A Simple But Exact and Efficient Algorithm for Complex Root Isolation*

Michael Sagraloff
Max Planck Institute for Informatics
msagralo@mpi-inf.mpg.de

Chee K. Yap
Courant Institute of Mathematical Sciences
yap@cs.nyu.edu

ABSTRACT

We present a new exact subdivision algorithm CEVAL for isolating the complex roots of a square-free polynomial in any given box. It is a generalization of a previous real root isolation algorithm called EVAL. Under suitable conditions, our approach is applicable for general analytic functions. CEVAL is based on the simple Bolzano Principle and is easy to implement exactly. Preliminary experiments have shown its competitiveness.

We further show that, for the "benchmark problem" of isolating all roots of a square-free polynomial with integer coefficients, the asymptotic complexity of both algorithms EVAL and CEVAL matches (up a logarithmic term) that of more sophisticated real root isolation methods which are based on Descartes' Rule of Signs, Continued Fraction or Sturm sequences. In particular, we show that the tree size of EVAL matches that of other algorithms.

Our analysis is based on a novel technique called δ-clusters from which we expect to see further applications.

1. INTRODUCTION

Root finding might be called the *Fundamental Problem of Algebra*, after the Fundamental Theorem of Algebra [**?**, **?**, **?**]. The literature on root finding is extremely rich, with a large classical literature. The work of Schönhage [**?**] marks the beginning of complexity-theoretic approaches to the Fundamental Problem. Pan [**?**] provides a history of root-finding from the complexity view point; see McNamee [**?**] for a general bibliography. The root finding problem can be studied as two distinct problems: root isolation and root refinement. In the complexity literature, the main focus is on what we call the **benchmark problem**, that is, isolating all the complex roots of a polynomial f of degree n with integer coefficients of at most L bits. Let $T(n, L)$ denote the (worst case) bit complexity of this problem. There are three variations on this benchmark problem:

- We can ask for only the real roots. Special techniques apply in this important case [**?**, **?**]. E.g., Sturm [**?**, **?**, **?**], Descartes [**?**, **?**, **?**, **?**, **?**], and continued fraction methods [**?**, **?**].
- We can seek the arithmetic complexity of this problem, that is, we seek to optimize the number $T_A(n, L)$ of arithmetic operations.
- We can add another parameter $p > 0$, and instead of isolation, we may seek to approximate each of the roots to p relative or absolute bits.

Schönhage achieved a bound of $T(n, L) = \widetilde{O}(n^3 L)$ for the benchmark isolation problem where $\widetilde{O}$ indicates the omission of logarithmic factors. This bound has remained intact. Pan and others [**?**, **?**] have given theoretical improvements in the sense of achieving $T_A(n, L) = \widetilde{O}(n^2 L)$ and $T(n, L) = T_A(n, L) \cdot \widetilde{O}(n)$, thus achieving record bounds simultaneously in both bit complexity and arithmetic complexity. Theoretical algorithms designed to achieve record bounds for the benchmark problem have so far not been used in practice. Moreover, the benchmark problem is inappropriate for some applications. For instance, we may only be interested in the first positive root (as in ray shooting in computer graphics), or in the roots in some specified neighborhood. In the numerical literature, there are many algorithms that are widely used and effective in practice but lack a guarantee on the global behavior (cf. [**?**] for discussion). Some "global methods" such as the Weierstrass or Durant-Kerner method that simultaneously approximates all roots seem ideal for the benchmark problem and work well in practice, but their convergence and/or complexity analysis are open. Thus, the benchmark complexity, despite its theoretical usefulness, has limitation as sole criterion in evaluating the usefulness of root isolation algorithms.

There are two sub-literature on "practical" root isolation algorithms: (1) One is the exact computation literature, providing algorithms used in various algebraic applications and computer algebra systems. Such exact algorithms have a well-developed complexity analysis and there is considerable computational experience especially in the context of cylindrical algebraic decomposition. The favored root isolation algorithms here, applied to the benchmark problem, tend to lag behind the theoretical algorithms by a factor of nL. Nevertheless, current experimental data justify their use [**?**, **?**]. (2) The other is the numerical literature mentioned above. Although numerical algorithms traditionally lack any exactness guarantees, they have many advantages that practitioners intuitively understand: compared to algebraic methods,

*The full paper is available from `http://www.mpi-inf.mpg.de/~msagralo/` or `http://cs.nyu.edu/exact/`.

they are easier to implement and their complexity is more adaptive. Hence, there is a growing interest in constructing numerical algorithms that are exact and efficient.

§1. The Subdivision Approach.

Among the exact root isolation algorithms, the subdivision paradigm is widely used. It is a generalization of binary search in which we search for roots in a given domain (say a box $B_0 \subseteq \mathbb{C}$). Its principle action is a simple **subdivision phase** where we keep subdividing boxes into 4 congruent subboxes until each box B satisfies a predicate $C_{stop}(B)$. Typically, $C_{stop}(B) \equiv C_{out}(B) \vee C_{in}(B)$ where $C_{out}(B)$ is an **exclusion predicate** whose truth implies that B has no roots, and $C_{in}(B)$ is an **inclusion predicate** whose truth implies that B contains a unique root. Unlike global root finding methods that must find all roots simultaneously, subdivision methods have the advantage of being "local": they can restrict computational effort to the given box B_0, and may terminate quickly if there few or no roots in B_0.

Exact implementation of $C_{stop}(B)$ can be based on algebraic properties such as generalized Sturm sequences [**?**, Chap. 7]. Unfortunately, algebraic predicates are expensive. Since finding a root is metaphorically like "finding a needle in a hay stack", an efficient exclusion predicate C_{out} can be highly advantageous. Numerical exclusion predicates have been used in Dedieu, Yakoubsohn and Taubin [**?**, **?**, **?**] but the inclusion predicate in these papers are inexact, based on an arbitrary ϵ-cutoff: $C_{in}(B) \equiv size(B) < \epsilon$. *Our paper will exploit numerical exclusion and inclusion predicates to yield exact subdivision algorithms.*

§2. Three Principles for Subdivision.

We compare three general principles used in subdivision algorithms for real root isolation: theory of Sturm sequences, Descartes' rule of sign, and the Bolzano principle. The latter principle is simple and intuitive: *if a continuous real function $f(x)$ satisfies $f(a)f(b) < 0$, then there is a point c between a and b such that $f(c) = 0$. Furthermore, if f is differentiable and f' does not vanish on (a, b), then this root is unique in (a, b).* Modern algorithmic treatment of the Descartes method began with Collins and Akritas [**?**]. In recent years, algorithms based on the first two principles have been called (respectively) **Sturm method** [**?**, **?**, **?**] and the **Descartes method** [**?**, **?**, **?**, **?**]. By analogy, algorithms based on the third principle may be classified under the **Bolzano method** [**?**, **?**, **?**]. Note that the Bolzano principle is an analytic one, while Sturm is algebraic (Descartes seems to have an intermediate status).

Johnson [**?**] has shown empirically that the Descartes method is more efficient than Sturm. Rouillier and Zimmermann [**?**] implemented a highly efficient exact real root isolation algorithm based on the Descartes method. Since their theoretical bounds are indistinguishable, any practical advantage of Descartes over Sturm must be derived from the fact that the predicates in the Descartes method are cheaper. We believe that Bolzano methods have a similar advantage over Descartes. Such evidence is provided in a recent empirical study of Kamath [**?**] where a version of Ceval is compared with several algorithms, including the well-known Mpsolve of Bini and Fiorentini [**?**, **?**]. Bolzano methods also have the advantage of greater generality: *The Bolzano method is applicable to the much larger class of complex analytic functions. Our* Ceval *algorithm can be adapted to such functions under mild conditions.*

§3. Complexity Analysis.

All complexity analysis is for the above benchmark problem of isolating all roots of a polynomial $f(z)$. There are two complexity measures for subdivision algorithms: the subdivision tree size $S(n, L)$ and the bit complexity $P(n, L)$ of the subdivision predicates. Clearly, $T(n, L) \leq S(n, L)P(n, L)$. But the analysis in this paper shows that $T(n, L)$ may be smaller than $S(n, L)P(n, L)$ by a factor of n. For the Sturm method, Davenport [**?**] has shown that the benchmark problem of isolating all real roots of $f(x)$ has tree size $S(n, L) = O(n(L + \log n))$. This is optimal if $L \geq \log n$ [**?**]. The tree size in the Descartes method was only recently proven to be $O(n(L + \log n))$ [**?**], matching the Sturm bound. In this paper, we will prove that the tree size in the Bolzano method is $\widetilde{O}(n(L+\log n))$ for real roots. Furthermore, in our extension of the Bolzano method for complex roots the corresponding tree size is $\widetilde{O}(n^2(L + \log n))$. Despite this larger tree size, we prove that both real and complex Bolzano have $\widetilde{O}(n^4L^2)$ bit complexity, matching Descartes and Sturm.

Our complexity analysis of Bolzano methods is novel, and it opens up the exciting possibility of analysis of similar subdivision algorithms as in meshing of algebraic surfaces [**?**, **?**, **?**]. Perhaps it is no surprise that Bolzano methods could outperform the more sophisticated algebraic methods in practice. *What seems surprising from our analysis is that Bolzano methods could also match (up to a logarithmic factor) the theoretical complexity of algebraic methods as well.*

§4. Contributions of this paper.

1. Our complex root isolation algorithm (Ceval) is a contribution to the growing literature on exact algorithms based on numerical techniques and subdivision. The algorithm is simple and practical. Preliminary implementation shows that it is competitive with the highly regarded `MPSOLVE`.
2. This paper provides a rather sharp complexity analysis of Eval. Somewhat surprisingly, the worst-case bit-complexity of this simple algorithm can match (up to logarithmic-factors) those of sophisticated methods like Sturm or Descartes.
3. We further show that the more general Ceval also achieves the same bit complexity as Eval (despite the fact that the tree size of Ceval may be quadratically larger).
4. Our analysis is based on the novel technique of δ-clusters. We expect to see other applications of cluster analysis. This is a contribution to the general challenge of analyzing the complexity of numerical subdivision algorithms.

§5. Overview of Paper.

Section 2 reviews related work. The algorithm is presented in Section 3. In Section 4, we sketch our approach of δ-cluster from which we derive the complexity analysis of Eval and Ceval. Complete proofs appear in the full paper [**?**] and appendix: Appendix A develops our δ-cluster analysis technique. Appendix B gives the complexity analysis of Eval and Ceval in terms of tree-size and bit-size.

2. PRIOR WORK

The main distinction among the various subdivision algorithms is the choice[1] of tests or predicates. One approach

[1]We use the terms "predicate" and "test" interchangeably.

is based on doing root isolation on the boundary of the boxes. Pinkert [**?**] and Wilf [**?**] (see also [**?**, Chap. 7]) use Sturm-like sequences, while Collins and Krandick [**?**] considered Descartes method. Such approaches are related to topological degree methods [**?**], which go back to Brouwer (1924). But root isolation on boundary of subdivision boxes and topological degrees computations are relatively expensive and unnecessary: as shown in this paper, weaker but cheaper predicates may be more effective. This key motivation for our present work came from subdivision algorithms for curve approximation where a similar phenomenon occurs [**?**]. We next review several previous work that are most closely related to our paper.

§6. Work of Pan, Yakoubsohn, Dedieu and Taubin.

Pan [**?**, **?**, **?**, **?**] describes a subdivision algorithm with the current record asymptotic complexity bound. Pan regards his work as a refinement of Weyl's Exclusion Algorithm (1924). Weyl is also the basis for Henrici and Gargantini (1969) and Renegar (1987) (see [**?**]). The predicates are based on estimating the distance from the midpoint of a box B to the nearest zero of the input polynomial $f(z)$. Turan (1968) provides such a bound up to a constant factor, say 5. Pan further reduce this factor to $(1+\epsilon)$ (for a small $\epsilon > 0$) by applying the Graeffe iteration to $f(z)$. Finally, he combines the exclusion test with Newton-like accelerations to achieve the bound of $O(n^2 \ln n \ln(hn))$, where h is the cut-off depth of subdivision. Pan noted that "*there remains many open problems on the numerical implementation of Weyl's algorithm and its modification*" [**?**, p. 216]; in particular, "*proximity tests should be modified substantially to take into account numerical problems ... and controlling the precision growth*" [**?**, p. 193].

The approach of Yakoubsohn and Dedieu [**?**, **?**] is much simpler than Pan's. Their algorithm keep subdividing boxes until each box B satisfies an exclusion predicate $C_{out}(B)$, or B is smaller than an arbitrary cut-off $\epsilon > 0$. For any analytic function f, their predicate $C_{out}(B)$ is "$M^f(z, r\sqrt{2}) > 0$" where B is a square centered at z of length $2r$, and

$$M^f(z,t) := |f(z)| - \sum_{k\geq 1} \frac{|f^{(k)}(z)|}{k!} t^k. \tag{1}$$

It is easy to see that if $C_{out}(B)$ holds, then B has no roots of f. Taubin [**?**, **?**] introduce exclusion predicates that can be viewed as the linearized form of $M^f(z,t)$ or a Newton correction term. He shows their effectiveness in approximating (rasterizing) surfaces. These algorithms are useful in practice, but the use of ϵ-cutoff does not constitute a true inclusion predicate in the sense on §1: at termination, we have a collection of non-excluded ϵ-boxes, none of which is guaranteed to isolate a root.

§7. The Eval Algorithm.

The starting point for this paper is a simple algorithm for real root isolation. Suppose we want to isolate the roots of a real analytic function $f : \mathbb{R} \to \mathbb{R}$ in the interval $I_0 = [a, b]$. Assume f has only simple roots in I_0. For any interval I with center $m = m(I)$ and width $w = w(I)$, we introduce two interval predicates using the function in (**??**):

$$\left.\begin{array}{rcl} C_0(I) & \equiv & M^f(m, w/2) > 0 \\ C_1(I) & \equiv & M^{f'}(m, w/2) > 0 \end{array}\right\} \tag{2}$$

Clearly, $C_0(I)$ is an exclusion predicate. Note that if $C_1(I)$ holds, then f has at most one zero in I. Thus $C_1(I)$, in combination with the following **root confirmation test**,

$$f(a)f(b) < 0, \qquad \text{where } I = [a, b], \tag{3}$$

constitute an inclusion predicate. Here is the algorithm:

```
EVAL(I_0):
    Q ← {I_0} where Q is a queue of intervals.
    While Q is non-empty:
        Remove I from Q.
1.      If C_0(I) holds, discard I.
2.      Else if C_1(I) holds,
3.          If I passes the root confirmation test (??), output I.
4.          Else, discard I.
5.      Else
6.          If f(m) = 0, output [m, m] where m = m(I).
7.          Split I at m and put the two subintervals into Q.
```

Termination and correctness are easy to see (e.g., [**?**]). Output intervals either have the exact form $[m, m]$ or are regarded as open intervals (a, b). This algorithm is easy to implement exactly if we assume that all intervals are represented by dyadic numbers.

Mitchell [**?**] seems to be the first to explicitly describe EVAL, but as he assumes approximate floating point arithmetic, he does not check if $f(m) = 0$ at the midpoint m. He attributes ideas to Moore [**?**]. The second author of the present paper initiated the complexity investigation of EVAL (and its extension for multiple roots) as the 1-D analogue of the surface meshing algorithm of Plantinga-Vegter [**?**, **?**, **?**]. In [**?**], we succeeded in obtaining a bound of $O(n^3(L+\log n))$ when EVAL is applied to the benchmark problem. The proof involves several highly technical tools, but the approach is based on the novel concept of **continuous amortization**. The idea is to bound the tree size in terms of an integral $\int_I \frac{dx}{F(x)}$ where $F(x)$ is a suitable "stopping function". Our complexity analysis also extends to the complex root isolation algorithm CEVAL. Our upper bound for the bit complexity of CEVAL matches those of EVAL, Sturm and Descartes method. It is unknown whether the continuous amortization approach can achieve similar bounds.

3. THE COMPLEX ROOT ALGORITHM

In this section, we describe CEVAL, the complex analogue of EVAL. In fact, we describe two versions of CEVAL, and only prove the correctness of the simpler version here. The algorithm in described in way that allows a straight forward exact implementation.

Notation. For the rest of this paper, we fix a square-free polynomial $f \in \mathbb{C}[z]$. Our goal is isolate the complex zeros of $f(z)$ in a given box $B_0 \subseteq \mathbb{C}$. Our algorithms use two basic shapes: boxes and disks. Let $\xi, \mu \in \mathbb{C}$ and $r > 0$. Let $D_r(m)$ denote the disk of radius $r > 0$ centered at $m \in \mathbb{C}$. We write "$\xi \leq \mu$" if $\mathtt{Re}(\xi) \leq \mathtt{Re}(\mu)$ and $\mathtt{Im}(\xi) \leq \mathtt{Im}(\mu)$. A subset $B \subseteq \mathbb{C}$ is called a **box** if $B = B(\xi, \mu) := \{z \in \mathbb{C} : \xi \leq z \leq \mu\}$ for some $\xi \leq \mu$. The **midpoint** of $B(\xi, \mu)$ is $m(B) := (\xi + \mu)/2$. The **width** and **radius** of $B(\xi, \mu)$ are given by $w(B) := \max\{\mathtt{Re}(\mu) - \mathtt{Re}(\xi), \mathtt{Im}(\mu) - \mathtt{Im}(\xi)\}$ and $r(B) := \sqrt{(w(B)/2)^2 + (d(B)/2)^2}$, respectively. We can split a box B into four equally dimensioned subboxes, called the **children** of B. The boundary

of a region $R \subseteq \mathbb{C}$ is denoted ∂R (R is usually a disk or a box). A box B or disk D is said to be **isolating** if it contains exactly one zero of $f(z)$.

§8. Complex Analogues of C_0 and C_1 Predicates.

For $m \in \mathbb{C}$ and $K, r > 0$, we define the **test function** $t^f(m,r)$ and the **predicate** $T_K^f(m,r)$ as follows:

$$t^f(m,r) := \sum_{k\geq 1} \left|\frac{f^{(k)}(m)}{f(m)}\right| \frac{r^k}{k!} \quad (4)$$

$$T_K^f(m,r) \equiv t^f(m,r) < \frac{1}{K} \quad (5)$$

Since f is fixed in this paper, we simply write $T_K(m,r)$ for $T_K^f(m,r)$. When f' is used in place of f, then we simply write $T'_K(m,r)$ for $T_K^{f'}(m,r)$. Moreover, for any disk D, we may write $T_K(D)$ for $T_K(m(D), r(D))$, etc. We further remark that the success of $T_K^f(m,r)$ implies the success of $T_{K'}^f(m,r)$ for any $K' \leq K$, and $T_K^f(m,r)$ is equivalent to $T_K^{f(m+rx/\lambda)}(0,\lambda)$ with $\lambda \in \mathbb{R}$ an arbitrary positive real value.

Lemma 1 (Exclusion-Inclusion Properties).
Consider any disk $D = D_r(m)$:
(i) If $T_1(D)$ holds, the closure $\overline{D}$ of D has no root of f.
(ii) If $T_1(D)$ fails, the disc $D_{2nr}(m)$ has some root of f.
(iii) If $T'_{\sqrt{2}}(D)$ holds, $\overline{D}$ has at most one root of f.

Proof. See [**?**, **?**] for the proof of (i) and (iii). We show the contrapositive of (ii): let $z_1, \ldots, z_n$ denote the roots of f and suppose that $D_{2nr}(m)$ contains no root. Then,

$$\left|\frac{f^{(k)}(m)}{f(m)}\right| = \left|\sum\nolimits'_{i_1,\ldots,i_k} \frac{1}{(m-z_{i_1})\ldots(m-z_{i_k})}\right| \leq \Sigma_k(m) := \left(\sum_{i=1}^n \left|\frac{1}{m-z_i}\right|\right)^k \leq \left(\frac{1}{2r}\right)^k, \quad (6)$$

where the prime means that the i_j's ($j = 1 \ldots k$) are chosen to be distinct. Hence, it follows that

$$\sum_{k\geq 1} \left|\frac{f^{(k)}(m)}{f(m)}\right| \frac{r^k}{k!} < \sum_{k\geq 1} \frac{1}{k!}\left(\frac{1}{2}\right)^k < e^{\frac{1}{2}} - 1 < 1$$

and, thus, $T_1(D)$ holds. **Q.E.D.**

Part (i) of the lemma shows that $T_1(D)$, in analogy to $C_0(I)$, is an exclusion predicate for $D = D_r(m)$. Part (ii) shows that the negation of $T_1(D)$ is a root confirmation test like (**??**), albeit for the enlarged disc $D^+ := D_{2nr}(m)$. Part (iii) shows that $T'_{\sqrt{2}}(D)$ plays the role of the predicate $C_1(I)$. From (ii) and (iii) we could derive an inclusion predicate.

The next lemma gives lower bounds on the size of discs that pass our tests. The bounds are in terms of the **separation** $\sigma(\xi) := \min_{j\neq i} |z_i - \xi|$ of a root $\xi := z_i$ of f, and the **separation** $\sigma(f) := \min_i \sigma(z_i)$ **of** f.

Lemma 2. *Consider any disk $D = D_r(m)$ and a root $\xi := z_i$ of f:*
(i) If $r \leq \sigma(f)/(4n^2)$, then either $T_1(D)$ or $T'_{\sqrt{2}}(D)$ holds.
(ii) If D contains ξ and $r \leq \sigma(\xi)/(4n^2)$, then $T'_{\sqrt{2}}(D)$ holds.
(iii) If D contains ξ and $r \leq \sigma(\xi)/(8n^3)$, then D^+ is isolating.

Proof. For (i), suppose that $r \leq \sigma(f)/(4n^2)$ and both $T_1(D)$ and $T'_{\sqrt{2}}(D)$ do not hold. Then, according to Lemma **??** (ii), $D_{2nr}(m)$ must contain a root z of f. The same result applied to f' shows that $D_{2nr}(m)$ also contains a root z' of f'. It follows that $|z - z'| < 4nr \leq \sigma(f)/n \leq \sigma(z)/n$ contradicting the fact [**?**, **?**] that $D_{\sigma(z)/n)}(z)$ does not contain any root of the derivative f'. Part (ii) follows from (i) since $\xi \in D$ implies that $T_1(D)$ does not hold. Part (iii) is a direct consequence of (ii). **Q.E.D.**

§9. Simplified Complex Root Isolation.

We are ready to present a complex version of Eval. Call a disk $D_r(m)$ **well-isolating** if $D_r(m)$ and $D_{2r}(m)$ are both isolating. The property we exploit is that if D and D' are both well-isolating with non-empty intersection, then they share a common root in $D \cap D'$. Our algorithm produces well-isolated disks:

Simplified Ceval(B_0, f):
Input: Box B_0, and polynomial $f(z)$ with only simple roots.
Output: List $\mathcal{L}$ of disjoint well-isolating disks, each centered in B_0.

$Q \leftarrow \{B_0\}$. $\mathcal{L} \leftarrow \emptyset$.
While Q is non-empty:
  Remove B from Q. Let $m = m(B)$ and $r = 3w(B)/4$.
1. If $T_1(m,r)$ holds, discard B.
2. Else if $T'_{\sqrt{2}}(m, 4nr)$ holds:
2.1 If $D_{2nr}(m)$ intersects any disk D' in $\mathcal{L}$,
2.2 replace D' by the smaller of $D_{2nr}(m)$ and D'.
2.3 Else insert $D_{2nr}(m)$ into $\mathcal{L}$.
3. Else
  Split B into four children and insert them into Q.

Correctness of our algorithm is based on three claims:

Theorem 3 (Correctness).
(i) The algorithm halts: indeed, no box of width less than $\sigma(f)/(12n^3)$ is subdivided.
(ii) $\mathcal{L}$ is a list of well-isolating disks, each centered in B_0.
(iii) Every root of $f(z)$ in B_0 is isolated by some disk in $\mathcal{L}$.

Proof. Claim (i) is true because Lemma **??**(i) implies that the tests in Steps 1 or 2 must pass when $r \leq \sigma(f)/(12n^3)$ and r is an upper bound on the radius $r(B)$ of B. To see (ii), observe that the disk $D_{2r}(m)$ is inserted into $\mathcal{L}$ in Steps 2.2 or 2.3. The m and r in Step 2.1 have the properties that $T_1(m,r)$ fails and $T'_{\sqrt{2}}(m, 4nr)$ succeeds. Then Lemma **??**(ii,iii) implies that $D_{2nr}(m)$ is well-isolating. To see (iii), observe that boxes $B \subseteq B_0$ are discarded in Steps 1 or 2.2 of the algorithm: Step 1 is justified by Lemma **??**(i) and Step 2.2 is justified because of the above-noted property of well-isolating disks. **Q.E.D.**

§10. The Eight Point Test.

Instead of relying on Lemma **??**(ii) for root confirmation, we offer another root confirmation test that is closer in spirit to the sign-change idea in (**??**). The idea is to look at the 8 compass points (N,S,E,W, NE, SE, NW, SW) on the disk $D_{4r}(m)$ as illustrated in Figure 1. These compass points divide the boundary $\partial D_{4r}(m)$ of the disk into 8 arcs $A_0, \ldots, A_7$ where $A_j := \{m + 4re^{\mathbf{i}\theta} : j\pi/4 \leq \theta < (j+1)\pi/4\}$.

We rewrite the function $f(z)$ as $f(x + \mathbf{i}y) = u(x,y) + \mathbf{i}v(x,y)$, where $z = x + \mathbf{i}y$, $\mathbf{i} = \sqrt{-1}$ and u and v are the real and imaginary part of f. So $f(x + \mathbf{i}y) = 0$ iff $u(x,y) = 0$

and $v(x,y)=0$. Since the roots are simple, the u- and v-curves intersect at right angles. We say that is an **arcwise u-crossing** at A_j if $u(m+4re^{\mathbf{i}j\pi/4})\cdot u(m+4re^{\mathbf{i}(j+1)\pi/4})<0$ or $u(m+4re^{\mathbf{i}j\pi/4})=0$.

If r is sufficiently small, then we want to detect roots in $D_r(m)$ by arcwise u- and v-crossings. More precisely: we say $D_{4r}(m)$ passes the **8-Point test** if there are exactly two arcwise u-crossings at A_j, A_k, $(j<k)$ and exactly two arcwise v-crossings at $A_{j'}, A_{k'}$ $(j'<k')$, and these **interleave** in the sense that either $0\le j<j'<k<k'<8$ or $0\le j'<j<k'<k<8$.

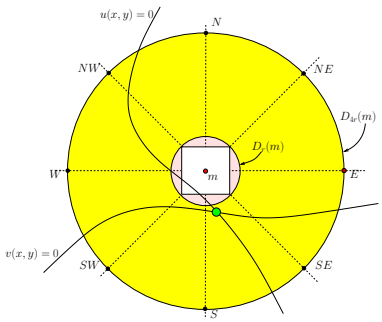

Figure 1: 8 compass points of D_{4r}

We introduce the following novel test to confirm the existence of ordinary roots.

THEOREM 4 (SUCCESS OF 8-POINT TEST). *Suppose $T_6'(m,4r)$ holds and the 8-point test is applied to $D_{4r}(m)$.*
(i) If $D_{4r}(m)$ fails the test, then $D_r(m)$ is non-isolating.
(ii) If $D_{4r}(m)$ passes the test, then $D_{4r}(m)$ is isolating.

Using the 8-point test, we devise an alternative to the simplified CEVAL. This **8-point Ceval** is described in the full version [**?**] of this paper including the proof of Theorem **??** which is non-trivial. The cardinal points (N,S,E,W) are dyadic assuming the center and radius are dyadic; however the ordinal points (NE,SE,SW,NW) are irrational. Hence for exact implementation, we show how the correctness of the 8-Point test is preserved if we use rational points that are slightly perturbed versions of ordinal points. The 8-point test has independent interest: (a) For analytic functions, we no longer have Lemma **??**(ii) for root confirmation, but some kind of 8-point test is applicable. More precisely, the tests $T_K^f(m,r)$ can be considered for arbitrary analytic function, and the same argumentation as in the case of polynomials shows the correctness of Lemma **??**(i),(iii) and Theorem **??**. (b) We can use it to "confirm" the output from pure-exclusion algorithms such as Yakoubsohn-Dedieu's in §6. The asymptotic complexity of these two forms of CEVAL for the benchmark problem are the same. This is due to the fact that there exists a corresponding result to Lemma **??** for the 8-point test.

4. COMPLEXITY ANALYSIS

In this section, we analyze the complexity of EVAL and the simplified CEVAL. For this purpose, we use the benchmark problem of isolating all roots of a square-free polynomial of degree n with L-bit integer coefficients. The initial start box for CEVAL may be assumed to be $B_0=B(-2^L(1+\mathbf{i}),2^L(1+\mathbf{i}))$. For EVAL, we can start with the interval $I_0=(-2^{-L},2^L)$. According to Cauchy's bound [**?**], B_0 contains all complex roots $z_1,\ldots,z_n\in\mathbb{C}$ of f (thus, I_0 all real roots of f). Throughout the following considerations, let $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$ denote the subdivision trees induced by CEVAL and EVAL, respectively.

§11. Cluster Analysis and Tree Size.

In (**??**), we have already seen that $\Sigma_k(m):=(\sum_i\frac{1}{|m-z_i|})^k=(\Sigma_1(m))^k$ constitutes an upper bound on $\frac{|f^{(k)}(m)|}{|f(m)|}$ for all $k\ge 1$. Furthermore, $\Sigma_1(m)<\nu$ for a $\nu>0$ implies that $\sum_{k\ge1}\left|\frac{f^{(k)}(m)}{f(m)}\right|\frac{r^k}{k!}<e^{\nu r}-1$ and, thus,

$$T_K^f(m,r)\text{ holds if }\Sigma_1(m)<\frac{1}{r}\ln\left(1+\frac{1}{K}\right). \qquad (7)$$

Now let us consider an arbitrary box B of depth h in the subdivision process, that is, B has width $w(B)=w_h:=2^{L+1-h}$. Let $r=\frac{3}{4}w(B)$ be the upper bound on the radius of B used in the CEVAL algorithm. If the midpoint $m(B)$ of B fulfills $|m(B)-z_i|>2n\cdot r$ for all $i=1,\ldots,n$, then $\Sigma_1(m(B))<\frac{1}{2r}<\frac{\ln 2}{r}$, thus $T_1(m(B),r)$ holds according to the above consideration and B is discarded. It follows that, for each root z_i, there exist at most $O(n^2)$ disjoint boxes B of the same size with $|m(B)-z_i|\le 2nr$. Hence, in total, at most $O(n^3)$ boxes are retained at each subdivision level h. From this straightforward observation we immediately derive the upper bound $O(n^3)$ on the width of $\mathcal{T}^{CE}$. For EVAL, a similar argumentation shows that $O(n^2)$ intervals are retained at each subdivision level. This consideration is based on a pretty rough estimation of $\Sigma_1(m)$ which assumes that, from a given point m, the distances to all roots z_i are nearly of the same minimal value. In order to improve the latter estimate, we introduce the concept of δ-**clusters** of roots, where δ is an arbitrary positive real value. We will show that, outside some "smaller" neighborhood of the roots of f, the sum $\Sigma_1(m)$ is sufficiently small to guarantee the success of our exclusion predicate T_1:

THEOREM 5. *For arbitrary $\delta>0$, there exist disjoint, axes-parallel, open boxes $B_1,\ldots,B_k\subset\mathbb{C}$ $(k\le n^2)$ such that:*
(i) $\mathcal{B}:=\bigcup_{i=1,\ldots,k}B_i$ covers all roots $z_1,\ldots,z_n$.
(ii) $\mathcal{B}$ covers an area of less than or equal to $4n^2\delta^2$.
(iii) For each point $m\notin\mathcal{B}$, we have $\Sigma_1(m)\le\frac{2(1+\ln\lceil n/2\rceil)}{\delta}$.

Proof. We only provide a sketch of the proof and refer the reader to Appendix **??** for a complete argumentation. The roots $z_1,\ldots,z_n$ are first projected onto the real axes. This defines a multiset (elements may appear several times) $R_{\mathtt{Re}}$ consisting of $|R_{\mathtt{Re}}|=n$ points (counted with multiplicity). The elements of $R_{\mathtt{Re}}$ are now partitioned into disjoint multisets $R_1,\ldots,R_l$ such that the following two properties are fulfilled:

(a) Each R_i is a so called δ-**cluster** which is defined as follows: The corresponding δ-**interval**

$$I_\delta(R_i)=(\mathrm{cg}(R_i)-\delta|R_i|,\mathrm{cg}(R_i)+\delta|R_i|),$$

with $\mathrm{cg}(R_i)=\frac{\sum_{x\in R_i}x}{|R_i|}$ the **center of gravity** of R_i, contains all elements of R_i. In addition, we can order the elements of R_i in way such that their distances to the right boundary of $I_\delta(R_i)$ are at least $\delta,2\delta,\ldots,|R_i|\delta$, respectively, and the same for the left boundary of $I_\delta(R_i)$.

(b) The δ-intervals $I_\delta(R_i)$ are pairwise disjoint.

The construction of a partition of $R_{\mathtt{Re}}$ with the above properties is rather simple (Appendix, Lemma **??**): We start with the trivial partition of $R_{\mathtt{Re}}$ into n δ-clusters each consisting of one element of $R_{\mathtt{Re}}$. An easy computation (Appendix A,

Lemma **??**) shows that the union of two δ-clusters for which (b) is not fulfilled is again a δ-cluster. Thus, we iteratively merge δ-clusters whose corresponding δ-intervals overlap until (b) is eventually fulfilled. It is now easy to see (Appendix A, Lemma **??**) that, for each $m \notin \bigcup_i I_\delta(R_i)$, the inequality in (iii) holds.

In a second step, we project the roots of f onto the imaginary axes defining a multiset $R_{\mathtt{Im}}$ for which we proceed in exactly the same manner as for $R_{\mathtt{Re}}$. Let $S_1, \ldots, S_{l'}$ be the corresponding partition of $R_{\mathtt{Im}}$, then the overlapping of the stripes $\mathtt{Re}(z) \in I_\delta(R_i)$ and $\mathtt{Im}(z) \in I_\delta(S_j)$ defines $k \le n^2$ boxes $B_1, \ldots, B_k$ covering an area of total size $\le 4n^2\delta^2$. Now, for each $m \notin \mathcal{B} = \bigcup_i B_i$, either $\mathtt{Re}(m) \notin \bigcup_i I_\delta(R_i)$ or $\mathtt{Im}(m) \notin \bigcup_i I_\delta(S_j)$, thus, it follows that

$$\Sigma_1(m) \le \frac{2(1+\ln\lceil n/2\rceil)}{\delta}.$$

Q.E.D.

We now apply the above theorem to

$$\delta := r \cdot \frac{(1+\ln\lceil n/2\rceil)}{\ln 2} = \frac{3w(B)(1+\ln\lceil n/2\rceil)}{4\ln 2}$$

and use (**??**). It follows that, for all m outside a union of boxes covering an area of size $w(B)^2 \cdot O((n\ln n)^2)$, we have $\Sigma_1(m) < \frac{1}{r}\ln 2$. Thus, at any level in the subdivision process, only $O((n\ln n)^2)$ boxes are retained. For Eval, we can apply the real counterpart of Theorem **??** which says that there exist $k \le n$ disjoint intervals $I_1, \ldots, I_k$ that cover the projections of all z_i onto the real axes, the total size of all intervals is $\le 2n\delta$, and $\Sigma_1(m) \le \frac{2(1+\ln\lceil n/2\rceil)}{\delta}$ for each m located outside all I_j. It follows that the width of $\mathcal{T}^{EV}$ can be bounded by $O(n\ln n)$. A more refined argument even shows that, at a subdivision level h, the width of the tree adapts itself to the number k_h of roots z_i with separation $\sigma(z_i) \le 16n^3 w_h = 2^{L+5-h}n^3$ related to the width $w_h = 2^{L+1-h}$ of the boxes at that level. We refer the reader to Appendix B, Theorem **??** and Theorem **??** for a proof.

Theorem 6. *Let h be an arbitrary subdivision level and k_h be the number of roots z_i with $\sigma(z_i) \le 2^{L+1-h}$. Then, the width of $\mathcal{T}^{CE}$ at level h is upper bounded by*

$$16k_{h-1}^2(17+\ln\lceil k_{h-1}/2\rceil) = O(k_{h-1}^2(\ln k_{h-1})^2) = O(n^2(\ln n)^2),$$

and the width of $\mathcal{T}^{EV}$ by

$$4k_{h-1}(17+\ln\lceil k_{h-1}/2\rceil) = O(k_{h-1}\ln k_{h-1}) = O(n\ln n).$$

In order to translate the above result on the treewidth into a bound on the treesize in terms of the degree n and the bitsize L, we have to derive an estimate for k_h. The main idea is to apply the generalized Davenport-Mahler bound [**?**, **?**] to the roots of f. In a first step, we partition the set $R = \{z_1, \ldots, z_n\}$ of roots into disjoint sets $R_1, \ldots, R_l$ such that $|R_{i_0}| \ge 2$ for each $i_0 = 1, \ldots, n$ and $|z_i - z_j| \le 2^{L+5-h}n^3 \cdot |R_{i_0}| \le 2^{L+5-h}n^4$ for all pairs $z_i, z_j \in R_{i_0}$: Starting with the set $R_1 := \{z_1\}$, we can iteratively add roots to R_1 that have distance $\le 2^{L+5-h}n^3$ to at least one root within R_1. When there is no further root to add, we proceed with a root z_i not contained in R_1 and construct a set R_2 from $\{z_i\}$ in the same manner, etc. (Appendix A, Lemma **??**).

In a second step, we consider a directed graph $\mathcal{G}_i$ on each R_i which connects consecutive points of R_i in ascending order of their absolute values. We define $\mathcal{G} := (R, E)$ as the union of all $\mathcal{G}_i$. Then $\mathcal{G}$ is a directed graph on R with the following properties:

1. each edge $(\alpha, \beta) \in E$ satisfies $|\alpha| \le |\beta|$,
2. $\mathcal{G}$ is acyclic, and
3. the in-degree of any node is at most 1.

Now, the generalized Davenport-Mahler bound applies:

$$\prod_{(\alpha,\beta)\in E} |\alpha - \beta| \ge \frac{1}{((n+1)^{1/2}2^L)^{n-1}} \cdot \left(\frac{\sqrt{3}}{n}\right)^{\#E} \cdot \left(\frac{1}{n}\right)^{n/2}$$

As each set R_i contains at least 2 roots, we must have $\#E \ge k_h/2$. Furthermore, for each edge $(\alpha, \beta) \in E$, we have $|\alpha - \beta| \le 16n^4 w_h = 2^{L+5-h}n^4$, thus,

$$\begin{aligned}\left(2^{L+5-h}n^4\right)^{\frac{k_h}{2}} &\ge \frac{1}{((n+1)^{1/2}2^L)^{n-1}} \cdot \left(\frac{\sqrt{3}}{n}\right)^{k_h} \cdot \left(\frac{1}{n}\right)^{n/2} \\ &> \frac{1}{(n+1)^n 2^{nL}} \cdot \left(\frac{3}{n^2}\right)^{k_h/2} > n^{-n-k_h}2^{-n(L+1)}.\end{aligned}$$

A simple computation then shows that

$$k_h < \frac{16n(L+\ln n)}{h-2L} \text{ for all } h > h_0 := \max(2L, \lceil 64\ln n + L\rceil). \tag{8}$$

In particular, the bound $O(n(L+\ln n)))$ on the depth of the subdivision tree immediately follows. Namely, if $k_{h+1} < 1$, then $k_h = 0$ and, thus, $\sigma(f) < 2^{L+4-h}n^3 < 12w_h n^3$. But this implies that, at subdivision level h, no box is further subdivided (Theorem **??**). For $h \le h_0$, we the trivial inequality $k_h \le n$ holds. Now, we can derive our bound on the tree size by summing up the number of nodes over all subdivision levels, where we use Theorem **??** and the bound (**??**) for k_h (Appendix B, Theorem **??**). A similar computation also applies to the tree induced by the Eval algorithm.

Theorem 7. *Let f be a square-free polynomial of degree n with integer coefficients of bit-size $\le L$. Then,*
(i) the subdivision tree $\mathcal{T}^{CE}$ has size $\widetilde{O}(n^2L)$.
(ii) the subdivision tree $\mathcal{T}^{EV}$ has size $\widetilde{O}(nL)$.

§12. Bit Complexity.

For the analysis of the bit complexity of Ceval, we have to consider the computational costs at a node (box B) of depth h, that is, B has width $w(B) = w_h = 2^{L+1-h}$. In order to evaluate $T_1^f(m(B), r)$ and $T_{\sqrt{2}}^{f'}(m(B), 2nr)$, where $r = \frac{3}{4}w(B)$ is an upper bound on the radius $r(B)$ of B, we compute

$$f_B(z) = f(m(B) + w(B)\cdot z)$$

and test whether $T_1^{f_B(z)}(0, 3/4)$ or $T_{\sqrt{2}}^{f'_B(z)}(0, 3n)$ holds. Notice that the latter two tests are equivalent to $T_1^f(m(B), r)$ and $T_{\sqrt{2}}^{f'}(m(B), 4nr)$, respectively. We first bound the costs for computing $f_B(z)$: For a polynomial $g(z) := \sum_{i=0}^n g_i z^i$ with binary fractions $g_i = m_i \cdot 2^{-\tau_i}$, $m_i \in \mathbb{Z}$ and $\tau_i \in \mathbb{N}_0$, as coefficients, we say that g **has bitsize** $\tau(g)$ if multiplication of g by the common denominator $2^{\max_i \tau_i}$ of all g_i leads to an integer polynomial with coefficients of at most $\tau(g)$ bits. For our starting box B_0, the polynomial $f_{B_0}(z) = f(2^{L+1}z)$ has

bitsize $O(nL)$ because of the scaling operation $z \mapsto 2^{L+1}z$. We incrementally compute $f_{B'}$ from f_B via the substitution $z \mapsto (z \pm 1 \pm \mathbf{i})/2$, where B' is one of the four children of B. Hence, the bitsize of $f_{B'}$ increases by at most n compared to the bitsize of f_B. It follows that, for a box B at subdivision level h, f_B has bitsize $\tau_B = O(n(L+h))$. $f_{B'}$ is computed from f_B by first substituting z by $z/2$ followed by a Taylor shift by 1 and then by $\mathbf{i}$, that is, $z \mapsto z \pm 1 \pm \mathbf{i}$. A Taylor shift by $\mathbf{i}$ can be realized as a Taylor shift by 1 combined with two scalings by $\mathbf{i}$, an immediate consequence of the identity $f(z+\mathbf{i}) = f(\mathbf{i}(-\mathbf{i}z+1))$. The scalings by $\mathbf{i}$ are easy. Using asymptotically fast Taylor shift [**?**], each shift by 1 requires $\widetilde{O}(n(n+\tau_B)) = O(n^2(L+h))$ bit operations.

For the polynomial evaluations needed in the predicates $T_1^{f_B(z)}(0, 3/4)$ and $T_{\sqrt{2}}^{f'_B(z)}(0, 3n)$, we have to compute the value of a polynomial of bitsize $O(n(L+h))$ at a point of bit size $O(1)$ and $O(\log n)$, respectively. Therefore, $\widetilde{O}(n(L+h))$ bit operations suffice and, thus, the overall number of bit operations for a box of depth h is bounded by $\widetilde{O}(n^2(L+h))$. We further remark that a completely analogous argumentation shows that, for an interval I at level h (i.e., $w(I) = 2^{L+1-h}$), Eval requires $\widetilde{O}(n^2(L+h))$ bit operations as well. Thus, the bit complexity at each node is bounded by $\widetilde{O}(n^3L)$ since $h = O(n(L + \ln n))$.

Readers familiar with the bit complexity analysis of the Descartes method will notice that the above bound matches the bound on the bit complexity at a node of depth h there. The latter result is due to the fact that also in the Descartes method, the main predicates are based on local Taylor expansions $f(a + (b-a)x)$, where $I = (a, b)$ is the actual interval processed.

Now, for Eval, the claimed bit complexity of $\tilde{O}(n^4L^2)$ follows immediately from multiplying the bound $\tilde{O}(nL)$ from Theorem **??** on the number of nodes with the bound $\widetilde{O}(n^3L)$ for the bit operations at each node. Furthermore, a simple computation (Appendix B, §17) which combines our results on the width of $\mathcal{T}^{CE}$ and the costs at each node at any subdivision level h, leads to the overall bit complexity of $\tilde{O}(n^4L^2)$ for Ceval. It seems to be worth mentioning that the larger tree size of $\mathcal{T}^{CE}$ (compared to $\mathcal{T}^{EV}$) does not effect the overall computational costs. This is due to the fact, for $\mathcal{T}^{CE}$, most of the node are at subdivision levels where the computational costs are considerably smaller than the worst case bound $\tilde{O}(n^3L)$.

Theorem 8. *For a square-free polynomial f of degree n with integer coefficients with absolute value bounded by 2^L, the algorithms* Ceval *and* Eval *isolate the complex (real) roots of f with a number of bit operations bounded by $\widetilde{O}(n^4L^2)$.*

5. CONCLUSION

This paper introduced Ceval, a new complex root isolation algorithm, continuing a line of recent work to develop exact subdivision algorithms based on the Bolzano principle. The primitives in such algorithms are based on numerical function evaluation and hence, simple to implement and extendible to analytic functions. Our 8-Point Ceval algorithm has been implemented in Kamath's thesis [**?**] using the `Core Library` [**?**], and compares favorably to Yakoubsohn's algorithm and Mpsolve [**?**, **?**].

The complexity of Ceval is theoretically competitive (up to logarithmic factors) with that of known exact practical algorithms for real root isolation. It is somewhat unexpected that algorithms based on simple primitives can match those based on more sophisticated ones based on Descartes or Sturm methods. Another surprise is that the complex case has (up to logarithmic terms) the same bit complexity as the real case.

Our complexity analysis introduces new ideas including a technique of root clusters which has proven to have other applications [**?**] as well. One open problem is to sharpen our complexity estimates (only improvements in logarithmic terms can be expected).

The Descartes method had been successfully extended to the bitstream model [**?**, **?**] in which the coefficients of the input polynomial are given by a bitstream on-demand. It has useful applications in situations where the coefficients are algebraic numbers (e.g., in cylindrical algebraic decomposition). Recent work [**?**] shows that the Ceval algorithm also extends to bitstream polynomials.

6. REFERENCES

[1] A. G. Akritas and A. Strzeboński. A comparative study of two real root isolation methods. Nonlinear Analysis:Modelling and Control, 10(4):297–304, 2005.

[2] E. Berberich, P. Emeliyanenko, and M. Sagraloff. An elimination method for solving bivariate polynomial systems: Eliminating the usual drawbacks. In Workshop on Algorithm Engineering and Experiments (ALENEX11), 2011. to appear, Jan 22, 2011. San Francisco, California.

[3] D. A. Bini. Numerical computation of polynomial zeroes by means of Aberth's method. Numerical Algorithms, 13:179–200, 1996.

[4] D. A. Bini and G. Fiorentino. Numerical Computation of Polynomial Roots Using MPSolve Version 2.2. Dipartimento di Matematica, Universitaá di Pisa, Via Bonarroti 2, 56127 Pisa, January 2000. Manual for the Mpsolve package. Available at `ftp://ftp.dm.unipi.it/pub/mpsolve/MPSolve-2.2.tgz`.

[5] M. Burr, S. Choi, B. Galehouse, and C. Yap. Complete subdivision algorithms, II: Isotopic meshing of singular algebraic curves. In Proc. Int'l Symp. Symbolic and Algebraic Computation (ISSAC'08), pages 87–94, 2008. Hagenberg, Austria. Jul 20-23, 2008. Accepted for Special Issue of ISSAC 2008 in JSC.

[6] M. Burr and F. Krahmer. Sqfreeeval: An optimal real-root isolation algorithm, Nov. 2010.

[7] M. Burr, F. Krahmer, and C. Yap. Continuous amortization: A non-probabilistic adaptive analysis technique. Electronic Colloquium on Computational Complexity (ECCC), TR09(136), December 2009.

[8] M. Burr, V. Sharma, and C. Yap. Evaluation-based root isolation, Feb. 2009. In preparation.

[9] G. E. Collins and A. G. Akritas. Polynomial real root isolation using Descartes' rule of signs. In R. D. Jenks, editor, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, pages 272–275. ACM Press, 1976.

[10] G. E. Collins, J. R. Johnson, and W. Krandick. Interval arithmetic in cylindrical algebraic decomposition. J. Symbolic Computation, 34:145–157, 2002.

[11] G. E. Collins and R. Loos. Real zeros of polynomials.

In B. Buchberger, G. E. Collins, and R. Loos, editors, Computer Algebra, pages 83–94. Springer-Verlag, 2nd edition, 1983.

[12] J. H. Davenport. Computer algebra for cylindrical algebraic decomposition. Tech. Rep., The Royal Inst. of Technology, Dept. of Numerical Analysis and Computing Science, S-100 44, Stockholm, Sweden, 1985. Reprinted as Tech. Report 88-10 , School of Mathematical Sci., U. of Bath, Claverton Down, Bath BA2 7AY, England. URL http://www.bath.ac.uk/ masjhd/TRITA.pdf.

[13] J.-P. Dedieu and J.-C. Yakoubsohn. Localization of an algebraic hypersurface by the exclusion algorithm. Applicable Algbebra in Engineering, Communication and Computing, 2:239–256, 1992.

[14] Z. Du, V. Sharma, and C. Yap. Amortized bounds for root isolation via Sturm sequences. In D. Wang and L. Zhi, editors, Symbolic-Numeric Computation, Trends in Mathematics, pages 113–130. Birkhäuser Verlag AG, Basel, 2007. Proc. Int'l Workshop on Symbolic-Numeric Computation, Xi'an, China, Jul 19–21, 2005.

[15] A. Eigenwillig. Real Root Isolation for Exact and Approximate Polynomials Using DescartesâĂŹ Rule of Signs. Ph.D. thesis, University of Saarland, Saarbruecken, Germany, May 2008.

[16] A. Eigenwillig, L. Kettner, W. Krandick, K. Mehlhorn, S. Schmitt, and N. Wolpert. A Descartes algorithm for polynomials with bit stream coefficients. In 8th Int'l Workshop on Comp.Algebra in Sci.Computing (CASC 2005), pages 138–149. Springer, 2005. LNCS 3718.

[17] A. Eigenwillig, V. Sharma, and C. Yap. Almost tight complexity bounds for the Descartes method. In Proc. Int'l Symp. Symbolic and Algebraic Computation (ISSAC'06), pages 71–78, 2006. Genova, Italy. Jul 9-12, 2006.

[18] J. Gerhard. Modular algorithms in symbolic summation and symbolic integration. LNCS, Springer, 3218, 2004.

[19] J. Johnson. Algorithms for polynomial real root isolation. In B. Caviness and J. Johnson, editors, Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts and monographs in Symbolic Computation, pages 269–299. Springer, 1998.

[20] N. Kamath. Subdivision algorithms for complex root isolation: Empirical comparisons. Master's thesis, Oxford University, Oxford Computing Laboratory, Aug. 2010.

[21] W. Krandick and G. E. Collins. An efficient algorithm for infallible polynomial complex root isolation. In ISSAC 97, pages 189–194, 1992.

[22] W. Krandick and K. Mehlhorn. New bounds for the Descartes method. J. Symbolic Computation, 41(1):49–66, 2006.

[23] T. Lickteig and M.-F. Roy. Sylvester-Habicht sequences and fast Cauchy index computation. J. Symbolic Computation, 31:315–341, 2001.

[24] L. Lin and C. Yap. Adaptive isotopic approximation of nonsingular curves: the parametrizability and non-local isotopy approach. In Proc. 25th ACM Symp. on Comp. Geometry, pages 351–360, June 2009. Aarhus, Denmark, Jun 8-10, 2009. To Appear, Special Issue of SoCG 2009 in DCG.

[25] J. McNamee. A bibliography on roots of polynomials. J. Comput. Appl. Math., 47:391–394, 1993. Available online at http://www.elsevier.com/homepage/sac/cam/mcnamee.

[26] K. Mehlhorn and M. Sagraloff. Isolating real roots of real polynomials. In ISSAC 09, 2009.

[27] D. P. Mitchell. Robust ray intersection with interval arithmetic. In Graphics Interface'90, pages 68–74, 1990.

[28] R. E. Moore. Interval Analysis. Prentice Hall, Englewood Cliffs, NJ, 1966.

[29] B. Mourrain, F. Rouillier, and M.-F. Roy. The Bernstein basis and real root isolation. In J. E. Goodman, J. Pach, and E. Welzl, editors, Combinatorial and Computational Geometry, number 52 in MSRI Publications, pages 459–478. Cambridge University Press, 2005.

[30] B. Mourrain, M. N. Vrahatis, and J. C. Yakoubsohn. On the complexity of isolating real roots and computing with certainty the topological degree. J. Complexity, 18:612–640, 2002.

[31] V. Y. Pan. Sequential and parallel complexity of approximate evaluation of polynomial zeros. Comput. Math. Applic., 14(8):591–622, 1987.

[32] V. Y. Pan. New techniques for approximating complex polynomial zeros. Proc. 5th ACM-SIAM Symp. on Discrete Algorithms (SODA94), pages 260–270, 1994.

[33] V. Y. Pan. Optimal (up to polylog factors) sequential and parallel algorithms for approximating complex polynomial zeros. Proc. 27th STOC, pages 741–750, 1995.

[34] V. Y. Pan. On approximating polynomial zeros: Modified quadtree (weyl's) construction and improved newton's iteration. Research report 2894, INRIA, Sophia-Antipolis, 1996.

[35] V. Y. Pan. Solving a polynomial equation: some history and recent progress. SIAM Review, 39(2):187–220, 1997.

[36] J. R. Pinkert. An exact method for finding the roots of a complex polynomial. ACM Trans. on Math. Software, 2:351–363, 1976.

[37] S. Plantinga and G. Vegter. Isotopic approximation of implicit curves and surfaces. In Proc. Eurographics Symposium on Geometry Processing, pages 245–254, New York, 2004. ACM Press.

[38] D. Reischert. Asymptotically fast computation of subresultants. In ISSAC 97, pages 233–240, 1997. Maui, Hawaii.

[39] F. Rouillier and P. Zimmermann. Efficient isolation of [a] polynomial's real roots. J. Computational and Applied Mathematics, 162:33–50, 2004.

[40] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity, 1982. Manuscript , Department of Mathematics, University of Tübingen. Updated 2004.

[41] V. Sharma. Complexity of real root isolation using continued fractions. Theor. Computer Science, 409(2), 2008. Also: proceedings ISSAC'07.

[42] S. Smale. The fundamental theorem of algebra and complexity theory. Bulletin (N.S.) of the AMS,

4(1):1–36, 1981.

[43] J. M. Snyder. Interval analysis for computer graphics. SIGGRAPH Comput.Graphics, 26(2):121–130, 1992.

[44] G. Taubin. Distance approximations for rasterizing implicit curves. ACM Transactions on Graphics, 13(1):3–42, 1994.

[45] G. Taubin. Rasterizing algebraic curves and surfaces. IEEE Computer Graphics and Applications, 14(2):14–23, 1994.

[46] J. von zur Gathen and J. Gerhard. Fast algorithms for Taylor shifts and certain difference equations. In Proc. 1997 International Symposium on Symbolic and Algebraic Computation (ISSAC 1997), pages 40–47. ACM, 1997.

[47] H. S. Wilf. A global bisection algorithm for computing the zeros of polynomials in the complex plane. J. ACM, 25(3):415–420, 1978.

[48] J.-C. Yakoubsohn. Numerical analysis of a bisection-exclusion method to find zeros of univariate analytic functions. J. of Complexity, 21:652–690, 2005.

[49] C. K. Yap. Fundamental Problems of Algorithmic Algebra. Oxford University Press, 2000.

[50] C. K. Yap. Theory of real computation according to EGC. In P. Hertling, C. Hoffmann, W. Luther, and N.Revol, editors, Reliable Implementation of Real Number Algorithms: Theory and Practice, number 5045 in Lecture Notes in Computer Science, pages 193–237. Springer, 2008.

APPENDIX

A. THE CLUSTERING APPROACH

Let $\delta > 0$, and suppose $R \subseteq \mathbb{R}$ is a non-empty multiset of real numbers. Multiset means that elements of R may appear several times, and its size is denoted $|R|$, with multiplicity counted. Then its **center of gravity** is

$$\mathrm{cg}(R) := \left(\sum_{x\in R} x\right)/|R|,$$

and δ**-interval** is

$$I_\delta(R) := (\mathrm{cg}(R) \pm |R|\delta).$$

Thus, the width of the $I_\delta(R)$ is $2|R|\delta$.

A **ranking** of R is a one-one onto function $r : R \to \{1, 2, \ldots, |R|\}$. We call R a **semi δ-cluster** if there is a ranking r of R such that, for all $x \in R$,

$$(\mathrm{cg}(R) + |R|\delta) - x \geq r(x)\delta. \tag{9}$$

In simpler words, we can order the elements of a semi δ-cluster R in a way such that their distances to the right endpoint of $I_\delta(R)$ are at least $\delta, 2\delta, 3\delta, \ldots, |R|\delta$.

In our context, it will turn out useful to guarantee the same property for the left endpoint $\mathrm{cg}(R) - |R|\delta$ of $I_\delta(R)$ as well. Hence, we introduce the following definition: R is a **δ-cluster** if both R and $-R = \{-x : x \in R\}$ are semi δ-clusters. We are mainly interested in clusters, but it is easier to prove properties for semi clusters and to extend them to clusters by symmetry.

Consider the following examples:

$$\begin{aligned} R_0 &= \{x_1, \ldots, x_n\}, \text{where } x_1 = x_i \text{ for all } i;\\ R_1 &= \{-3, 1, 2\};\\ R_2 &= \{x_1, x_2\};\\ R_3 &= \{-x, 0, x\}. \end{aligned}$$

R_0 is a δ-cluster for any $\delta > 0$. R_1 is a semi 1-cluster with $\mathrm{cg}(R_1) = 0$, but it is not a 1-cluster. R_2 is a δ-cluster iff $|x_0 - x_1| \leq 2\delta$. R_3 is a δ-cluster iff $|x| \leq 2\delta$.

§13. Properties of Clusters.

The following property of δ-clusters is immediate:

LEMMA 9. *If R is a δ-cluster, then R is contained in $I_\delta(R)$. In fact, a stronger containment is true:*

$$R \subseteq [cg(R) \pm (|R| - 1)\delta].$$

We now generalize our definition of a δ-cluster. Let us consider a partition $R = \bigcup_{i=1}^k R_i$ of a multiset R. We then call $\mathcal{P} = \{R_1, \ldots, R_k\}$ a δ**-partition of** R if each R_i is a δ-cluster and the intervals $I_\delta(R_i)$ are pairwise disjoint. Clearly, if R is a δ-cluster, the trivial partition $\mathcal{P} = \{R\}$ is a δ-partition of R. We further denote $I_\delta(\mathcal{P}) := \bigcup_{i=1}^k I_\delta(R_i)$.

The following useful property of δ-partitions now follows from an easy consideration:

LEMMA 10. *If R is a δ-cluster and $m \notin I_\delta(R)$, then*

$$\sum_{x\in R} \frac{1}{|m-x|} \leq \frac{1 + \ln|R|}{\delta}.$$

If $\mathcal{P} = \bigcup_{i=1,\ldots,k} R_i$ is a δ-partition of a multiset R, and $m \notin I_\delta(\mathcal{P})$ then

$$\sum_{x\in R} \frac{1}{|m-x|} \leq \frac{2(1 + \ln\lceil|R|/2\rceil)}{\delta}.$$

Proof. Since $m \notin I_\delta(R)$, we either have $m > x$ for all $x \in R$ or $m < x$ for all $x \in R$. Let us consider the first case. If r is the ranking function that witnesses R as a semi δ-cluster, then we have

$$\sum_{x\in R} \frac{1}{|m-x|} \leq \sum_{i=1}^{|R|} \frac{1}{|m - r^{-1}(i)|} \leq \sum_{i=1}^{|R|} \frac{1}{i\delta} \leq \frac{1 + \ln|R|}{\delta}.$$

The second case, that is, $m < x$ for all $x \in R$, is then treated in completely analogous manner, where we use that $-R$ is a semi δ-cluster too.

For the proof of the second claim we assume, w.l.o.g., that the clusters are ordered in way such that $x < y$ for all $i < j$ and $x \in R_i$, $y \in R_j$. Let $\mathcal{R}_0 := \bigcup_{i=1}^{k_0} R_i$ be the union of all points $x \in R$ with $x < m$ and $\mathcal{R}_1 := \bigcup_{i=k_0+1}^{k} R_i$. Notice that m separates clusters as it is not contained in any $I_\delta(R_i)$. For $i \leq k_0$ and $x \in R_i$, we define the ranking function $r : \mathcal{R}_0 \to \{1, \ldots, |\mathcal{R}_0|\}$ by $r(x) := \sum_{j=i+1}^{k_0} |R_i| + r_i(x)$ where r_i denotes the ranking function that witnesses R_i as a semi δ-cluster. It follows that $|m - x| \geq r(x)\delta \geq j\delta$ if x is the j-th element of $\mathcal{R}_0$ left to m. Hence, we get

$$\sum_{x\in\mathcal{R}_0} \frac{1}{|m-x|} \leq \sum_{j=1}^{|\mathcal{R}_0|} \frac{1}{|m - r^{-1}(l)|} \leq \sum_{j=1}^{|\mathcal{R}_0|} \frac{1}{j\delta} \leq \frac{1 + \ln|\mathcal{R}_0|}{\delta}.$$

In an analogous manner, we also show that $\sum_{x\in\mathcal{R}_1} |m - x|^{-1} \leq (1 + \ln|\mathcal{R}_1|)/\delta$ and, thus,

$$\sum_{x\in R} \frac{1}{|m-x|} \leq \frac{2 + \ln|\mathcal{R}_0| + \ln|\mathcal{R}_1|}{\delta} \leq \frac{2(1 + \ln\lceil|R|/2\rceil)}{\delta}.$$

Q.E.D.

The following shows that we can merge δ-clusters to a δ-cluster again if the corresponding δ-intervals do not overlap.

LEMMA 11. *Let R, R' be semi δ-clusters of sizes n and n', respectively. If $|cg(R) - cg(R')| \leq (n + n')\delta$, then*
(i) $\max\{cg(R) + n\delta, cg(R') + n'\delta\} \leq cg(R \cup R') + (n + n')\delta$
(ii) $R \cup R'$ is a semi δ-cluster.
The union of δ-clusters R, R' is again a δ-cluster if

$$I_\delta(R) \cap I_\delta(R') \neq \emptyset.$$

Proof. W.l.o.g., let $\mathrm{cg}(R') \leq \mathrm{cg}(R \cup R') \leq \mathrm{cg}(R)$, as in Figure **??**.
(i) Clearly, $\mathrm{cg}(R') + n'\delta \leq \mathrm{cg}(R \cup R') + (n + n')\delta$. Furthermore, we have

$$\begin{aligned} (n + n')\mathrm{cg}(R \cup R') &= n\mathrm{cg}(R) + n'\mathrm{cg}(R')\\ &\geq n\mathrm{cg}(R) + n'(\mathrm{cg}(R) - (n + n')\delta)\\ &= (n + n')(\mathrm{cg}(R) - n'\delta) \end{aligned}$$

and, thus, $\mathrm{cg}(R \cup R') \geq \mathrm{cg}(R) - n'\delta$ which shows the second part of (i).
(ii) Let $r : R \to \{1, \ldots, n\}$ and $r' : R' \to \{1, \ldots, n'\}$ be the ranking functions that witness R and R' as the semi

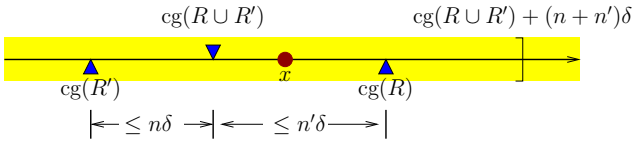

Figure 2: The union of two δ-clusters R, R'

δ-clusters, respectively. We choose a new ranking function $\overline{r} : R \cup R' \to \{1, \ldots, n+n'\}$, where

$$\overline{r}(x) = \begin{cases} r(x) & \text{if } x \in R, \\ n + r'(x) & \text{if } x \in R'. \end{cases}$$

If $x \in R$, then we have

$$\mathrm{cg}(R \cup R') + (n+n')\delta - x \geq \mathrm{cg}(R) + n\delta - x \geq r(x)\delta = \overline{r}(x)\delta$$

as desired. If $x \in R'$, then we also have

$$\begin{aligned} \mathrm{cg}(R \cup R') + (n+n')\delta - x &\geq (\mathrm{cg}(R') + n'\delta - x) + n\delta \\ &\geq r'(x)\delta + n\delta = \overline{r}(x)\delta. \end{aligned}$$

From the definition of $I_\delta(R)$ and $I_\delta(R')$ it is immediate that $|\mathrm{cg}(R) - \mathrm{cg}(R')| \leq (|R| + |R'|)\delta$ if $I_\delta(R) \cap I_\delta(R') \neq \emptyset$ and, thus, $R \cup R'$ is a semi δ-cluster according to (ii). A completely symmetric argument then also shows that $-(R \cup R')$ is a semi δ-cluster as well. Hence, the claim follows. **Q.E.D.**

LEMMA 12. *Let R be a multiset that contains n points $x_1, \ldots, x_n \in \mathbb{R}$ and $\delta > 0$ an arbitrary real value. Then, there exists a δ-partition $\mathcal{P}$ of R and for each $m \notin I_\delta(\mathcal{P})$ it holds that*

$$\sum_{i=1}^{n} \frac{1}{|p - x_i|} \leq \frac{2(1 + \ln \lceil n/2 \rceil)}{\delta}.$$

Proof. Let $\mathcal{P} = \{R_1, \ldots, R_k\}$ be a partition of R, where each R_i is a δ-cluster. We will keep transforming $\mathcal{P}$ until it becomes a δ-partition. We start with $\mathcal{P} = \{\{x_1\}, \ldots, \{x_n\}\}$. In each step, we consider clusters $R, R' \subset \mathcal{P}$ with $I_\delta(R) \cap I_\delta(R') \neq \emptyset$. Their union $R \cup R'$ is again a δ-cluster due to Lemma **??**. We remove R and R' from $\mathcal{P}$ and insert $R \cup R'$. When all the intervals $I_\delta(R)$ for $R \in \mathcal{P}$ are pairwise disjoint, we have the desired δ-partition. The statement about the bound on the sum $\sum_{i=1}^{k} \frac{1}{|m - x_i|}$ follows directly from Lemma **??**. **Q.E.D.**

§14. Complex Clusters.

We now extend the concept of δ-clusters to a multiset $R = \{z_1, \ldots, z_n\}$ of complex numbers. Let $\mathtt{Re}[R]$ and $\mathtt{Im}[R]$ denote the multiset of the real and imaginary part of elements in R.

Due to Lemma **??** there exists a δ-partition $\{R_1, \ldots, R_{k_{\mathtt{Re}}}\}$ of $\mathtt{Re}[R]$. Similarly, let $\{\widetilde{R}_1, \ldots, \widetilde{R}_{k_{\mathtt{Im}}}\}$ denote a δ-partition of $\mathtt{Im}[R]$. Each interval $I_\delta(R_i)$ ($I_\delta(\widetilde{R}_j)$) defines a vertical (horizontal) stripe (see Figure **??**) in the complex plane, containing all points $z \in \mathbb{C}$ with $\mathtt{Re}(z) \in I_\delta(R_i)$ ($\mathtt{Im}(z) \in I_\delta(\widetilde{R}_j)$). Their overlapping consists of $k := k_{\mathtt{Re}} \cdot k_{\mathtt{Im}}$ disjoint boxes which we denote by $B_1, \ldots, B_k$. For any point $p \notin \bigcup_{i=1}^{k} B_i$, either $\mathtt{Re}(p) \notin \bigcup_{i=1}^{k_{\mathtt{Re}}} I_\delta(R_i)$ or $\mathtt{Im}(p) \notin \bigcup_{i=1}^{k_{\mathtt{Im}}} I_\delta(\widetilde{R}_i)$, hence from Lemma **??** we get $\sum_{i=1}^{n} \frac{1}{|p - z_i|} \leq \frac{2(1+\ln\lceil n/2 \rceil)}{\delta}$. Furthermore, let $\epsilon \geq 0$ be an arbitrary positive value and B_i^ϵ the box that is obtained by enlarging B_i by ϵ in each direction. If $\mathcal{B} := \bigcup_{i=1,\ldots,k} B_i$, then the total area covered by the union $\mathcal{B}^\epsilon := \bigcup_{B \in \mathcal{B}} B^\epsilon$ of all these enlarged boxes is upper bounded by

$$\begin{aligned} &\sum_{i,j} (w(I_\delta(R_i)) + 2\epsilon)(w(I_\delta(\widetilde{R}_j)) + 2\epsilon) \\ &= \sum_{i} (w(I_\delta(R_i)) + 2\epsilon) \cdot \sum_{j} (w(I_\delta(\widetilde{R}_j)) + 2\epsilon) \\ &\leq (2n\delta + 2n\epsilon)^2 = 4n^2(\delta + \epsilon)^2. \end{aligned}$$

where the sum is taken over all $i = 1, \ldots, k_{\mathtt{Re}} \leq n$, $j = 1, \ldots, k_{\mathtt{Im}} \leq n$. We fix this result.

THEOREM 13. *Let R be a multiset consisting of n points $z_1, \ldots, z_n$ in the complex space and $\epsilon \geq 0$, $\delta > 0$ arbitrary real values. Then there exist disjoint axes-parallel boxes $B_1, \ldots, B_k \subset \mathbb{C}$, $k \leq n^2$, with the following properties:*
(i) The union $\mathcal{B} := \bigcup_{i=1,\ldots,k} B_i$ of all boxes covers R.
(ii) $\mathcal{B}^\epsilon = \bigcup_{i=1,\ldots,k} B_i^\epsilon$ covers an area of less than or equal to $4n^2(\delta + \epsilon)^2$.
(iii) For each point $m \notin \mathcal{B}$ we have $\sum_{i=1}^{n} \frac{1}{|m - z_i|} \leq \frac{2(1+\ln\lceil n/2 \rceil)}{\delta}$.

We conclude this section with another useful lemma. Again we consider a multiset R, consisting of n complex points $z_1, \ldots, z_n$. We are interested in a partition of R into multisets that consist of nearby points, only. Let $\sigma(z_i) := \min_{j \neq i} |z_i - z_j|$ denote the distance of z_i to its nearest point in R. Furthermore, for an arbitrary $\delta > 0$, we consider the multiset R_δ that contains exactly those z_i with $\sigma(z_i) \leq \delta$.

LEMMA 14. *There exists a partition of R_δ into disjoint multisets $R_1, \ldots, R_k$ such that $|R_{i_0}| \geq 2$ for each $i_0 \in \{1, \ldots, k\}$ and $|z_i - z_j| \leq |R_\delta|\delta$ for all $z_i, z_j \in R_{i_0}$.*

Proof. Wlog we can assume that R_δ consists of the points $z_1, \ldots, z_l$ with an $l \leq n$. We start with z_1 and define $R_1 := \{z_1\}$. We further put all points z_i in R_1 that satisfy $|z_i - z_1| \leq \delta$. Then we proceed with each point in R_1 in the same way. If no further point can be added to R_1 we consider the set $R_\delta \backslash R_1$ of the remaining points and treat it in exactly the same manner. Finally, we end up with a partition $R_1, \ldots, R_k$ of R such that for any two points in any R_{i_0}, their distance is less than or equal to $(|R_{i_0}| - 1)\delta \leq |R_\delta|\delta$. Furthermore, each of the multisets R_i must contain at least two points as $\sigma(z_i) \leq \delta$ for all $i = 1, \ldots, l$. **Q.E.D.**

B. COMPLEXITY ANALYSIS

In addition to our previously fixed notations, we denote by $z'_1, \ldots, z'_{n-1}$ the roots of the derivative f' of f. We further assume that the roots $z_1, \ldots, z_n$ of f are ordered with

respect to their separations, that is, $\sigma(z_1) \le \ldots \le \sigma(z_n)$. Since we start subdividing an initial box B_0 (interval I_0) of width $w_0 := w(B_0) = 2^{L+1}$, all boxes (intervals) B at a certain subdivision level h have width $w(B) = w_h := 2^{L+1-h}$ and radius bounded by $r(B) < r_h := \frac{3}{4}w_h$. We further denote k_h *the largest index* k such that

$$\sigma(z_k) \le 16n^3 w_h = 2^{L+5-h}n^3.$$

§15. Width of $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$.

THEOREM 15. *(Width of $\mathcal{T}^{CE}$) For each subdivision level h, the width w_h of $\mathcal{T}^{CE}$ is bounded by*

$$16k_{h-1}^2(17+16\ln\lceil k_{h-1}/2\rceil)^2 = O(k_{h-1}^2(\ln k_{h-1})^2) = O(n^2(\ln n)^2).$$

PROOF. For a fixed h, consider the set $R = \{z_1, \ldots, z_{k_h}\}$ of roots with $\sigma(z_i) \le 16n^3 w_h$, and let

$$\delta := 16(1 + \ln\lceil k_h/2\rceil)w_h.$$

Theorem **??** applied to R, δ and $\epsilon := w_h$ ensures the existence of disjoint open axes-parallel boxes $B_1, \ldots, B_k$, $k \le k_h^2$, such that their union $\tilde{\mathcal{B}} := \bigcup_{i=1}^k B_i$ has the following properties:

(a) $\tilde{\mathcal{B}}$ contains all roots $z_1, \ldots, z_{k_h}$, and each B_i contains at least one root of R.

(b) $\tilde{\mathcal{B}}^{w_h}$ covers an area of at most $4k_h^2(w_h+\delta)^2$, where $\tilde{\mathcal{B}}^{w_h}$ denotes the union of all boxes $B_i \in \tilde{\mathcal{B}}$, each enlarged by w_h in each direction as in §14.

(c) For an arbitrary $m \notin \tilde{\mathcal{B}}$, we have $\sum_{i=1}^{k_h} \frac{1}{|m-z_i|} \le \frac{1}{8w_h}$.

Let $\partial\mathcal{B} := \bigcup_{i=1,\ldots,k} \partial B_i$ be the union of the boundaries of all boxes in $\mathcal{B}$. Then, for any $m \in \partial\mathcal{B}$, the inequality in (c) holds as well because the boxes B_i (for all i) are disjoint and, thus, $m \notin \tilde{B}$. For the remaining roots $z_{k_h+1}, \ldots, z_n$, we consider discs $D_i := D_{8n^2w_h}(z_i)$, $i = k_h+1, \ldots, n$, of radius $r_i := 8n^2w_h$, centered at z_i. We denote the union of these discs by $\mathcal{D} := \bigcup_{i=k(\delta_h)+1}^n D_i$.

In the first step, we want to show that for any $m \notin \mathcal{B}$, either $T_1(m, r_h) = T_1(m, 3w_h/4)$ or $T'_{\sqrt{2}}(m, 4nr_h)$ holds. We distinguish two cases:

- $m \in \mathcal{D}$: Then there exists an $i_0 \in \{k_h+1, \ldots, n\}$ with $m \in D_{i_0}$. By definition of k_h, we have $\sigma(z_{i_0}) > 16n^3w_h$. From [**?**, **?**] we know that the distance from z_{i_0} to any root $z'_1, \ldots, z'_{n-1}$ of f' is larger than $\sigma(z_{i_0})/n > 16n^2w_h = 2r_{i_0}$. Hence, the distance from m to any z'_i is larger than $8n^2w_h$ and, thus,

$$\sum_{i=1}^{n-1} \frac{1}{|m-z'_i|} < \frac{1}{8nw_h} = \frac{3}{32nr_h} < \frac{1}{4nr_h}\ln(1+\frac{1}{\sqrt{2}}).$$

  Now from (**??**), it follows that $T'_{\sqrt{2}}(m, 4nr_h)$ succeeds. Thus, any box B with center $m = m(B)$ and width $w(B) \le w_h$ is terminal.

- $m \notin \mathcal{B} \cup \mathcal{D}$: On $\mathbb{C}\setminus(\mathcal{B}\cup\mathcal{D})$, each quotient $\frac{f^{(k)}}{f}$, $k = 1, \ldots, n$, defines a holomorphic function, and, for each of these functions, we have $\lim_{z\to\infty} \frac{f^{(k)}}{f}(z) = 0$. According to the maximum principle, their maxima are either taken on the boundary of $\mathcal{B}$ or on the boundary $\partial\mathcal{D}$ of $\mathcal{D}$. Hence, in order to bound $\left|\frac{f^{(k)}}{f}(m)\right|$, we can restrict to these cases. If $m \in \partial D_i$ for one of the discs D_i (say D_{i_0}), then m is at least $r_{i_0} = 8n^2w_h$ away from z_{i_0} and at least $\sigma(z_{i_0}) - r_{i_0} \ge 8n^3w_h$ away from all other roots of f. It follows that

$$\left|\frac{f^{(k)}}{f}(m)\right| \le \left(\sum_{i=1}^n \frac{1}{8n^2w_h}\right)^k = \left(\frac{1}{8nw_h}\right)^k < \left(\frac{1}{r_h}\ln 2\right)^k.$$

  It remains to discuss the case where m is on the boundary of one of the boxes. Then, the inequality in (c) holds and, in addition, $|m - z_i| \ge 8n^2w_h$ for all $i = k_h+1, \ldots, n$. It follows that

$$\left|\frac{f^{(k)}}{f}(m)\right| \le \left(\sum\nolimits_{i=1}^{k_h} \frac{1}{|z_i-m|} + \sum\nolimits_{i=k_h+1}^{n} \frac{1}{|z_i-m|}\right)^k$$
$$\le \left(\frac{1}{8w_h} + (n-k_h)\cdot\frac{1}{8n^2w_h}\right)^k < \left(\frac{1}{r_h}\ln 2\right)^k.$$

  Hence, in both situations, we have $\left|\frac{f^{(k)}}{f}(m)\right| < \left(\frac{1}{r_h}\ln 2\right)^k$, and, thus, it follows that $\sum_{k=1}^n \left|\frac{f^{(k)}(m)}{f(m)}\right| \frac{r_h^k}{k!} < e^{\ln 2} - 1 = 1$. The latter inequality implies the success of $T_1(m, r_h)$, thus, any box with center m and radius smaller than r_h is terminal.

We can now easily prove our claim about the number of boxes B at subdivision level h. If the midpoint $m(B)$ of B is contained in $\mathcal{B}$, then B is completely contained in $\mathcal{B}^{w_h}$. $\mathcal{B}^{w_h}$ covers an area of at most $4k_h^2(\delta+w_h)^2$. As all boxes B at depth h are pairwise disjoint and each of them covers an area of w_h^2 it follows that at most

$$\frac{4k_h^2(\delta+w_h)^2}{w_h^2} < 4k_h^2(17+16\ln\lceil k_h/2\rceil)^2$$

boxes are retained. Since each non-terminal box has four children, the width w_h of $\mathcal{T}^{CE}$ at height h is bounded by

$$16k_{h-1}^2(17+16\ln\lceil k_{h-1}/2\rceil)^2 = O(k_{h-1}^2(\ln k_{h-1})^2) = O(n^2(\ln n)^2).$$

□

From our above considerations, it is now easy to derive a corresponding bound on the width of the tree $\mathcal{T}^{EV}$ induced by the EVAL algorithm.

THEOREM 16. *(Width of $\mathcal{T}^{EV}$) For each subdivision level h, the width w_h of $\mathcal{T}^{CE}$ is bounded by*

$$4k_{h-1}(17+16\ln\lceil k_{h-1}/2\rceil) = O(k_{h-1}\ln k_{h-1}) = O(n\ln n).$$

PROOF. We will use the same notations as in the proof of Theorem **??**. In order reuse our argument from before, we prove a slightly stronger result, namely, we show that the above bound on the width even holds when we replace the two tests $T_1(m(I), w(I)/2)$ and $T'_1(m(I), w(I)/2)$ in EVAL by the stronger tests $T_1(m(I), r_h)$ and $T'_{\sqrt{2}}(m(I), 4nr_h)$, respectively, where I is an interval of width $w(I) = w_h = 2^{L+1-h}$ and $r_h = \frac{3}{4}w_h > w(I)/2$ an upper bound on its radius.

Consider the intersection of $\mathcal{B}$ with the real axes. From the construction of $\mathcal{B}$ it follows that the intersection consists of at most k_h intervals $I_1, \ldots, I_{\tilde{k}}$, $\tilde{k} \le k_h$, and the total length of their union $\mathcal{I} := \bigcup_{l=1}^{\tilde{k}} I_l$ is bounded by $2k_h\delta = 32k_h(1+\ln\lceil k_h/2\rceil)w_h$. We have already shown that, for all

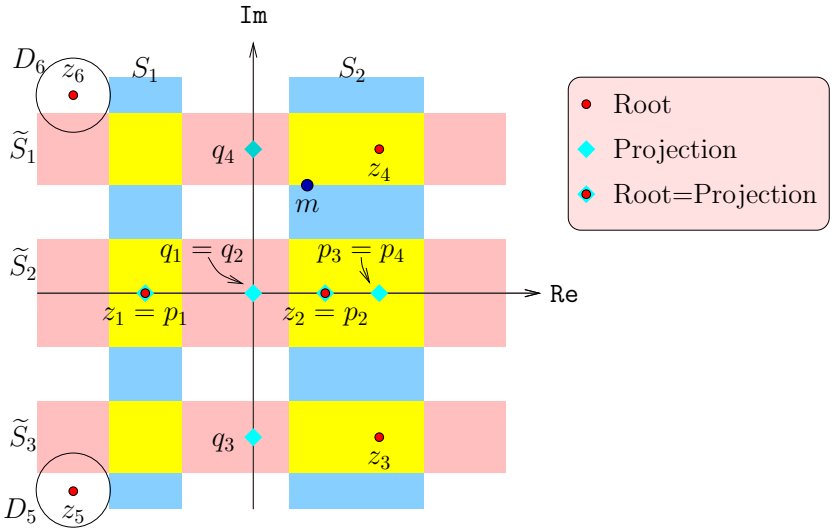

Figure 3: The roots $z_1, \ldots, z_4$ define a multiset R with $\mathtt{Re}[R] = \{p_1, \ldots, p_4\}$ and $\mathtt{Im}[R] = \{q_1, \ldots, q_4\}$ the projections of R onto the real and imaginary axes. The corresponding δ-partitions define horizontal (pink) and vertical (blue) strips $\widetilde{S}_i$ and S_j which intersect in disjoint boxes (yellow). The boxes which contains $z_1, \ldots, z_4$ are denoted by $B_1, \ldots, B_4$. Let m be a point on the boundary of one of the boxes B_i which is not contained in $D_5 \cup D_6$. Then its distance to z_5 and z_6 is larger than $8n^2 w_h$, thus $\sum_{i=1}^{6} \frac{1}{|z_i - m|} < \frac{1}{8w_h} + \frac{1}{8n^2 w_h} = \frac{\ln 2}{r_h}$.

points m outside $\mathcal{B}$, either $T_1(m, r_h)$ or $T'_{\sqrt{2}}(m, 4nr_h)$ succeeds. Hence, for any real valued m outside $\mathcal{I}$, one of the latter tests and, thus, also $T_1(m, w(I)/2)$ or $T'_1(m, w(I)/2)$ succeeds. Hence, I is terminal if its midpoint $m(I) \notin \mathcal{I}$. If $m(I) \in \mathcal{I}$, then I is completely contained in $\mathcal{I}^{w_h} := \bigcup_{l=1,\ldots,\bar{k}} I_l^{r_h}$, where $I_l^{w_h}$ is obtained by enlarging I_l by w_h at both sides. $\mathcal{I}^{w_h}$ has total length less than or equal to $2k_h(\delta + w_h)$ and each interval I at subdivision level h covers less than w_h. It follows that at most

$$\frac{2k_h(\delta + w_h)}{w_h} < 2k_h(17 + 16 \ln \lceil k_h/2 \rceil)$$

intervals are not terminal. Since each non-terminal node in $\mathcal{T}^{EV}$ has two children, the width of $\mathcal{T}^{EV}$ at depth h is bounded by $4k_{h-1}(17+16 \ln \lceil k_{h-1}/2 \rceil) = O(k_{h-1} \ln k_{h-1})$. □

§16. Size of $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$.

The preceding analysis provides bounds on the width of the trees $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$. Using the generalized Davenport-Mahler bound, we now derive a bound on their sizes in terms of n and L. Before proving the bound on tree size, we derive a preparatory bound on tree height that has independent interest:

THEOREM 17. *The height of $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$ is at most*

$$\max\{L + 64 \ln n, \lceil 16n(L + \ln n) + 2L \rceil\} \tag{10}$$

which is $O(n(L + \ln n)$. Moreover, for $h > L + 64 \ln n$,

$$k_h < \frac{16n(L + \ln n)}{h - 2L}. \tag{11}$$

Proof. We may assume that $h > L + 64 \ln n$ since otherwise the theorem is true. We first investigate in a bound on k_h. As in the proof of Theorem **??**, consider the set R consisting of those roots $z_1, \ldots, z_{k_h}$ with separation $\sigma(z_i) \le 16n^3 w_h = 2^{L+5-h} n^4$. Then, according to Lemma **??**, there exists a partition of R into disjoints sets $R_1, \ldots, R_k$ such that $|R_{i_0}| \ge 2$ for each $i_0 = 1, \ldots, k$ and $|z_i - z_j| \le 16n^3 w_h k_h \le 16n^4 w_h$ for all pairs $z_i, z_j \in R_{i_0}$. To use the generalized Davenport-Mahler bound [**?**, **?**], we consider a directed graph $\mathcal{G}_i$ on R_i which connects consecutive points of R_i in ascending order of their absolute values. We define $\mathcal{G} := (R, E)$ as the union of all $\mathcal{G}_i$. Then $\mathcal{G}$ is a directed graph on R with the following properties:

1. each edge $(\alpha, \beta) \in E$ satisfies $|\alpha| \le |\beta|$,
2. $\mathcal{G}$ is acyclic, and
3. the in-degree of any node is at most 1.

The generalized Davenport-Mahler bound implies

$$\prod_{(\alpha,\beta)\in E} |\alpha - \beta| \ge \frac{1}{((n+1)^{1/2} 2^L)^{n-1}} \cdot \left(\frac{\sqrt{3}}{n}\right)^{\#E} \cdot \left(\frac{1}{n}\right)^{n/2}$$

As each set R_i contains at least 2 roots, we must have $\#E \ge k_h/2$. Furthermore, for each edge $(\alpha, \beta) \in E$, we have $|\alpha - \beta| \le 16n^4 w_h = 2^{L+5-h} n^4$. Our assumption that $h > L + 64 \ln n$ implies $2^{L+5-h} n^4 < 1$ and, hence,

$$\begin{aligned}\left(2^{L+5-h} n^4\right)^{\frac{k_h}{2}} &\ge \frac{1}{((n+1)^{1/2} 2^L)^{n-1}} \cdot \left(\frac{\sqrt{3}}{n}\right)^{k_h} \cdot \left(\frac{1}{n}\right)^{n/2} \\ &> \frac{1}{(n+1)^n 2^{nL}} \cdot \left(\frac{3}{n^2}\right)^{k_h/2} > n^{-n-k_h} 2^{-n(L+1)}.\end{aligned}$$

Squaring and taking logarithm on both sides then leads to

$$k_h(6 \ln n + \ln 2(L + 5 - h)) > -2n((L+1) \ln 2 + \ln n).$$

For $h > 64 \ln n + L > 10 + \frac{6 \ln n}{\ln 2} + L$, the left side is negative

and thus,

$$k_h < \frac{2n((L+1)\ln 2 + \ln n)}{(h-5-L)\ln 2 - 6\ln n} < \frac{16n(L+\ln n)}{h-2L}, \qquad (12)$$

where we used that $\frac{h}{8} > 5\ln 2 + 6\ln n$. This proves the second assertion of this theorem.

Observe that by Theorems **??** and **??**, the heights of $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$ can both be bounded by the smallest h such that $k_h < 1$; as k_h is integer, this implies $k_h = 0$. But **??** shows that such a bound is given by $h = \lceil 16n(L+\ln n) + 2L\rceil$. This provides (**??**). **Q.E.D.**

THEOREM 18. *For a square-free polynomial f of degree n with integer coefficients of bitsize less than L,* CEVAL *induces a subdivision tree $\mathcal{T}^{CE}$ of size*

$$O((n\ln n)^2(L+\ln n)) = \widetilde{O}(n^2 L).$$

The subdivision tree $\mathcal{T}^{EV}$ induced by EVAL *has size*

$$O(n\ln n(L+\ln n)(\ln L + \ln n)) = \widetilde{O}(nL).$$

Proof. According to Theorem **??**, we can bound the height of $\mathcal{T}^{CE}$ and $\mathcal{T}^{EV}$ by

$$h_{\max} := \max\{\lceil 16n(L+\ln n) + 2L\rceil, L + 64\ln n\}. \qquad (13)$$

From Theorem **??**, the size of $\mathcal{T}^{CE}$ is given by

$$\left|\mathcal{T}^{CE}\right| \le \sum_{h=1}^{h_{\max}} 16k_h^2 \left(17 + 16\ln\left\lceil\frac{k_h}{2}\right\rceil\right)^2. \qquad (14)$$

To bound k_h in the summation (**??**), we consider two cases. First, let

$$h_0 := \max(2L, \lceil 64\ln n + L\rceil) \qquad (15)$$

and write each $h \ge h_0$ as $h = h' + h_0$. For $h \le 2h_0$, we use the trivial inequality $k_h \le n$, and for $h > 2h_0$, we use the bound (**??**) from Theorem **??**. We rewrite (**??**) as

$$k_h < \frac{16n(L+\ln n)}{h'}, \qquad (16)$$

where we used the fact $h - 2L = h' + h_0 - 2L \ge h'$. Thus (**??**) becomes

$$\begin{aligned}
\left|\mathcal{T}^{CE}\right| &\le 16\sum_{h=1}^{2h_0} n^2(17+16\ln n)^2 \\
&\quad + 16^3 \sum_{h'=1+h_0}^{h_{\max}-h_0} (n^2\left(\frac{L+\ln n}{h'}\right)^2 \cdot (17+16\ln n)^2) \\
&= O((n\ln n)^2)\cdot h_0 + O((n\ln n(L+\ln n))^2)\cdot \sum_{h'=1+h_0}^{h_{\max}-h_0}\left(\frac{1}{h'}\right)^2 \\
&= O((n\ln n)^2(L+\ln n)) + O((n\ln n(L+\ln n))^2)\cdot\frac{1}{h_0} \\
&= O((n\ln n)^2(L+\ln n)) \\
&= \tilde{O}(n^2 L).
\end{aligned}$$

For the size of $\mathcal{T}^{EV}$, we similarly obtain

$$\begin{aligned}
\left|\mathcal{T}^{CE}\right| &\le \sum_{h=1}^{h_{\max}} 4k_h(17+16\ln\left\lceil\frac{k_h}{2}\right\rceil) \\
&\quad \text{(by Theorem **??**)} \\
&\le 4\sum_{h=1}^{h_0} n(17+16\ln n) + 64n(17+16\ln n)\sum_{h'=1}^{h_{\max}-h_0}\frac{L+\ln n}{h'} \\
&= O(n\ln n)\cdot h_0 + O(n\ln n(L+\ln n))\sum_{h'=1}^{h_{\max}-h_0}\frac{1}{h'} \\
&= O(n\ln n)\cdot(L+\ln n) + O(n\ln n(L+\ln n))\cdot\ln h_{\max} \\
&= O(n\ln n(L+\ln n)) + O(n\ln n(L+\ln n))\cdot(\ln L + \ln n)) \\
&= O(n\ln n(L+\ln n)(\ln L+\ln n)) = \widetilde{O}(nL).
\end{aligned}$$

Q.E.D.

§17. Bit Complexity.

The bit complexity for EVAL follows directly from the above bound $\widetilde{O}(nL)$ on the tree size and our bound of $\widetilde{O}(n^3 L)$ on the costs at each node derived in §12. This proves that EVAL requires at most $\widetilde{O}(nL)\cdot\widetilde{O}(n^3 L) = \widetilde{O}(n^4 L^2)$ bit operations.

The following computation further shows that the larger tree size of $\mathcal{T}^{CE}$ does not lead to an asymptotically larger bit complexity when compared to $\mathcal{T}^{EV}$. Again, we use result from §12, where we bound the number of bit operations for a box at subdivision level h by $\widetilde{O}(nL+n^2 h)$. In particular, for all $h \le 2h_0 = \Theta(L+\ln n)$, this simplifies to $\widetilde{O}(n^2 L)$. Thus, the number of bit operations needed in CEVAL is bounded by

$$\begin{aligned}
&\sum_{h=1}^{2h_0}(n\ln n)^2\widetilde{O}(n^2 L) + \sum_{h'=1}^{h_{\max}-h_0} n^2\left(\frac{L+\ln n}{h'}\right)^2\widetilde{O}(n^2 h') \qquad (17)\\
&= \widetilde{O}(n^4 L^2) + n^4\sum_{h'=1}^{h_{\max}-h_0}\left(\frac{L+\ln n}{h'}\right)^2\widetilde{O}(h') \\
&= \widetilde{O}(n^4 L^2)\left(1 + \sum_{h'=1}^{h_{\max}-h_0}\frac{1}{h'}\right) = \widetilde{O}(n^4 L^2).
\end{aligned}$$

In the above inequality (**??**), we used that the costs at a node at level $h = h' + h_0 > 2h_0$ are bounded by $\widetilde{O}(nL + n^2(h'+h_0)) = \widetilde{O}(nL + n^2 h') = \widetilde{O}(n^2 h')$ because of $h' > h_0 > L$.