On the complexity of complex root isolation

Bernard Mourrain* Elias Tsigaridas†

April 5, 2010

Abstract

We consider the problem of analyzing the complexity of isolating the complex roots of polynomials with Gaussian integers as coefficients. We provide a simplified proof for the number of steps that a subdivision-based algorithm performs. If d is the degree of the polynomial and τ the maximum coefficient bitsize, then we prove a bound of $\tilde{\mathcal{O}}_B(d^7 + d^6\tau + d^5\tau^2)$, for algorithms based on Sturm sequences, thus improving the previously known by a factor.

1 Introduction

One of the fundamental operations in algebraic algorithms is root isolation of univariate polynomials, i.e. given a polynomial to compute intervals (*isolating intervals*) in the case of the real roots, or squares (*isolating squares*) in the case of the complex roots, that contain one and only one root of the polynomial, for every root.

In this paper we consider exact algorithms, that is algorithms that perform computations with rational numbers of arbitrary size, for the complex case. Given a polynomial with Gaussian integers as coefficients we wish to isolate its complex roots in a given square. Exact algorithms for this problem are typically based on Sturm sequences (denoted STURM-$\mathbb{C}$) [1, 6, 10]. For other certified approaches to this problem see, e.g., [4, 5, 7]. For the worst-case analysis of such algorithms, we significantly simplify the proof in [1] for bounding the number of subdivisions, and we improve the total complexity by a factor of d, thus obtaining a new bound of $\tilde{\mathcal{O}}_B(d^7 + d^6\tau + d^5\tau^2)$. We also prove that the same bound holds when the polynomial has Gaussian rationals as coefficients.

Notation. $\mathcal{O}_B$ means bit complexity and the $\tilde{\mathcal{O}}_B$-notation means that we are ignoring logarithmic factors. For $\mathsf{a} \in \mathbb{Q}$, $\mathcal{L}(\mathsf{a}) \geq 1$ is the maximum bitsize of the numerator and the denominator. We consider square-free polynomials. For $A = \sum_{i=1}^{d} c_i X^i \in (\mathbb{Z}[\mathbf{i}])[X]$, $\mathrm{dg}(A)$ denotes its degree. $\mathcal{L}(A)$ denotes an upper bound on the bitsize of the coefficients of A (including a bit for the sign), i.e. if $c_i = a_i + b_i$, then $\mathcal{L}(A) = \max_i\{\mathcal{L}(a_i), \mathcal{L}(b_i)\}$. Δ is the separation bound of A, that is the smallest distance between two complex roots of A and Δ_i is the smallest distance between the root i of A and all the other roots. Notice that $\Delta = \min_i\{\Delta_i\}$.

*project GALAAD, INRIA Méditerranée, Sophia-Antipolis, France. mourrain(at)sophia.inria.fr

†project GALAAD, INRIA Méditerranée, and Laboratoire I3S, CNRS and the University of Nice, Sophia-Antipolis, France. elias.tsigaridas(at)sophia.inria.fr

2 Complex root isolation

The first in analyzing the complexity of complex root isolation is to bound the number of steps (subdivisions) that an algorithm performs. The exact algorithms that we consider are based on Sturm sequences and computation of the Cauchy index, cf. [6, 10, 11]. For this we call the algorithm STURM-$\mathbb{C}$. The idea is, using a Sturm-based method, to count the number of complex roots in a square of the complex plane. If this number is ≥ 2, then the square is subdivided to 4 (equal) squares and the algorithm continues on each square.

We need the following proposition. For a proof we refer the reader to [3, 9].

Theorem 1 (Davenport-Mahler-Mignotte). *Let $A \in \mathbb{C}[X]$, with $\deg(A) = d$ and $\mathcal{L}(A) = \tau$, where $A(0) \neq 0$. Let Ω be any set of k couples of indices (i, j) such that $1 \leq i < j \leq d$ and let the non-zero (complex) roots of A be $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_d|$. Then*

$$2^k \mathcal{M}(A)^k \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{k-\frac{d(d-1)}{2}} \mathcal{M}(A)^{1-d-k} \sqrt{|\mathsf{disc}(A)|},$$

where $\mathcal{M}(A)$ is the Mahler measure of A.

If $A \in (\mathbb{Z}[\mathbf{i}])[x]$, that is its coefficients are Gaussian integers, $\{a + \mathbf{i}b \mid a, b \in \mathbb{Z}\}$ where $\mathcal{L}(a) \leq \tau$, then $\mathcal{M}(A) \leq \|A\|_2 \leq 2^{\tau+1/2}\sqrt{d+1}$.

2.1 The number of subdivisions

Thm. 1 allows us to prove a bound on the number of subdivisions needed to isolate all complex roots. Suppose that, initially, all complex roots are in a square of side B. This is either given, or derived as a bound on the roots' magnitude, e.g. $\mathsf{B} \leq 2^{\tau+1}$ [3, 11]. At step h, we check for complex roots in squares that have sides equal to $\mathsf{B}/2^h$.

Consider the algorithm expressed as a tree of out-degree 4, where each node holds a square and the root holds the initial square. Each leaf contains a square that isolates a complex root and, since there are at most d complex roots, this bounds the number of leaves. The squares that correspond to leaves have sides of length $\leq \Delta_j$ and the number of nodes from a leaf to the root is

$$\left\lceil \log \frac{\mathsf{B}}{\Delta_j} \right\rceil.$$

The number of subdivisions equals the number of nodes, which is

$$\#(T) = \sum_{j=1}^{d} \left\lceil \lg \frac{\mathsf{B}}{\Delta_j} \right\rceil = 2d + d\tau - \sum_{j=1}^{d} \lg \Delta_j = 2d + d\tau - \lg \prod_{j=1}^{d} \Delta_j. \tag{1}$$

It remains to bound $\prod_{j=1}^{d} \Delta_j$. For this we use Thm. 1. Recall that the hypotheses of the theorem are not fulfilled when symmetric products occur. So, $\prod_{i=1}^{d} \Delta_i = \prod_{i=1}^{k_1} \Delta_i \prod_{i=1}^{k_2} \Delta_i$, where $k_1 + k_2 = d$ and the factors are such that no symmetric products occur. By applying to each factor Thm. 1 and by taking into account that $|\mathsf{disc}(A)| \geq 1$ we have:

$$\prod_{i=1}^{d} \Delta_i \geq 2^{d^2} \mathcal{M}(A)^{2-3d} \geq 2^{d^2} (2^{\tau}\sqrt{d+1})^{2-3d},$$

since $\mathcal{M}(A) \leq 2^{\tau}\sqrt{d+1}$. If we combine the last equation with (1) we obtain:

Lemma 2. *The number of subdivisions for complex root isolation is* $\mathcal{O}(d^2 + d\tau)$.

The proof of this lemma simplifies significantly the proof appeared in [1], where an amortized-like argument is used. Our bound on the number of subdivisions has d^2 instead of $d \lg d$ which, as in the real root case, is immaterial when $d = \mathcal{O}(\tau)$. Moreover, if the initial polynomial is not square-free, this is again immaterial, because the square-free factorization causes the square-free polynomial to have coefficients of size $\mathcal{O}(d + \tau)$.

2.2 Overall complexity

Consider a polynomial $A(X) \in (\mathbb{Z}[\mathbf{i}])[X]$, where X is a complex variable, i.e. $X = x + \mathbf{i}y$. After substitution and some elementary operations, A can be written as $A(X) = A_0(x, y) + \mathbf{i}A_1(x, y)$, where $A_0, A_1 \in \mathbb{Z}[x, y]$ and x, y are real variables.

To count the number of complex roots in a square we will use the notion of the degree of the Gauss map [8]. We refer the reader to Wilf [10], Pinkert [6], for alternative, however equivalent, approaches. Let $\mathbf{SR}(f, g)$ denote a signed polynomial remainder sequence of the polynomials f and g and $\mathtt{VAR}(\mathbf{SR}(f, g)\,;\,\mathsf{a}))$ the number of sign variation occur when we evaluate the sequence over a rational number a. The Cauchy index of the real function g/f in an interval $[\mathsf{a}, \mathsf{b}]$ is

$$I_{\mathsf{a}}^{\mathsf{b}}(g/f) = \mathtt{VAR}(\mathbf{SR}(f, g)\,;\,\mathsf{a})) - \mathtt{VAR}(\mathbf{SR}(f, g)\,;\,\mathsf{b})).$$

The following holds

Proposition 3. *[8] The number of roots, r, of $A(X)$ in a square in the complex plane defined by $a_1 \leq x \leq a_2$ and $a_3 \leq y \leq a_4$, is given by*

$$r = -\frac{1}{2}(R_1 + R_2 + R_3 + R_4)$$

where

$$R_1 = I_{a_1}^{a_2}(A_1(x, a_3), A_0(x, a_3)), \quad R_2 = I_{a_3}^{a_4}(A_1(a_2, y), A_0(a_2, y)),$$
$$R_3 = I_{a_2}^{a_1}(A_1(x, a_4), A_0(x, a_4)), \quad R_4 = I_{a_4}^{a_3}(A_1(a_1, y), A_0(a_1, y)).$$

To isolate the complex root of A we start with the first quadrant, i.e. we isolate the roots in the square $[0, \mathsf{B}] \times [0, \mathsf{B}]$. We apply Prop. 3 and we count the complex roots. If there are more than one roots, then we split the square to four squares and we continue the process to each of them.

Applying Prop. 3 consists in computing 4 times the Cauchy index. Each such computation corresponds to the evaluation of signed polynomial remainder sequence. It suffices to study only the complexity of computing R_1. The polynomials $A_0(x, y)$ and $A_1(x, y)$ are of degree at most d and maximum coefficient bitsize τ. At the h step of algorithm, we have to compute the Cauchy index of $A_0(x, \mathsf{B}/2^h)$ and $A_1(x, \mathsf{B}/2^h)$, over rationals of magnitude at most $\mathsf{B}/2^h$; thus of bitsize $\leq h + \lg B = h + \tau$. The degree of these polynomials is $\leq d$ and their bitsize is $\widetilde{\mathcal{O}}(\tau + d\tau + dh)$, or $\widetilde{\mathcal{O}}(d\tau + dh)$. The computation of Cauchy index costs $\widetilde{\mathcal{O}}_B(d^2(d\tau + dh + \tau + h)$, or $\widetilde{\mathcal{O}}_B(d^3\tau + d^3h)$ [2]. Multiplying by the number of steps, h, we get a bound of $\widetilde{\mathcal{O}}_B(d^3\tau h + d^3h^2)$, and by applying Lem. 2 we get an overall complexity of $\widetilde{\mathcal{O}}_B(d^7 + d^6\tau + d^5\tau^2)$, or $\widetilde{\mathcal{O}}_B(N^7)$, where $N = \max\{d, \tau\}$.

This completes the proof of the following:

Theorem 4. *The worst-case complexity of complex root isolation, of a polynomial with Gaussian integers as coefficients of degree bounded by d and bitsize bounded by τ, is in $\widetilde{\mathcal{O}}_B(d^7 + d^6\tau + d^5\tau^2)$, or $\widetilde{\mathcal{O}}_B(N^7)$.*

The previous theorem improves the bound in [1] by a factor.

2.3 The case of Gaussian rationals

In the previous analysis we assumed that the coefficients of the polynomial where Gaussian integers. A natural question to ask is whether the complexity bound holds if the coefficients are Gaussian rationals, that is numbers in the set $\{a + \mathbf{i}b \mid a, b \in \mathbb{Q}\}$. Recall, that the bitsize of a rational number is the maximum of the bitsizes of the numerator and the denominator.

We could eliminate denominators by multiplying by their least common multiple. Since the bitsize of the coefficients is $\leq \tau$, after the elimination we get a polynomial with Gaussian integers as coefficients, the bitsize of which is bounded by $d\tau$.

Even though the bitsize of the polynomial increases, we observe that the Mahler bound of the polynomial does not change, since it is the product of the roots with measure greater than one. This implies, refer to Thm. 1, that the bitsize of the separation bound, and the number of subdivisions remains the same, i.e. $\tilde{\mathcal{O}}_B(d^2 + d\tau)$.

Following the analysis of the previous section, we see that also in this case, at each step, we have to compute the Cauchy index of polynomials of degree d and of bitsize $\mathcal{O}(d\tau + dh)$. Thus the overall complexity remains the same.

Corollary 5. *The bound of Thm. 4 holds even in the case where the coefficients are Gaussian rationals.*

3 Conclusion and future work

In this paper we simplified the proof for computing the number of steps that a subdivision algorithm performs to isolate the complex roots of a polynomial with Gaussian coefficients, we improved the bound of the exact algorithms for the problem, based on Sturm sequences, by a factor d and we proved that the bound also holds when the polynomial has Gaussian rationals, of the same bitsize, as coefficients.

The techniques that we presented will be useful to study the complexity of algorithms for complex root isolation that are based on the computation of the topological degree, e.g.[4]. Such algorithms allows complex root counting to be performed to more complicated areas than squares, e.g. polygons, and they are amenable to efficient implementations.

Last, but not least, we are currently working towards obtaining output-sensitive complexity results, as well as bounds for the average case.

Acknowledgments.

This work is partially supported by contract ANR-06-BLAN-0074 "Decotes".

References

[1] Z. Du, V. Sharma, and C. K. Yap. Amortized bound for root isolation via Sturm sequences. In D. Wang and L. Zhi, editors, *Int. Workshop on Symbolic Numeric Computing*, pages 113–129, School of Science, Beihang University, Beijing, China, 2005. Birkhauser.

[2] T. Lickteig and M-F. Roy. Sylvester-Habicht Sequences and Fast Cauchy Index Computation. *J. Symb. Comput.*, 31(3):315–341, 2001.

[3] M. Mignotte. *Mathematics for computer algebra.* Springer-Verlag, New York, 1991.

[4] B. Mourrain, M. Vrahatis, and J.C. Yakoubsohn. On the complexity of isolating real roots and computing with certainty the topological degree. *J. Complexity*, 18(2), 2002.

[5] V.Y. Pan. Univariate polynomials: Nearly optimal algorithms for numerical factorization and rootfinding. *J. Symbolic Computation*, 33(5):701–733, 2002.

[6] J. R. Pinkert. An exact method for finding the roots of a complex polynomial. *ACM Trans. Math. Softw.*, 2(4):351–363, 1976. ISSN 0098-3500. doi: http://doi.acm.org/10.1145/355705.355710.

[7] S. M. Rump. Solving algebraic problems with high accuracy (habilationsschrift). In U. W. Kulish and W. L. Miranker, editors, *A new approach to Scientific Computation*, pages 51–120. Academic Press, New York, 1983.

[8] T. Sakkalis. The Euclidean Algorithm and the Degree of the Gauss Map. *SICOMP: SIAM Journal on Computing*, 19(3):538–543, 1990.

[9] E. P. Tsigaridas and I. Z. Emiris. On the complexity of real root isolation using Continued Fractions. *Theoretical Computer Science*, 392:158–173, 2008.

[10] H. S. Wilf. A global bisection algorithm for computing the zeros of polynomials in the complex plane. *J. ACM*, 25(3):415–420, 1978. ISSN 0004-5411. doi: http://doi.acm.org/10.1145/322077.322084.

[11] C.K. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.