On Approximate GCDs of Univariate Polynomials

N. K. KARMAKAR†§¶ AND Y. N. LAKSHMAN‡∥∗

†School of Mathematics, Institute for Advanced Study, Princeton, NJ, U.S.A.
‡Department of Mathematics and Computer Science, Drexel University, Philadelphia, PA 19104 U.S.A.

In this paper, we consider computations involving polynomials with inexact coefficients, i.e. with bounded coefficient errors. The presence of input errors changes the nature of questions traditionally asked in computer algebra. For instance, given two polynomials, instead of trying to compute their greatest common divisor, one might now try to compute a pair of polynomials with a non-trivial common divisor close to the input polynomials. We consider the problem of finding approximate common divisors in the context of inexactly specified polynomials. We develop efficient algorithms for the so-called nearest common divisor problem and several of its variants.

1. Introduction

The problem of computing the greatest common divisor (GCD) of two polynomials $f, g \in \mathcal{A}[z]$, $\mathcal{A}$ being a unique factorization domain, is well understood and there are a number of efficient algorithms for computing polynomial GCDs beginning with the the work of Collins and Brown (Collins, 1967; Brown and Traub, 1971). These algorithms assume that the input is error-free and perform exact computations producing provably correct results which is the hallmark of computer algebra.

Recently, there has been much interest in computing with polynomials with rational/real/complex coefficients in the presence of bounded coefficient errors. The presence of errors in the input changes the nature of questions traditionally asked in computer algebra. For instance, a question such as “Given two polynomials with rational number coefficients, do they have a non-trivial GCD?” changes to, perhaps, “Are the given polynomials near a pair of polynomials that have a non-trivial GCD?”; the question “Does a given polynomial with rational number coefficients have a root of multiplicity $r$?” may change to “Is the given polynomial near a polynomial that has a root of multiplicity $r$?” with respect to some appropriate measure of nearness. Such questions are not handled well by existing symbolic algorithms or purely numerical algorithms and, in our view, the following issues need addressing:

†Supported by the Alfred P. Sloane Foundation, Grant No. 96-6-2.
§E-mail: nkarmarkar@math.ias.edu
¶Supported in part by NSF Grants CCR-9527130 and CCR-9712219
∥E-mail: lakshman@math.drexel.edu
∗E-mail: lakshman@math.drexel.edu

0747–7171/98/120653 + 14 $30.00/0 © 1998 Academic Press
characterization of the solutions of a symbolic/numerical problem in the presence of small input errors;

(2) design of efficient “hybrid” algorithms for solving symbolic/numerical problems that work in limited (or adaptive) precision and understanding the factors that affect the stability of these algorithms;

In this paper, we investigate the so-called approximate GCD problem and several of its variants in the above framework. We use the following notation:

(1) \( \mathcal{F}[x,y] \) denotes the polynomial ring in \( x, y \) over the field \( \mathcal{F} \).
(2) \( \mathcal{F}(x,y) \) denotes the field of rational functions in \( x, y \) over \( \mathcal{F} \).
(3) \( A \) denotes a unique factorization domain.
(4) \( C \) denotes the field of complex numbers.
(5) \( R \) denotes the field of real numbers.
(6) \( Q \) denotes the field of rational numbers.
(7) \( \alpha^* \) denotes the complex conjugate of \( \alpha \).
(8) for a polynomial \( f = \sum_{n=0}^{n} f_i z^i \in \mathcal{C}[z] \), and \( \alpha \in \mathcal{C} \), \( f^*(\alpha) = \sum_{n=0}^{n} f_i \alpha^i \).
(9) for a polynomial \( f = \sum_{n=0}^{n} f_i z^i \in \mathcal{C}[z] \), \( \| f \| \) denotes its 2-norm \( (\sum_{n=0}^{n} f_i^2)^{1/2} \).

We start with the following problems and then treat several variants:

1. THE NEAREST GCD PROBLEM. Given two monic polynomials \( f, g \in \mathcal{C}[x] \) with \( \deg(f) = m \), \( \deg(g) = n \), find monic polynomials \( \hat{f}, \hat{g} \in \mathcal{C}[x] \) with \( \deg(\hat{f}) = m \), \( \deg(\hat{g}) = n \) such that \( \hat{f} \) and \( \hat{g} \) have a non-trivial GCD and \( N = \| f - \hat{f} \|^2 + \| g - \hat{g} \|^2 \) is minimized.

We describe the first polynomial time algorithm for the nearest GCD problem. The running time of our algorithm is polynomial in the degrees \( m, n \) and a bound on the bit sizes of the coefficients of \( f, g \).

2. THE HIGHEST DEGREE APPROXIMATE COMMON DIVISOR PROBLEM. Given two monic polynomials \( f, g \in \mathcal{C}[x] \) with \( \deg(f) = m \), \( \deg(g) = n \), and error bounds \( 0 < r_1, r_2 \in R \), let \( \mathcal{P} \) denote the set of all ordered pairs \((\Phi, \Gamma)\) where \( \Phi, \Gamma \in \mathcal{C}[x] \) are monic with \( \deg(\Phi) = m \), \( \deg(\Gamma) = n \) and \( \| f - \Phi \|^2 \leq r_1 \) and \( \| g - \Gamma \|^2 \leq r_2 \). Let \( \mathcal{P}_d \subseteq \mathcal{P} \) denote the set of pairs \((\Phi, \Gamma)\) such that the degree \( d \) of the GCD of \( \Phi, \Gamma \) is maximized over all pairs in \( \mathcal{P} \). The highest degree approximate common divisor problem asks for a pair \((\hat{f}, \hat{g})\) in \( \mathcal{P}_d \) such that \( \| f - \hat{f} \|^2 + \| g - \hat{g} \|^2 \) is minimized over all pairs in \( \mathcal{P}_d \).

We formulate the highest degree approximate common divisor problem as an explicit multivariate minimization problem.

Various versions of approximate common divisors have been considered by several authors in the past including Hough (1977), Schönhage (1985), Noda and Sasaki (1991). More recently, Hribernig and Stetter (1997), Corless et al. (1995), Emiris et al. (1996), and Pan (1996) have addressed the same problem.

Schönhage (1985) assumes that the input is arbitrarily precise, i.e. that one can get as many digits of the input coefficients as needed on demand. Our model is different in that we assume that the input coefficients are given to a fixed precision to within a known error bound.

Noda and Sasaki (1991) describe a version of Euclid’s algorithm with scaling that produces a common divisor of polynomials that are close to the input polynomials. Hribernig and Stetter (1997) also use polynomial remainder sequences and provide a lower bound.
on the degree of the highest degree approximate common divisor. The paper by Corless et al. (1995) applies the singular value decomposition technique to the Sylvester resultant of \( f, g \) and extends the technique to finding approximate common zeros of systems of polynomial equations. Pan describes a geometric algorithm based on explicit computation of the roots of the input polynomials and finding pairwise close roots. While these algorithms produce, under various situations, polynomials close to the given polynomials that have a non-trivial GCD, they do not offer guarantees on how far the results are from the nearest GCD or the highest degree approximate common divisor nor can they answer qualitative questions such as “Are the given polynomials within a distance \( \epsilon \) of a pair of polynomials that have a non-trivial GCD?” with certainty in all cases. The paper by Emiris et al. (1997) (see also the paper by Emiris et al. (1996)) describes a gap theorem which they use to modify the SVD algorithm to produce a highest degree approximate common divisor in certain cases.

The distinguishing feature of our results is that we are able to precisely characterize the least perturbations with the desired properties for the nearest and highest degree approximate common divisor problem and we provide efficient algorithms to compute these perturbations. The approach taken by Hough (1977) in his thesis is the one closest to our approach conceptually but he only treats the nearest singular polynomial problem. Our formulation is different from Hough’s and avoids some of the technical difficulties encountered in his approach. We give a more complete development of the parametric minimization approach including a polynomial time algorithm that computes a pair of polynomials having a non-trivial GCD that is provably nearest to the given pair of polynomials.

The rest of the paper is organized as follows. In the next section, we describe our approach to the nearest GCD problem, prove bounds on the magnitude of the smallest GCD-producing perturbations and describe our algorithm for computing such perturbations. In Section 3, we describe several variants of the nearest GCD problem including perturbations with respect to an arbitrary basis, perturbations with respect to a weighted 2-norm and, sparse perturbations, meaning perturbations affecting selected coefficients. Section 4 deals with the highest degree approximate common divisor problem. We conclude with some interesting open problems. Some of the results in this paper appeared in a preliminary form in the paper (Karmarkar and Lakshman, 1996).

2. Computing GCD-introducing Perturbations

For the sake of simplifying the exposition, we begin with two polynomials \( f, g \in \mathbb{C}[z] \), both of degree \( n \), and monic. We perturb them to monic polynomials \( \hat{f}, \hat{g} \) respectively. The perturbed polynomials have a common root \( \alpha \). We have

\[
\begin{align*}
  f(z) &= \sum_{i=0}^{n} f_i z^i, & g(z) &= \sum_{i=0}^{n} g_i z^i, & f_n = g_n = 1, \\
  \hat{f}(z) &= \sum_{i=0}^{n} \hat{f}_i z^i, & \hat{g}(z) &= \sum_{i=0}^{n} \hat{g}_i z^i, & \hat{f}_n = \hat{g}_n = 1, \\
  \hat{f}(\alpha) &= 0, & \hat{g}(\alpha) &= 0.
\end{align*}
\]

The coefficients are perturbed by \( \lambda_i = f_i - \hat{f}_i, \mu_i = g_i - \hat{g}_i, \) \( i = 0, \ldots, n - 1 \). Let \( \lambda_i = \zeta_i + i\eta_i, \mu_i = u_i + iv_i \), where \( \zeta, \eta, u, v \) are real variables. We try to minimize

\[
N = \sum_{i=0}^{n-1} \lambda_i \lambda_i^* + \sum_{i=0}^{n-1} \mu_i \mu_i^*.
\]
as a function of \( \alpha \) and subject to the constraints \( f(\alpha) = 0, g(\alpha) = 0 \). We make use of Lagrange multipliers. Consider

\[
\mathcal{N} + 2A \Re(\hat{f}(\alpha)) + 2B \Im(\hat{f}(\alpha)) + 2C \Re(\hat{g}(\alpha)) + 2D \Im(\hat{g}(\alpha)) = 0
\]

where \( A, B, C, D \) are undetermined multipliers and \( \Re(\hat{f}(\alpha)), \Im(\hat{f}(\alpha)) \) denote the real and imaginary parts of \( \hat{f}(\alpha) \) respectively, i.e.

\[
2 \Re(\hat{f}(\alpha)) = \hat{f}(\alpha) + \hat{f}^*(\alpha),
\]

\[
2 \Im(\hat{f}(\alpha)) = -i(\hat{f}(\alpha) - \hat{f}^*(\alpha))
\]

and so on. Differentiating (1) with respect to the real and imaginary parts of each \( \lambda_i, \mu_i \) and solving for the various multipliers, we find that at the minima of \( \mathcal{N} \),

\[
\lambda_i = -(A + iB)\alpha^{\ast i}, \quad \mu_i = -(C + iD)\alpha^{\ast i}.
\]

and

\[
A + iB = -\frac{f(\alpha)}{\sum_{k=0}^{n-1}(\alpha^{\ast} \alpha^k)}, \quad C + iD = -\frac{g(\alpha)}{\sum_{k=0}^{n-1}(\alpha^{\ast} \alpha^k)}.
\]

Substituting (3) in (2), we get the following expression for the minimum value of \( \mathcal{N} \) as a function of \( \alpha \) which we denote by \( \mathcal{N}_M \).

\[
\mathcal{N}_M = \frac{\sum_{k=0}^{n-1}|f(\alpha)f^*(\alpha)\alpha^i \alpha^{\ast i} + g(\alpha)g^*(\alpha)\alpha^i \alpha^{\ast i}|}{(\sum_{k=0}^{n-1}(\alpha^{\ast} \alpha^k))(\sum_{k=0}^{n-1}(\alpha^{\ast} \alpha^k)^2)}.
\]

As a function of the complex parameter \( \alpha \), \( \mathcal{N}_M \) is real valued, continuous and positive semi-definite. We wish to minimize \( \mathcal{N}_M \) over \( \alpha \). Let \( \alpha = u + iv \) where \( u, v \) are real variables. \( \mathcal{N}_M \in \mathcal{R}(u, v) \) and \( \mathcal{N}_M \) attains local minima at its stationary points given by \( \partial \mathcal{N}_M / \partial u = 0 \) and \( \partial \mathcal{N}_M / \partial v = 0 \). We are only interested in the real stationary points of \( \mathcal{N}_M \).

We now compute bounds on the absolute minimum of \( \mathcal{N}_M \). We also estimate the precision required in the calculation of the real intersection points of the partial derivatives of \( \mathcal{N}_M \) so as to be within a pre-specified \( \epsilon \) of the absolute minimum of \( \mathcal{N}_M \). The estimates we provide in the following discussion are quite rough. A more careful analysis taking into account the structure of \( \mathcal{N}_M \) might yield better bounds. Our main concern at this point is to show that we can get arbitrarily close to the absolute minimum of \( \mathcal{N}_M \) by expending polynomial amount of work (in the input size).

Let \( \mathcal{N}_M(u, v) \) attain its absolute minimum at \( (u, v) = (a, b) \). The perturbed polynomials (with minimum perturbation) \( \hat{f} \) and \( \hat{g} \) have the common root \( \alpha = a + ib \). If \( f, g \) have \( d \) distinct common roots, then \( \mathcal{N}_M = 0 \) has at least \( d \) real points. The converse is also true, i.e. if \( \mathcal{N}_M(a, b) = 0 \) for \( a, b \in \mathcal{R} \), then \( a + ib \) is an exact common root of \( f, g \). Therefore, the number of distinct real points on \( \mathcal{N}_M = 0 \) is a lower bound on the degree of the GCD of \( f, g \).

**Lemma 1.**

\[
\| \mathcal{N}_M(a, b) \| \leq 4 \max(\| f \|^2, \| g \|^2), \quad \| a + ib \| \leq 5 \max(\| f \|^2, \| g \|^2).
\]

**Proof.** Choose \( \hat{f} = g \) and \( \hat{g} = g \). Clearly \( \hat{f} \) and \( \hat{g} \) have a non-trivial GCD. In this case,
we have
\[
\| f - \tilde{f} \|^2 + \| g - \tilde{g} \|^2 - \| g - f \|^2 \geq N_M(a, b)
\]

and 4 max(\| f \|^2, \| g \|^2) \geq \| g - f \|^2. Suppose we denote the minimally perturbed polynomials by \( f, \tilde{g} a + ib \) is a root of \( \tilde{f} \) whose coefficients are bounded in magnitude by 4 max(\| f \|^2, \| g \|^2). The roots of \( \tilde{f} \) are bounded in magnitude by 1 + max{coefficients of \( \tilde{f} \}). Since max(\| f \|^2, \| g \|^2) \geq 1, \| a + ib \| \leq 5 \max(\| f \|^2, \| g \|^2). \)

Let \( B = 5 \max(\| f \|^2, \| g \|^2) \). The above lemma tells us that we need to be concerned only with the real stationary points of \( N_M \) in the box \(-B \leq u, v \leq B\). The next lemma provides a rough estimate of the precision required in the calculation of the real roots of the partial derivatives of \( N_M \).

**Lemma 2.** For a given \( \varepsilon > 0 \), if \( \delta_1, \delta_2 < \sqrt{\varepsilon/5(2n)}^{-9/2}c^{-n}B^{-2n+1/2} \) where \( c \) is a known positive constant, then, \( N_M(a + \delta_1, b + \delta_2) - N_M(a, b) \leq \varepsilon \).

**Proof.** Let \( \delta = \delta_1 + i\delta_2 \).

\[
N_M(a + \delta_1, b + \delta_2) - N_M(a, b) = f(a + \delta)f^*(a + \delta) + g(a + \delta)g^*(a + \delta) - f(a)f^*(a) - g(a)g^*(a)
\]

\[
= \sum_{k=0}^{n-1}((a + \delta)^k((a + \delta)^k)^* - \sum_{k=0}^{n-1}((a + \delta)^k((a + \delta)^k)^*)^* (\sum_{k=0}^{n-1}(a + \delta)^k((a + \delta)^k)^*))
\]

\[
\leq (f(a + \delta)f^*(a + \delta) + g(a + \delta)g^*(a)) \left( \sum_{k=0}^{n-1}(a + \delta)^k((a + \delta)^k)^* \right)
\]

The polynomial on the right-hand side of the next to last inequality is of total degree no more than 4n - 2 (in \( u, v, \delta_1, \delta_2 \)) with each coefficient bounded in absolute value by \( n^{9/2}2^{4n+9} \max(\| f \|^2, \| g \|^2) \). Each term in this polynomial is divisible by \( \delta_1 \delta_2 \) and some power product \( u^kv^l \) of total degree less than 4n. At the absolute minimum \( (a, b) \), \( u, v \) are bounded in absolute value by \( B \) and the last inequality follows. By choosing \( \delta_1, \delta_2 < \sqrt{\varepsilon/5(2n)}^{-9/2}c^{-n}B^{-2n+1/2} \),

(\text{where } c = 2^4), \text{we can ensure that}

\[
N_M(a + \delta_1, b + \delta_2) - N_M(a, b) \leq \varepsilon. \]

The lemma implies that if we compute \( a, b \) to \( o(\log \varepsilon + n \log B) \) bits precision, we are
guaranteed to be within $\epsilon$ of the absolute minimum of $N_M$. Notice that the number of bits of precision required depends linearly on the degrees of $f, g$ and logarithmically on the norms of $f, g$ which is usually the case with exact root finding problems in computer algebra. We now sketch our algorithm for the nearest GCD problem.

The Nearest GCD Algorithm

Input: Monic polynomials $f, g \in \mathbb{C}[x]$ of degree $n$, and an error bound $\epsilon$.
Output: Monic polynomials $f, g \in \mathbb{C}[x]$ and $\alpha = a' + ib' \in \mathbb{C}$ such that $\alpha$ is a common root of $f, g$ and $N_M(a', b') - (\text{absolute minimum of } N_M) \leq \epsilon^2$.

1. Determine
   \[ N_M = f(a)f'(a) + g(a)g'(a) \sum_{j=0}^{n-1} (\alpha^*)^j. \]
2. Find the real points of intersection of the curves given by setting the numerators of $\partial N_M/\partial u$ and $\partial N_M/\partial v$ to zero, inside the box $-B \leq u, v \leq B$. Compute the coordinates of each intersection point to a precision of $l$ bits (choose $l \geq \log_2(\sqrt{\epsilon/5}2n^{-9/2}c^{-1}B^{-(2n+1)/2}))$ with $c$ as in lemma 2). Let $(a', b')$ be the point of intersection where $N_M$ takes on the least value.
3. Compute the coefficient-wise perturbations using the formulas
   \[ \lambda_i = \frac{\alpha^* f(a)}{\sum_{k=0}^{n-1}(\alpha^*)^k}, \quad \mu_i = \frac{\alpha^* g(a)}{\sum_{k=0}^{n-1}(\alpha^*)^k}. \]
   at $\alpha = a' + ib'$ to obtain the perturbed polynomials that have a GCD of degree at least one.

The most time-consuming step in the above algorithm is step 2 in which we need to compute all the real intersection points of the numerators of $\partial N_M/\partial u$ and $\partial N_M/\partial v$ set to zero inside the box $-B \leq u, v \leq B$. These are polynomials in $u, v$ of degree no more than $4n$ and coefficients of magnitude $O(n^{c1}B^{c2}2^{c3n})$ for some constants $c1, c2, c3$. We can find all the real common zeros of the two polynomials in the box $-B \leq u, v \leq B$ to the required $l$-bit precision in time polynomial in $n, \log B, \log \epsilon$ using exact methods (running time is measured as proportional to the number of bit operations). We just note that a polynomial bound can be achieved by several methods including elimination based ones (see Arnon and McCallum (1988), and Manocha and Demmel (1994), for two different approaches). It may be possible to take advantage of the structure of $N_M$ to obtain a more efficient minimization algorithm.

Example 2.1. Let us consider the two polynomials
   \[ f = x^2 - 6x + 5 = (x - 1)(x - 5), \]
   \[ g = x^2 - 6.3x + 5.72 = (x - 1.1)(x - 5.2). \]
We see that there is a natural pairing of the roots of the two polynomials. The minimum norm change function in this case is
   \[ N_M = \frac{(\alpha^* - 6\alpha + 5)((\alpha^*)^2 - 6\alpha^* + 5) + (\alpha^2 - 6.3\alpha + 5.72)((\alpha^*)^2 - 6.3\alpha^* + 5.72)}{1 + \alpha\alpha^*}. \]
After substituting $\alpha = u + iv$, we have
\[
N_M = (2u^4 + 2v^4 + 4u^2v^2 - 123/5u^3 - 123/5uv^2 + 9713/100u^2 \\
+ 217/4v^2 - 16509/125u + 36074/625)/(1 + u^2 + v^2).
\]
The numerators of the two partial derivatives of $N_M$ meet at two real points. Computed to within $10^{-6}$ of the coordinates of the minima (using Maple), the two points are $(1.054336548, 0.0), (5.096939087, 0.0)$. In other words, the two candidates for a perturbed common root are 1.054336548, 5.096939087. The perturbed polynomials corresponding to the perturbed common root 1.054336548 are
\[
f_1 = x^2 - 5.892953016x + 5.101530184, \\
g_1 = x^2 - 6.394520309x + 5.630350913,
\]
and the net perturbation is 0.03873846846. The perturbed polynomials corresponding to the perturbed common root 5.096939087 are
\[
f_1 = x^2 - 6.075031814x + 4.985279044, \\
g_1 = x^2 - 6.222176901x + 5.735268595,
\]
and the net perturbation is 0.01213605293. This is an “easy” example in the sense that there is a natural pairing of the roots of the input polynomials (their resultant is small: $-0.3276$). In addition, the polynomials are stable, i.e. they are not very close to having multiple roots and we see that the perturbations required to produce a common root are quite small and indeed, each minimum brings together one “natural pair” of roots. However, notice that the pair that was farther (5.0, 5.2) came together to produce a smaller net perturbation than the closer pair (1.0, 1.1). If the roots are wildly scattered or if one/both the input polynomials are close to the discriminant variety (such as the well-known Wilkinson polynomial), one will see that relatively large perturbations are needed to produce a common root and, consequently, in the root domain one might see a wild scattering of the roots of the perturbed polynomials relative to the roots of the input polynomials.

3. Some Variants of the Nearest GCD Problem

The expression for $N_M$ generalizes in many different and interesting ways. We do not provide explicit derivations for the norm change expressions below. However, they can all be obtained by following the derivation of the expression for $N_M$ in the previous section in a straightforward manner.

**different degrees**

In the preceding section, in order to keep the exposition simple, we had assumed that $f, g$ have the same degree. If the degrees of $f, g$ are different, say, $\deg f = m, \deg g = n$, then we can essentially follow the steps in the previous derivation to arrive at the following expression for the minimum norm change:
\[
N_M = \frac{f(\alpha)f^*(\alpha)}{\sum_{i=0}^{m-1}(\alpha^i\alpha)^i} + \frac{g(\alpha)g^*(\alpha)}{\sum_{j=0}^{n-1}(\alpha^j\alpha)^j}.
\]
In the rest of this section, we assume that $\deg f = m, \deg g = n$, and without loss of generality, $m \geq n$. 
If one uses a weighted 2-norm such as \((\sum_{i=0}^{n} W_i f_i f_i^*)^{1/2}\), then the corresponding expression for the minimum norm change is

\[
N_M = \frac{f(\alpha)f^*(\alpha)}{\sum_{i=0}^{n-1} W_i(\alpha^*\alpha)^i} + \frac{g(\alpha)g^*(\alpha)}{\sum_{i=0}^{n-1} W_i(\alpha^*\alpha)^i}.
\]

**REPRESENTATION IN OTHER BASES**

If the polynomials are represented in some other basis, such as the Bernstein basis or the Chebyshev basis, we can rewrite the norm change expression as follows:

\[
N_M = \frac{f(\alpha)f^*(\alpha)}{\sum_{i=0}^{n-1} (b_i(\alpha)^*) b_i(\alpha))} + \frac{g(\alpha)g^*(\alpha)}{\sum_{i=0}^{n-1} (b_i(\alpha)^*) b_i(\alpha))}
\]

where \(b_i\) is the basis element of degree \(i\), i.e. \(f(x) = \sum_{i=0}^{n} f_i b_i(x)\) and \(g(x) = \sum_{i=0}^{n} g_i b_i(x)\).

**SPARSE PERTURBATIONS**

If \(f, g\) are sparse, i.e. some of \(f_i, g_j\) are zero and we are only allowed to perturb the non-zero coefficients of \(f, g\), then the corresponding expression for the minimum norm change is

\[
N_M = \frac{f(\alpha)f^*(\alpha)}{\sum_{i<\mu} (\alpha^*\alpha)^i} + \frac{g(\alpha)g^*(\alpha)}{\sum_{i<j} (\alpha^*\alpha)^j}.
\]

Stetter (1997) points out that sometimes, \(f, g\) may not be sparse but we may only be allowed to perturb certain coefficients (perhaps, the others are known exactly). This is a situation similar to the sparse perturbation situation. The expression for the minimum norm change is

\[
N_M = \frac{f(\alpha)f^*(\alpha)}{\sum_{i<\mu, \lambda_i \neq 0} (\alpha^*\alpha)^i} + \frac{g(\alpha)g^*(\alpha)}{\sum_{j<\nu, \mu_j \neq 0} (\alpha^*\alpha)^j}.
\]

The notation \(\lambda_i \neq 0, \mu_j \neq 0\) in the summations indicates that the summations are over those terms whose coefficients can be perturbed.

**REAL PERTURBATIONS**

Suppose \(f, g \in \mathcal{R}[x]\) and we want the smallest real perturbation that results in the perturbed polynomials having a non-trivial GCD. Find \(\alpha \in \mathcal{R}, \phi_1(x), \gamma_1(x) \in \mathcal{R}[x]\) of degrees \(m-1, n-1\) respectively that minimize \(N_1 = \| f - (x - \alpha) \phi_1 \|^2 + \| g - (x - \alpha) \gamma_1 \|^2\) by finding an \(\alpha \in \mathcal{R}\) that minimizes

\[
\frac{f(\alpha)^2}{\sum_{i=0}^{n-1} \alpha^{2i}} + \frac{g(\alpha)^2}{\sum_{i=0}^{n-1} \alpha^{2i}}.
\]

Find \(\alpha, \beta \in \mathcal{R}\), and \(\phi_2(x), \gamma_2(x) \in \mathcal{R}[x]\) of degrees \(m - 2, n - 2\) respectively that minimize \(N_2 = \| f - (x^2 + \alpha x + \beta) \phi_2 \|^2 + \| g - (x^2 + \alpha x + \beta) \gamma_2 \|^2\). To minimize \(N_2\), treat it as a function of the unknown coefficients of \(\phi_2(x), \gamma_2(x)\), minimize in the usual way by
setting the partial derivatives of \( N_2 \) with respect to these coefficients to zero. The partial derivatives are linear in the unknown coefficients and hence, the unknown coefficients can be eliminated in favor of \( \alpha, \beta \). The resulting minimum is a function of \( \alpha, \beta \). Minimize this over \( \alpha, \beta \). The perturbed polynomials corresponding to the smaller of the two minima (of \( N_1, N_2 \)) are the least perturbed polynomials relative to \( f, g \) in \( \mathcal{R}[x] \) that have a non-trivial GCD.

**Nearest Singular Polynomial**

Given a polynomial \( f \) of degree \( n \), find a polynomial close to it that has multiple roots; explicit expressions for the minimum value of the perturbation as a function of the coordinates of the multiple root, depending on the multiplicity, can be constructed. For instance, the smallest perturbation to the given polynomial \( f \) resulting in a polynomial that has a double root (which is not a triple root) can be obtained by minimizing the expression

\[
\frac{f(\alpha)f^*(\alpha)}{\sum_{i=0}^{n-1} (\alpha^* \alpha)^i} + \frac{f'(\alpha)f'^*(\alpha)}{\sum_{j=0}^{n-2} (\alpha^* \alpha)^j}
\]

with respect to \( \alpha \).

**4. Highest Degree Approximate Common Divisors**

In the nearest GCD problem, we concentrate on minimizing the net perturbations to the input polynomials \( f, g \). In the version of the highest degree approximate common divisor problem considered here, we are only allowed to perturb each of \( f \) and \( g \) up to separate error bounds \( r_1, r_2 \). We have to deal with this variation a little differently and we illustrate by considering the following simpler version of the problem first: given \( f, g \in \mathcal{R}[x] \) of respective degrees \( m \) and \( n \), and \( 0 < r_1, r_2 \in \mathcal{R} \) find \( \hat{f}, \hat{g} \) with \( \| f - \hat{f} \| \leq r_1, \| g - \hat{g} \| \leq r_2 \) such that \( \hat{f}, \hat{g} \) have a common real root and \( \| f - \hat{f} \|^2 + \| g - \hat{g} \|^2 \) is minimized. We set up a parametric minimization problem similar to the ones in the previous sections. Let

\[
N_M^{(f)} = \frac{f(\alpha)f^*(\alpha)}{\sum_{i=0}^{m-1} (\alpha^* \alpha)^i}, \quad N_M^{(g)} = \frac{g(\alpha)g^*(\alpha)}{\sum_{j=0}^{n-1} (\alpha^* \alpha)^j}.
\]

We need to find out whether the inequalities \( N_M^{(f)} \leq r_1 \) and \( N_M^{(g)} \leq r_2 \) can be simultaneously satisfied, and if so, find an \( \alpha \) satisfying the inequalities that minimizes \( N_M^{(f)} + N_M^{(g)} \). Let \( N_M^{(f)} = C_f/D_f \) and \( N_M^{(g)} = C_g/D_g \) with \( C_f, D_f, C_g, D_g \in \mathcal{R}[\alpha] \). The problem of checking whether the inequalities \( N_M^{(f)} \leq r_1 \) and \( N_M^{(g)} \leq r_2 \) can be simultaneously satisfied is solved by checking whether the polynomial inequalities

\[
C_f - r_1 D_f \leq 0 \quad \text{and} \quad C_g - r_2 D_g \leq 0
\]

can be simultaneously satisfied.

Satisfiability of univariate polynomial inequalities over \( \mathcal{R} \) is a classical problem and can be solved by Sturm sequence based methods or other real root isolation methods. \( N_M^{(f)} + N_M^{(g)} \) attains its absolute minimum inside the region \( N_M^{(f)} \leq r_1, N_M^{(g)} \leq r_2 \) either at one of its stationary points inside the region or on the boundary of the region. The
boundary points are some real roots of \( C_f - r_1 D_f = 0 \) or \( C_g - r_2 D_g = 0 \). Hence we can compute an \( \alpha \) where \( N_M^{(f)} + N_M^{(g)} \) attains its absolute minimum inside the region of interest by real root isolation. Some recent algorithms for real root isolation can be found in Johnson and Krandick (1997).

### 4.1. A Generalization of the Expression for the Change in Norm

As in Section 2, we start with polynomials \( f, g \), both of degree \( n \), monic. We perturb them to \( \hat{f}, \hat{g} \) such that the perturbed polynomials have \( d \) distinct common roots \( \alpha_1, \alpha_2, \ldots, \alpha_d \).

\[
\begin{align*}
 f(z) &= \sum_{i=0}^{n} f_i z^i, & g(z) &= \sum_{i=0}^{n} g_i z^i, & f_n = g_n = 1 \\
 \hat{f}(z) &= \sum_{i=0}^{n} \hat{f}_i z^i, & \hat{g}(z) &= \sum_{i=0}^{n} \hat{g}_i z^i, & \hat{f}_n = \hat{g}_n = 1 \\
 \hat{f}(\alpha_j) &= 0, & \hat{g}(\alpha_j) &= 0, & j = 0, \ldots, d.
\end{align*}
\]

The coefficients are perturbed by

\[
\lambda_i = f_i - \hat{f}_i, \quad \mu_i = g_i - \hat{g}_i, \quad i = 0, \ldots, n - 1.
\]

Let

\[
\lambda_i = \zeta_i + i\eta_i, \quad \mu_i = u_i + iv_i,
\]

where \( \zeta, \eta, u, v \) are real variables. We need to minimize

\[
N_{dd} = \sum_{i=0}^{n-1} \lambda_i \lambda_i^* + \sum_{i=0}^{n-1} \mu_i \mu_i^*.
\]

As before, we use Lagrange multipliers. Consider

\[
N_{dd} + \sum_{j=1}^{d} 2A_j \text{Re}(\hat{f}(\alpha_j)) + \sum_{j=1}^{d} 2B_j \text{Im}(\hat{f}(\alpha_j)) + \sum_{j=1}^{d} 2C_j \text{Re}(\hat{g}(\alpha_j)) + \sum_{j=1}^{d} 2D_j \text{Im}(\hat{g}(\alpha_j))
\]

(5)

where \( A_j, B_j, C_j, D_j \) are undetermined multipliers and \( \text{Re}(\hat{f}(\alpha_j)), \text{Im}(\hat{f}(\alpha_j)) \) denote the real and imaginary parts of \( \hat{f}(\alpha_j) \) respectively. Differentiating 5 with respect to the real and imaginary parts of each \( \lambda_i, \mu_i \) and solving for the various multipliers, we find that at the minima of \( N_{dd} \),

\[
\lambda_i = - \sum_{j=1}^{d} (A_j + iB_j) \alpha_j^{*i}, \quad \mu_i = - \sum_{j=1}^{d} (C_j + iD_j) \alpha_j^{*i}.
\]

(6)

and

\[
\begin{align*}
 f(\alpha_i) + \sum_{j=1}^{d} (A_j + iB_j)(\sum_{k=0}^{n-1} (\alpha_j^* \alpha_i)^k) &= 0, \\
g(\alpha_i) + \sum_{j=1}^{d} (C_j + iD_j)(\sum_{k=0}^{n-1} (\alpha_j^* \alpha_i)^k) &= 0, & i = 1, \ldots, d.
\end{align*}
\]

Let us rewrite this in matrix form as

\[
Mp = -f, \quad Mq = -g
\]
By Cramer’s rule, we have
\[ M_{i,j} = \sum_{k=0}^{n-1} (\alpha_i \alpha_j^*)^k, \]
and
\[
\begin{align*}
p &= \begin{pmatrix} (A_1 + iB_1) & \vdots & (A_d + iB_d) \\ (C_1 + iD_1) & \vdots & (C_d + iD_d) \end{pmatrix}, & f &= \begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_d) \end{pmatrix}, \\
q &= \begin{pmatrix} (C_1 + iD_1) & \vdots & (C_d + iD_d) \end{pmatrix}, & g &= \begin{pmatrix} g(\alpha_1) \\ \vdots \\ g(\alpha_d) \end{pmatrix}.
\end{align*}
\]
Let \( \Delta \) denote the determinant of \( M \), \( \Delta_{i,f} \) denote the determinant of the matrix obtained by replacing the \( j \)-th column of \( M \) by \( f \), \( \Delta_{j,g} \) denote the determinant of the matrix obtained by replacing the \( j \)-th column of \( M \) by \( g \), and \( \Delta_{i,j} \) denote the determinant of the \((d-1) \times (d-1)\) matrix obtained by deleting the \( i \)-th row and the \( j \)-th column of \( M \). By Cramer’s rule, we have
\[
\begin{align*}
(A_j + iB_j) &= -\Delta_{j,f}/\Delta, \quad j = 1, \ldots, d. \\
(C_j + iD_j) &= -\Delta_{j,g}/\Delta, \quad j = 1, \ldots, d. \tag{7}
\end{align*}
\]
Substituting (8) in (6), we obtain the following expression for the minimum value of \( \mathcal{N}_{dd} \) as a function of \( \alpha_1, \ldots, \alpha_d \), which we denote by \( \mathcal{N}_{ddM} \):
\[
\begin{align*}
\mathcal{N}_{ddM} &= \sum_{k=0}^{n-1} \left[ \frac{1}{\Delta} \sum_{i=1}^{d} \Delta_{i,f} \alpha_i^{*k} \left( \frac{1}{\Delta} \sum_{i=1}^{d} \Delta_{i,f} \alpha_i^{*k} \right)^* \right] \\
&\quad + \sum_{k=0}^{n-1} \left[ \frac{1}{\Delta} \sum_{i=1}^{d} \Delta_{i,g} \alpha_i^{*k} \left( \frac{1}{\Delta} \sum_{i=1}^{d} \Delta_{i,f} \alpha_i^{*k} \right)^* \right] \tag{8}
\end{align*}
\]
We will simplify the first summand in (9): the second summand simplifies in an identical manner. Since \( M \) is Hermitian, \( \Delta^* = \Delta \) and \( \Delta_{i,j}^* = \Delta_{j,i}^* \).
\[
\begin{align*}
\sum_{k=0}^{n-1} &\left[ \frac{1}{\Delta} \sum_{i=1}^{d} \Delta_{i,f} \alpha_i^{*k} \left( \frac{1}{\Delta} \sum_{i=1}^{d} \Delta_{i,f} \alpha_i^{*k} \right)^* \right] \\
&= \frac{1}{\Delta^2} \sum_{k=0}^{n-1} \sum_{i=1}^{d} \sum_{j=1}^{d} (-1)^{i+j} \Delta_{i,j} \alpha_i^{*k} \left( \sum_{i=1}^{d} (-1)^{i+j} \Delta_{i,j} \alpha_i^{*k} \right)^* \tag{9}
\end{align*}
\]
\[
\begin{align*}
&= \frac{1}{\Delta^2} \left[ \sum_{i=1}^{d} f(\alpha_i) f^*(\alpha_i) \Delta_{i,i} \Delta + \sum_{\substack{i,j=1 \colon i \neq j}}^{d} (-1)^{i+j} (f(\alpha_i) f^*(\alpha_j) \Delta_{i,j} \Delta + f(\alpha_j) f^*(\alpha_i) \Delta_{j,i} \Delta) \tag{10}
\right]
\end{align*}
\]
\[
\begin{align*}
&= \frac{1}{\Delta} \left[ \sum_{i=1}^{d} f(\alpha_i) f^*(\alpha_i) \Delta_{i,i} \Delta + \sum_{\substack{i,j=1 \colon i \neq j}}^{d} (-1)^{i+j} (f(\alpha_i) f^*(\alpha_j) \Delta_{i,j} + f(\alpha_j) f^*(\alpha_i) \Delta_{j,i}) \right] \tag{11}
\end{align*}
\]
Equation (10) is obtained by expanding each $\Delta_{i,f}$ on left-hand side along the $i$th column and collecting multiples of $f(\alpha_i)$, $f^*(\alpha_i)$.

Equation (11) is obtained by expanding the products in the summands in the right-hand side of (10), interchanging the summation (with respect to $k$ and $i$), collecting multiples of $f(\alpha_i)f^*(\alpha_i)$ together and collapsing them to the product $\Delta_{i,j}\Delta$.

Hence, we have

$$Ndd_M = \frac{1}{\Delta} \left[ \sum_{i=1}^{d} f(\alpha_i)f^*(\alpha_i)\Delta_{i,i} + \sum_{i,j=1 \atop i \neq j}^{d} (-1)^{i+j}(f(\alpha_i)f^*(\alpha_j)\Delta_{i,j} + f(\alpha_j)f^*(\alpha_i)\Delta_{j,i}) ight. $$

$$+ \sum_{i=1}^{d} g(\alpha_i)g^*(\alpha_i)\Delta_{i,i} + \sum_{i,j=1 \atop i \neq j}^{d} (-1)^{i+j}(g(\alpha_i)g^*(\alpha_j)\Delta_{i,j} + g(\alpha_j)g^*(\alpha_i)\Delta_{j,i}) \right].$$

We can rewrite this as

$$Ndd_M = FM^{-1}F^*T + GM^{-1}G^*T$$

where

$$F = [f(\alpha_1) \ f(\alpha_2) \ldots f(\alpha_d)], \quad G = [g(\alpha_1) \ g(\alpha_2) \ldots g(\alpha_d)],$$

$^*$ denotes conjugate transpose.

If the polynomials $f, g$ have different degrees, say, $m,n$ respectively, the corresponding expression of the minimum norm change turns out to be

$$Ndd_M = Ndd, f_M + Ndd, g_M$$

where

$$Ndd, f_M = FM^{(f)}M^{-1}F^*T, \quad Ndd, g_M = GM^{(g)}G^{-1}G^*T,$$

$F,G$ are as before and $M^{(f)}, M^{(g)}$ are $d \times d$ Hermitian matrices given by

$$M^{(f)}_{i,j} = \sum_{k=0}^{m-1} (\alpha_i\alpha_j^*)^k, \quad M^{(g)}_{i,j} = \sum_{k=0}^{n-1} (\alpha_i\alpha_j^*)^k.$$

It is not difficult to generalize the norm change expression for many of the variants listed in Section 3 to the degree $d$ case.

These expressions can be used in an obvious (but inefficient) manner to determine the highest degree approximate common divisor of $f, g$. Recall that we need to find $\hat{f}, \hat{g}$ with

$$\| f - \hat{f} \| \leq r_1, \| g - \hat{g} \| \leq r_2$$

for given $0 < r_1, r_2 \in \mathbb{R}$ such that GCD($f, g$) is the highest degree approximate common divisor of $f, g$. This can be computed by finding the largest integer $d$ for which

$$Ndd, f_M \leq r_1 \quad \text{and} \quad Ndd, g_M \leq r_2$$

and minimizing

$$Ndd, f_M + Ndd, g_M$$

for that $d$. The computation can be set up as a quantifier elimination problem over $\mathbb{R}$ in $\min(m,n)(\min(m,n) + 1)$ variables (variables being the real and imaginary parts of $\alpha_i$, $i = 1, \ldots, d$, $d$ varying from $1$ to $\min(m,n)$) with polynomial equalities and inequalities of degree $O(d(m+n))$. One can use the algorithm of Grigoriev and Vorobjov (1988) or of Renegar (1992) to perform the quantifier elimination and the complexity is doubly
exponential in $m, n$. This, as we well know, is not a feasible computation. It would be interesting to turn it into one. The norm change expression derived here leads to a GCD of the perturbed polynomials that is square-free — this may not be the highest degree approximate common divisor in some cases. A general expression taking this into account is used in the paper Karmarkar and Lakshman (1996).

5. Concluding Remarks

We have given precise characterizations of the nearest and highest degree approximate common divisors of a pair of polynomials and we have shown how to compute them by providing explicit expressions for the minimum perturbation of the input polynomials needed to obtain the nearest and highest degree approximate common divisors. Our characterizations appear to be robust as they can be adapted to a number of variations with ease. However, several questions are in need of good answers. We list a few that are of particular interest to us:

1. Can the knowledge of the norm change functions be built into Euclid-like algorithms that work in limited/adaptive precision for computing highest degree approximate common divisors?
2. How well does approximate computation carry over to other operations with polynomials, such as computing a square-free kernel or real root counting?
3. Does there exist a polynomial time algorithm for the general highest degree approximate common divisor problem?

The last question is an interesting theoretical question that has implications for several related approximation problems.

Acknowledgements

We are grateful to Professor Hans Stetter and an anonymous referee for several helpful suggestions leading to significant improvements in the presentation.

References

Karmarkar, N. K., Lakshman, Y. N. (1996). Approximate polynomial greatest common divisors and
INRIA, Sophia-Antipolis, France.
Renegar, J. (1992). On the computational complexity and geometry of the first-order theory of the reals:

Originally Received 6 December 1997
Accepted 21 July 1998