and the location of the close-root cluster of $A(x)$.

Determining fairly accurate *a priori* upper bounds of δ and α_c is not easy. We can, however, determine an *a posteriori* upper bound of δ so long as δ is small. We

shift the origin to α'_c , an approximate center of the close-root cluster, determined in 3.2. We express $A(x + \alpha'_c)$ as follows.

$$A(x + \alpha'_c) \stackrel{\text{def}}{=} A'(x) = a'_n x^n + \cdots + a'_m x^m + \cdots + a'_0. \quad (3.8)$$

Then, we have (see [Sas03] for the proof; see also Example 1)

$$|a'_{m-1}/a'_m| = O(\delta^2), \quad |a'_{m-j}/a'_m| = O(\delta^j) \quad (j = 2, 3, \dots). \quad (3.9)$$

Note that the coefficients of x^{m-2} , x^{m-3} , \dots , x^0 -terms of $A'(x)$ decrease steadily, hence we will be able to apply Theorem 1 to $A'(x)$.

PROPOSITION 2. *Let $1/d = \max\{|a'_{m+1}/a'_m|, |a'_{m+2}/a'_m|^{1/2}, |a'_n/a'_m|^{1/(n-m)}\}$, and put $\bar{e} = e/d$. If $\bar{e} < 1/9$ then the cluster size δ is bounded as $\delta < \bar{R}_{\text{in}} d$, where \bar{R}_{in} is defined in (2.5). \square*

As for α'_c , the problem is much more difficult. So, we give only an order estimation, which is simple. Since the leading coefficients of elements of the normalized PRS are shift-invariant, we can consider the PRS by shifting the origin to a favorite point. Thus, moving the origin to the cluster center α_c , we express $A(x)$ and P_k as

$$\begin{cases} A(x) &= a''_n (x - \alpha_c)^n + \cdots + a''_m (x - \alpha_c)^m + \cdots + a''_0, \\ P_k &= p''_{m-1} (x - \alpha_c)^{m-1} + p''_{m-2} (x - \alpha_c)^{m-2} + \cdots + p''_0. \end{cases} \quad (3.10)$$

PROPOSITION 3. *We have $|\alpha'_c - \alpha_c| = O(\delta^2)$.*

Proof We note that $\alpha'_c - \alpha_c = \frac{-1}{m-1} p''_{m-2}/p''_{m-1}$. Since α_c is the center of roots $\alpha_1, \dots, \alpha_m$, we have $a''_m = O(\delta^0)$ and $a''_{m-1} = O(\delta^2)$. As shown in [Sas03] by using the subresultant, this fact gives us $p''_{m-1} = O(\delta^0)$ and $p''_{m-2} = O(\delta^2)$, proving the proposition. \square

3.4. Separating the factor of a close-root cluster

In this subsection, we consider to separate a factor of $A(x)$ to arbitrary accuracy, where the factor contains only m mutually close roots of closeness $\leq O(\delta)$, with $\delta = \delta_1$. (Applying the separation algorithm recursively, we can separate any close-root cluster of size $O(\delta_i)$).

We already know α'_c , an approximate cluster center. First, we move the origin to α'_c , and compute $A'(x) = A(x + \alpha'_c)$ given in (3.8). Next, we compute the following number e .

$$e = \max\{|a'_{m-1}/a'_m|, |a'_{m-2}/a'_m|^{1/2}, \dots, |a'_0/a'_m|^{1/m}\}. \quad (3.11)$$

Using e , we transform $A'(x)$ to the following regularized form:

$$\begin{cases} \bar{A}(x) \stackrel{\text{def}}{=} A'(ex)/a'_m e^m = \bar{a}_n x^n + \cdots + 1 \cdot x^m + \bar{a}_{m-1} x^{m-1} + \cdots + \bar{a}_0, \\ d \stackrel{\text{def}}{=} \max\{|\bar{a}_n|^{1/(n-m)}, \dots, |\bar{a}_{m+1}|^{1/1}\}, \quad \max\{|\bar{a}_{m-1}|, \dots, |\bar{a}_0|\} = 1. \end{cases} \quad (3.12)$$

By assumptions, e must be a small number of magnitude $O(\delta)$, and so is d .

We want to factor $\bar{A}(x)$ as $\bar{A}(x) = H(x)C(x)$, where $C(x) = x^m + c_{m-1}x^{m-1} + \dots + c_0$. $H(x)$ can be expressed as $H(x) = 1 + d h_1 x + d^2 h_2 x^2 + \dots + d^{n-m} h_{n-m} x^{n-m}$, where d is given in (3.12) and $\max\{|h_1|, |h_2|, \dots, |h_{n-m}|\} \approx 1$.

Since we assumed d to be small enough, the lower degree terms $x^m + \bar{a}_{m-1}x^{m-1} + \dots + \bar{a}_0$ of $\bar{A}(x)$ is approximately equal to $C(x)$. Therefore, we can determine $H(x)$ and $C(x)$ iteratively as follows. As initial approximations, put $H(x) \approx H^{(0)} = 1$ and $C(x) \approx C^{(0)} = x^m + \bar{a}_{m-1}x^{m-1} + \dots + \bar{a}_0$. Expressing $\bar{A}(x)$ as $\bar{A}(x) = [1 + \Delta_H] \cdot [C^{(0)} + \Delta_C]$, where $\Delta_H = O(d)$, $\Delta_C = O(d)$, $\deg(\Delta_H) < n-m$ and $\deg(\Delta_C) < m$, we have $\bar{A}(x) - C^{(0)} = \Delta_H C^{(0)} + \Delta_C + O(d^2)$. Thus, Δ_H and Δ_C up to $O(d)$ are equal to the quotient and the remainder, respectively, of $\bar{A}(x) - C^{(0)}$ divided by $C^{(0)}$: $\Delta_H = \text{quo}(\bar{A} - C^{(0)}, C^{(0)}) + O(d^2)$, $\Delta_C = \text{rem}(\bar{A} - C^{(0)}, C^{(0)}) + O(d^2)$. Assume that we have determined $H(x)$ and $C(x)$ to order d^k as $H(x) = H^{(k)} + O(d^{k+1})$ and $C(x) = C^{(k)} + O(d^{k+1})$. We shall determine $H^{(k+1)}$ and $C^{(k+1)}$ so as to satisfy $\bar{A}(x) = H^{(k+1)}C^{(k+1)} + O(d^{k+2})$. Putting $H^{(k+1)} = H^{(k)} + \Delta_H$ and $C^{(k+1)} = C^{(k)} + \Delta_C$, with $\deg(\Delta_H) < n-m$ and $\deg(\Delta_C) < m$, we have $\bar{A} - H^{(k)}C^{(k)} = \Delta_H C^{(k)} + \Delta_C + O(d^{k+2})$ (note that $\deg(\bar{A} - H^{(k)}C^{(k)}) \leq n-1$). Hence, we can determine $H^{(k+1)}$ and $C^{(k+1)}$ by the following formulas.

$$\begin{cases} H^{(k+1)} &= H^{(k)} + \text{quo}(\bar{A} - H^{(k)}C^{(k)}, C^{(0)}), \\ C^{(k+1)} &= C^{(k)} + \text{rem}(\bar{A} - H^{(k)}C^{(k)}, C^{(0)}). \end{cases} \quad (3.13)$$

Remark 4 It should be emphasized that, since $\|C^{(0)}\| = 1 = \text{lc}(C^{(0)})$, the algorithm is quite stable; if d is smaller then the algorithm is more stable and it converges faster. Note that, in the step of computing $H^{(k+1)}$ and $C^{(k+1)}$, we have only to compute $\bar{A} - H^{(k)}C^{(k)}$ to order d^{k+1} ; we may handle only $x^{m+k}, x^{m+k-1}, \dots, x^0$ -terms of $\bar{A} - H^{(k)}C^{(k)}$. Hence, the above algorithm is pretty efficient. The above algorithm is of linear convergence. If we determine Δ_H and Δ_C to satisfy $\bar{A} - H^{(k)}C^{(k)} = \Delta_H C^{(k)} + \Delta_C H^{(k)} + O(d^{2k+1})$, then we get an algorithm of quadratic convergence. \square

Remark 5 If a coefficient of a polynomial containing m multiple roots is perturbed by a small relative magnitude ε , then the m multiple roots are split into m close roots which are distributed within a circle of radius $\leq O(\varepsilon^{1/m})$. Therefore, in order to compute the roots of $C(x)$ to accuracy 2^{-p} , with p a positive integer, we must compute $C(x)$ to accuracy 2^{-mp} at least (if a close-root cluster of $C(x)$ contains smaller close-root clusters, we must compute $C(x)$ much more accurately). This means that we must compute $A'(x) = A(x + \alpha'_c)$ to accuracy 2^{-mp} at least, which is quite time-consuming. However, since the x^k -term of $\bar{A}(x)$, $k > m$, is of magnitude $O(d^{n-m-k})$, we have only to compute its coefficient to accuracy $O(2^{-mp-g}/d^{n-m-k})$, with g the number of guard bits. \square

Example 2 We consider the polynomial in Example 1.

We already know that $\alpha'_c = 0.31139\dots$. Shifting the origin to α'_c , we obtain

the polynomial $A'(x)$ given in Example 1. From the coefficients a'_5, a'_4, \dots, a'_0 , we obtain $e = 0.042814 \dots$, which gives us $\bar{A}(x)$ as follows.

$$\begin{cases} \bar{A}(x) &= 1 \cdot C^{(0)} + (-0.0020291 \dots x^2 - 0.029374x) \cdot x^5, \\ C^{(0)} &= x^5 - 0.093589 \dots x^4 + \dots + x^2 + \dots - 0.011226 \dots. \end{cases}$$

Performing the above factor-separation algorithm, we find that the norm of difference $\Delta^{(k)} \stackrel{\text{def}}{=} \bar{A} - H^{(k)}C^{(k)}$ decreases as follows.

$$\begin{aligned} \|\Delta^{(0)}\| &\approx 2.94 \times 10^{-2} &\Rightarrow &\|\Delta^{(1)}\| \approx 8.00 \times 10^{-4} &\Rightarrow &\|\Delta^{(2)}\| \approx 4.04 \times 10^{-5} \\ \cdot &\cdot &\cdot &\cdot &\cdot &\cdot \\ &&&\Rightarrow &\|\Delta^{(8)}\| \approx 4.00 \times 10^{-13} &\Rightarrow &\|\Delta^{(9)}\| \approx 1.60 \times 10^{-14}. \end{aligned}$$

We note that, since the cluster size is pretty large ($\delta \sim 10^{-1}$) hence the separation of the cluster is not easy for many separation algorithms, our algorithm works quite well and stably. \square

Hribernic and Stetter [HS97] constructed an algorithm for separating a close-root cluster, and the algorithm has some similarity to ours. Their algorithm is, however, complicated compared with our algorithm, because they did not utilize the fact that the coefficients $|a'_{m-1}|, |a'_{m-2}|, \dots, |a'_0|$ of $A'(x + \alpha'_c)$ decrease steadily as expressed in (3.9).

4. On the Minimum Root Separation in a Cluster

Let $C(x)$ be a factor of $\bar{A}(x)$, corresponding to the smallest close root cluster of size $O(\delta_\tau)$, with $\deg(C) = m \geq 3$. The factor $C(x)$ is obtained by a repetition of cluster separations and scale transformations, and we can obtain $\text{sep}(A)$ if $\text{sep}(C)$ is determined. After regularizing $C(x)$ as in 3.4, $C(x)$ will contain no close-root cluster which can be separated by Theorem 1. In order to derive formulas on $\text{sep}(C)$, however, we consider the case that $C(x)$ has only two close roots. We also assume that we have computed α'_c , an approximate cluster center, by the normalized PRS of $C(x)$ and dC/dx , and the origin has been shifted to α'_c . We denote the roots of $C(x)$ by $\gamma_1, \dots, \gamma_m$, among which γ_1 and γ_2 are the close roots around the origin.

4.1. A lower bound for $|\gamma_1 - \gamma_2|$

Under some conditions, we can bound $|\gamma_1 - \gamma_2|$ by applying Theorem 1 to $C(x)$ (we may use Theorem 4 but the statement becomes complicated). We regularize $C(x)$ and define e as follows.

$$\begin{cases} C(x) &= c_m x^m + \dots + c_3 x^3 + x^2 + c_1 x + c_0, \\ \max\{|c_m|, \dots, |c_3|\} &= 1, \quad e \stackrel{\text{def}}{=} \max\{|c_1|, |c_0|^{1/2}\}. \end{cases} \quad (4.1)$$

THEOREM 5. *Let \bar{R}_{in} be the same as that in Theorem 1, with \bar{e} replaced by e . If $e < 1/9$ and $|c_1^2 - 4c_0|/4|c_0| > \bar{R}_{\text{in}}/(1 - \bar{R}_{\text{in}})$ then the following inequality holds.*

$$|\gamma_1 - \gamma_2| > \frac{\sqrt{|c_1^2 - 4c_0| - 4|c_0| \bar{R}_{\text{in}}/(1 - \bar{R}_{\text{in}})} \times (1 - 2\bar{R}_{\text{in}})(1 - \bar{R}_{\text{in}})}{1 + (|c_1|/2)(1 - \bar{R}_{\text{in}})^2/(1 - 2\bar{R}_{\text{in}})^3}. \quad (4.2)$$

Proof Put $C(x) = L(x)x^2 + c_1x + c_0$, with $L(x) = c_mx^{m-2} + \dots + c_3x + 1$, and let $\gamma \in \{\gamma_1, \gamma_2\}$. We regard γ as a root of $L(\gamma)x^2 + c_1x + c_0$, then we obtain

$$(\gamma_1 - \gamma_2) - \frac{c_1}{2} \cdot \frac{L(\gamma_1) - L(\gamma_2)}{L(\gamma_1)L(\gamma_2)} = \frac{\sqrt{c_1^2 - 4c_0L(\gamma_1)}}{2L(\gamma_1)} + \frac{\sqrt{c_1^2 - 4c_0L(\gamma_2)}}{2L(\gamma_2)}.$$

Since $L(\gamma) = 1 + c_3\gamma + \dots + c_m\gamma^{m-2}$ and $|\gamma| < \bar{R}_{\text{in}} < 1/3$, we can bound $|L(\gamma)|$ as

$$1 - \bar{R}_{\text{in}}/(1 - \bar{R}_{\text{in}}) < |L(\gamma)| < 1 + \bar{R}_{\text{in}}/(1 - \bar{R}_{\text{in}}). \quad (4.3)$$

We bound $|L(\gamma_1) - L(\gamma_2)|$ as $|L(\gamma_1) - L(\gamma_2)| = |\gamma_1 - \gamma_2| \cdot |c_3 + c_4(\gamma_1 + \gamma_2) + c_5(\gamma_1^2 + \gamma_1\gamma_2 + \gamma_2^2) + \dots| < |\gamma_1 - \gamma_2| \cdot (1 + 2|\gamma| + 4|\gamma|^2 + \dots) = |\gamma_1 - \gamma_2|/(1 - 2|\gamma|) < |\gamma_1 - \gamma_2|/(1 - 2\bar{R}_{\text{in}})$.

Putting $R(\gamma) = \sqrt{c_1^2 - 4c_0L(\gamma)}/2L(\gamma)$, we search for a lower bound of $|R(\gamma_1) + R(\gamma_2)|$. Although the roots γ_1 and γ_2 are mutually related in that they are two different roots of $C(x)$, we neglect this fact and change $L(\gamma_1)$ and $L(\gamma_2)$ arbitrarily under the restriction (4.3). Then, the numerator of $|R(\gamma)|$ is bounded as

$$\sqrt{|c_1^2 - 4c_0L(\gamma)|} > \sqrt{|c_1^2 - 4c_0| - 4|c_0| \bar{R}_{\text{in}}/(1 - \bar{R}_{\text{in}})}.$$

Noting that $L(\gamma)$ is a complex number, we bound $|1/L(\gamma_1) + 1/L(\gamma_2)|$ as

$$\left| \frac{1}{L(\gamma_1)} + \frac{1}{L(\gamma_2)} \right| = \frac{|L(\gamma_1) + L(\gamma_2)|}{|L(\gamma_1)L(\gamma_2)|} > 2(1 - 2\bar{R}_{\text{in}})(1 - \bar{R}_{\text{in}}).$$

Summarizing the above bounds, we obtain the theorem. \square

4.2. Basic lemmas

The formula in Theorem 5 is rather complicated, so we search for another formula. In this and the next subsections, we regularize $C(x)$ as $A(x)$ in (3.1) and define d as follows.

$$\begin{cases} C(x) = x^m + c_{m-1}x^{m-1} + \dots + c_2x^2 + c_1x + c_0, \\ \max\{|c_{m-1}|, \dots, |c_2|\} = 1 \gg |c_1|, |c_0|, \\ 1/d = \max\{|c_3/c_2|, |c_4/c_2|^{1/2}, \dots, |1/c_2|^{1/(m-2)}\}. \end{cases} \quad (4.4)$$

Put $\sigma = (\gamma_1 + \gamma_2)/2$ and $\hat{\gamma} = (\gamma_1 - \gamma_2)/2$, and define $H(x)$ and η as follows.

$$\begin{cases} C(x) = H(x) \cdot (x - \sigma - \hat{\gamma})(x - \sigma + \hat{\gamma}), \\ H(x) = x^{m-2} + h_{m-3}x^{m-3} + \dots + h_1x + h_0, \\ 1/\eta = \max\{|h_1/h_0|, |h_2/h_0|^{1/2}, \dots, |1/h_0|^{1/(m-2)}\}. \end{cases} \quad (4.5)$$

Expressing c_0, c_1, c_2, \dots by h_0, h_1, h_2, \dots , we obtain $c_0 = (\sigma^2 - \hat{\gamma}^2)h_0$, $c_1 = (\sigma^2 - \hat{\gamma}^2)h_1 - 2\sigma h_0$, $c_j = (\sigma^2 - \hat{\gamma}^2)h_j - 2\sigma h_{j-1} + h_{j-2}$ ($j \geq 2$). By these, we obtain

$$\frac{c_1}{c_0} = -\frac{2\sigma}{\sigma^2 - \hat{\gamma}^2} + \frac{h_1}{h_0}, \quad \frac{c_2}{c_0} = \frac{1}{\sigma^2 - \hat{\gamma}^2} - \frac{2\sigma}{\sigma^2 - \hat{\gamma}^2} \frac{h_1}{h_0} + \frac{h_2}{h_0}.$$

Solving σ and $\hat{\gamma}$ from these equations, we obtain

$$2\sigma = \gamma_1 + \gamma_2 = -\frac{C_1}{C_2}, \quad 2\hat{\gamma} = \gamma_1 - \gamma_2 = \frac{\sqrt{C_1^2 - 4C_2}}{C_2}, \quad (4.6)$$

where

$$C_1 = \frac{c_1}{c_0} - \frac{h_1}{h_0}, \quad C_2 = \frac{c_2}{c_0} - \frac{c_1}{c_0} \frac{h_1}{h_0} + \frac{h_1^2}{h_0^2} - \frac{h_2}{h_0}. \quad (4.7)$$

The roots of $C_2 x^2 + C_1 x + 1$ are γ_1 and γ_2 . In fact, equalities in (4.6) give us

$$C_2 = \frac{1}{\sigma^2 - \hat{\gamma}^2} = \frac{1}{\gamma_1 \gamma_2}, \quad C_1 = \frac{-2\sigma}{\sigma^2 - \hat{\gamma}^2} = \frac{-\gamma_1 - \gamma_2}{\gamma_1 \gamma_2}. \quad (4.8)$$

The above relation on c_j and h_j ($j \geq 2$) also gives us

$$\frac{c_j}{c_2} = \frac{(h_{j-2}/h_0) - 2\sigma(h_{j-1}/h_0) + (\sigma^2 - \hat{\gamma}^2)(h_j/h_0)}{1 - 2\sigma(h_1/h_0) + (\sigma^2 - \hat{\gamma}^2)(h_2/h_0)} \quad (j \geq 3). \quad (4.9)$$

LEMMA 2. *The following inequalities hold for $|C_1|$, $|C_2|$ and $|C_1^2 - 4C_2|/|C_2|^2$.*

$$\left\{ \begin{array}{l} \frac{|c_1|}{|c_0|} - \frac{1}{\eta} \leq |C_1| \leq \frac{|c_1|}{|c_0|} + \frac{1}{\eta}, \\ \frac{|c_2|}{|c_0|} - \frac{1}{\eta} \frac{|c_1|}{|c_0|} - \frac{2}{\eta^2} \leq |C_2| \leq \frac{|c_2|}{|c_0|} + \frac{1}{\eta} \frac{|c_1|}{|c_0|} + \frac{2}{\eta^2}, \\ \frac{|c_1^2 - 4c_2c_0| - 2|c_1c_0|/\eta - 7|c_0|^2/\eta^2}{(|c_2| + |c_1|/\eta + 2|c_0|/\eta^2)^2} \leq |C_1^2 - 4C_2|/|C_2|^2. \end{array} \right. \quad (4.10)$$

Proof Definition of η gives $|h_j/h_0| \leq 1/\eta^j$ for $j = 1, 2, \dots$. From these inequalities and the equality $C_1^2 - 4C_2 = (c_1/c_0)^2 - 4(c_2/c_0) + 2(c_1/c_0)(h_1/h_0) - 3(h_1/h_0)^2 + 4(h_2/h_0)$, we obtain the above inequalities easily. \square

Assuming that $|\sigma|$ and $|\hat{\gamma}|$ are small enough, let us bound η/d .

LEMMA 3. *So long as $|\sigma|/\eta \ll 1$ and $|\sigma^2 - \hat{\gamma}^2|/\eta^2 \ll 1$, the following inequalities hold.*

$$\frac{1 - 2|\sigma|/\eta - |\sigma^2 - \hat{\gamma}^2|/\eta^2}{1 + 2|\sigma|/\eta + |\sigma^2 - \hat{\gamma}^2|/\eta^2} \leq \frac{\eta}{d} \leq \frac{1 + 2|\sigma|/\eta + |\sigma^2 - \hat{\gamma}^2|/\eta^2}{1 - 2|\sigma|/\eta - |\sigma^2 - \hat{\gamma}^2|/\eta^2}. \quad (4.11)$$

Proof We can bound the r.h.s. expression in (4.9), let it be R_j , by inequalities $|h_{j'}/h_0| \leq 1/\eta^{j'}$ ($j' = j, j-1, j-2$). Then, the above bound is obtained by bounding $|c_j/c_0| = |R_j|^{1/j}$ by inequality $[(1+r)/(1-r)]^{(1/j)} \leq (1+r)/(1-r)$ which is valid for any integer $j > 0$ and any real number r such that $0 < r < 1$.

We note that there exists a positive integer j'' such that $1/\eta = |h_{j''}/h_0|^{1/j''}$. For $j = j'' + 2$, we obtain $|(h_{j''}/h_0) - 2\sigma(h_{j''+1}/h_0) + (\sigma^2 - \hat{\gamma}^2)(h_{j''+2}/h_0)| \geq$

$(1/\eta^{j''}) \cdot (1 - 2|\sigma|/\eta - |\sigma^2 - \hat{\gamma}^2|/\eta^2)$. Bounding $|c_j/c_2|$ in (4.9) by this inequality, and using $[(1-r)/(1+r)]^{(1/j)} \geq (1-r)/(1+r)$ which is valid for r such that $0 < r < 1$, we obtain the lower bound. \square

We investigate the above inequalities by transforming $C(x)$ as

$$C(x) \mapsto C(\eta x)/h_0\eta^2 \stackrel{\text{def}}{=} C'(x).$$

Then, $H(x)$ is transformed as follows.

$$\begin{cases} H(x) \mapsto H(\eta x)/h_0 \stackrel{\text{def}}{=} H'(x), \\ H'(x) = h'_{m-2}x^{m-2} + \cdots + h'_1x + 1, \\ \max\{|h'_{m-2}|, \dots, |h'_1|\} = 1. \end{cases}$$

Applying formula (2.2) to $H'(x)$, we see that

$$|\gamma_j/\eta| \geq 1/2 \quad \text{or} \quad |\gamma_j| \geq \eta/2 \quad (j \geq 3). \quad (4.12)$$

Therefore, η is a number showing how the roots $\gamma_3, \dots, \gamma_m$ are distributed. In fact, expressing the quantities in (4.10) by $c'_0 = c_0/\eta^2$, $c'_1 = c_1/\eta$, $c'_2 = c_2$, $C'_1 = C_1\eta$ and $C'_2 = C_2\eta^2$, we can remove η from inequalities in (4.10). Let the roots of $C'(x)$ be $\gamma'_1, \dots, \gamma'_m$ ($\gamma'_i = \gamma_i/\eta$; $i = 1, \dots, m$). With γ'_1, γ'_2 , we can rewrite (4.11) as follows.

$$\frac{1 - |\gamma'_1 + \gamma'_2| - |\gamma'_1\gamma'_2|}{1 + |\gamma'_1 + \gamma'_2| + |\gamma'_1\gamma'_2|} \leq \frac{\eta}{d} \leq \frac{1 + |\gamma'_1 + \gamma'_2| + |\gamma'_1\gamma'_2|}{1 - |\gamma'_1 + \gamma'_2| - |\gamma'_1\gamma'_2|}. \quad (4.13)$$

So long as γ'_1 and γ'_2 are small enough, the above inequalities are fairly accurate.

4.3. A formula for the minimum root separation

A fairly accurate upper bound of α'_c is currently not obtained, although we have an order estimation by Proposition 3. Therefore, we set the following condition on c_2, c_1, c_0 .

$$|c_1/c_2|^2 < |c_0/c_2| \iff |c_1|^2 < |c_2c_0|. \quad (4.14)$$

Since the origin has been moved to α'_c , this condition will be well satisfied. If the condition is not satisfied, we shift the origin slightly to satisfy the condition. With the above condition, we define e as follows.

$$e \stackrel{\text{def}}{=} \max\{|c_1/c_2|, |c_0/c_2|^{1/2}\} = |c_0/c_2|^{1/2}. \quad (4.15)$$

Note that, if we transform $C(x)$ to a regularized form by $C(x) \mapsto \bar{C}(x) = C(dx)/c_2d^2 = \bar{c}_m x^m + \cdots + x^2 + \bar{c}_1 x + \bar{c}_0$ and define \bar{e} as $\bar{e} = \min\{|\bar{c}_1|, |\bar{c}_0|^{1/2}\}$, then we have $\bar{e} = e/d$.

THEOREM 6. *Let \bar{R}_{in} be the same as that in Theorem 1, with \bar{e} replaced by e/d . Let \bar{R}_{in} be such that the polynomial $y^3 - (1 - 2\bar{R}_{\text{in}})y^2 + \bar{R}_{\text{in}}(2 + \bar{R}_{\text{in}})y + \bar{R}_{\text{in}}^2$ has three real roots, and the largest root (a little smaller than 1) be η_{min}/d (η_{min} is a lower bound of η). If $e/d < 0.03$ as well as $|c_1|^2 < |c_2c_0|$ then the following inequality holds.*

$$|\gamma_1 - \gamma_2|^2 > \frac{|c_1^2 - 4c_2c_0| - 2|c_1c_0|/\eta_{\text{min}} - 7|c_0|^2/\eta_{\text{min}}^2}{(|c_2| + |c_1|/\eta_{\text{min}} + 2|c_0|/\eta_{\text{min}}^2)^2}. \quad (4.16)$$

Proof We note that if $e/d < 0.03$ then $\bar{R}_{\text{in}} < 0.0621 \dots$ and the above cubic polynomial has three real roots. The regularization of $C(x)$ in (4.4) tells us that $|\gamma_1|, |\gamma_2| < \bar{R}_{\text{in}}d$, hence $|\sigma|/\eta < \bar{R}_{\text{in}}(d/\eta)$ and $|\sigma^2 - \hat{\gamma}^2|/\eta^2 < \bar{R}_{\text{in}}^2(d/\eta)^2$. Then, by putting $y = \eta/d$, (4.11) becomes

$$\frac{y^2 - 2\bar{R}_{\text{in}}y - \bar{R}_{\text{in}}^2}{y^2 + 2\bar{R}_{\text{in}}y + \bar{R}_{\text{in}}^2} < y < \frac{y^2 + 2\bar{R}_{\text{in}}y + \bar{R}_{\text{in}}^2}{y^2 - 2\bar{R}_{\text{in}}y - \bar{R}_{\text{in}}^2}.$$

The l.h.s. of this inequality gives us a lower bound of η , and we obtain η_{min} as in the theorem. Replacing η by η_{min} in the bottom inequality in (4.10), we obtain (4.16). \square

COROLLARY 5. *If $e/d \geq 0.03$ then we have the following inequality.*

$$|\gamma_1 - \gamma_2| \geq 0.03d \cdot \frac{\sqrt{3 - 2\xi - 7\xi^2}}{1 + \xi + 2\xi^2}, \quad \text{where } \xi = 0.0442 \dots \quad (4.17)$$

Proof As a critical case that the close-root cluster of γ_1 and γ_2 are separated from the other roots and inequality (4.11) holds narrowly, we consider the case of $\bar{e} = e/d = 0.03$ (this number is pretty small compared with $1/9$). In this case, we have $|c_1/c_2| \leq 0.03d$, $|c_0/c_2| = (0.03d)^2$, $\bar{R}_{\text{in}} = 0.0621 \dots$, and $\eta_{\text{min}}/d = 0.678 \dots$. ($\xi = \bar{e}d/\eta_{\text{min}} = 0.0442 \dots$). We bound $|c_1^2 - 4c_2c_0|$ as $|c_1^2 - 4c_2c_0| \geq |4c_2c_0| - |c_1|^2$, then the r.h.s. of (4.16) is monotone increasing for $\bar{e} \in [0, 1]$. Hence, substituting the actual values to $|c_1/c_2|$ etc. in the r.h.s. of (4.16), we obtain (4.17). \square

5. Discussions

Our study in this paper is restricted in that the close roots are assumed to form well-separated clusters and that only polynomials over \mathbf{C} are treated. Developing an algebraic algorithm for separating close roots distributed arbitrarily is a challenging theme. A more challenging theme is to find a reasonable lower bound for the minimum root separation for polynomials over \mathbf{Z} .

The separation algorithm presented in **3** will be very useful practically. The underlying idea is so simple and effective that it will be applied to various problems. In fact, collaborating with Terui, one of the present authors (T.S.) developed recently a numerical algorithm for computing the close roots in a cluster simultaneously and efficiently.

The formula in the corollary of Theorem 6 is practically not bad as the lower bound for the minimum root separation. However, our formulas are not expressed by the coefficients of the original polynomial $A(x)$ but undergone a repetition of separation of close-root clusters, and they are not elaborated yet. Furthermore, our theory is not complete in that we set the condition (4.14). We should develop a theory without such a condition.

References

- [CH74] G.E. Collins and E. Horowitz: The minimum root separation of a polynomial. *Math. Comp.* **28** (1974), 589–597.
- [Col01] G.E. Collins: Polynomial minimum root separation. *J. Symb. Comp.* **32** (2001), 467–473.
- [CWZ02] R.M. Corless, S.M. Watt and L. Zhi: QR factoring to compute the GCD of univariate approximate polynomial. Preprint of Univ. Western Ontario, Canada, 2002.
- [HS97] V. Hribernik and H. J. Stetter: Detection and validation of clusters of zeros of polynomials. *J. Symb. Comp.* **24** (1997), 667–681.
- [IS04] D. Inaba and T. Sasaki: Certification of analytic continuation of algebraic functions. *Proc. CASC2004*, (Eds. V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov), 249–260. July 2004.
- [Mig92] M. Mignotte: *Mathematics for Computer Algebra*. Springer-Verlag, New York, 1992, Ch. 4.
- [OST97] H. Ohsako, H. Sugiura and T. Torii: A stable extended algorithm for generating polynomial remainder sequence (in Japanese). *Trans. of JSIAM (Japan Society for Indus. Appl. Math.)* **7** (1997), 227–255.
- [Pan95] V.Y. Pan: Optimal (up to polylog factors) sequential and parallel algorithms for approximating complex polynomial zeros. *Proc. 27th Ann. ACM Symp. on Theory of Computing*, 741–750. ACM Press, New York, 1995.
- [Pan96] V.Y. Pan: Optimal and nearly optimal algorithms for approximating complex zeros. *Computers & Math. (with Applications)*, **31** (1996), 97–138.
- [Pan01] V.Y. Pan: Univariate polynomials: nearly optimal algorithms for factorization and rootfinding. *Proc. ISSAC 2001*, (Ed. J.R. Sendra), 253–267. ACM Press, 2001.
- [Sas03] T. Sasaki: The subresultant and clusters of close roots. *Proc. ISSAC 2003*, (Ed. B. Mourrain), 232–239. ACM Press, 2003.
- [SN89] T. Sasaki and M.-T. Noda: Approximate square-free decomposition and root-finding of ill-conditioned algebraic equations. *J. Inf. Process.* **12** (1989), 159–168.
- [SS89] T. Sasaki and M. Sasaki: Analysis of accuracy decreasing in polynomial remainder sequence with floating-point number coefficients. *J. Inf. Process.*, **12** (1989), 159–168.
- [SS97] T. Sasaki and M. Sasaki: Polynomial remainder sequence and approximate GCD. *SIGSAM Bulletin* **31** (1997), 4–10.
- [SST92] T. Sakurai, H. Sugiura and T. Torii: Numerical factorization of polynomial by rational Hermite interpolation. *Numerical Algorithms* **3** (1992), 411–418.
- [ST02] T. Sasaki and A. Terui: A formula for separating small roots of a polynomial. *ACM SIGSAM Bulletin* **36** (2002), 19–29.
- [TS00] A. Terui and T. Sasaki: “Approximate zero-points” of real univariate polynomial with large error terms. *IPSJ Journal (Information Processing Society of Japan)* **41** (2000), 974–989.
- [WH90] X.H. Wang and D.F. Han: On dominating sequence method in the point estimate and Smale theorem. *Sci. China (Series A)* **33** (1990), 135–144.
- [Yak00] J.C. Yakoubsohn: Finding a cluster of zeros of univariate polynomials. *J. Complexity* **16** (2000), 603–636.

[Zen03] Z. Zeng: A method computing multiple roots of inexact polynomials. Proc. ISSAC 2003, (Ed. B. Mourrain), 166–272. ACM Press, 2003.

Tateaki Sasaki

Institute of Mathematics, University of Tsukuba, Tsukuba-shi, Ibaraki 305-8571, Japan
e-mail: `sasaki@math.tsukuba.ac.jp`

Fujio Kako

Dept. Information and Computer Sciences, Nara Women's University, Nara-shi, Nara 630-8506, Japan
e-mail: `kako@ics.nara-wu.ac.jp`