Efficient root counting for analytic functions on a disk*

Joris van der Hoeven

LIX, CNRS
École polytechnique
91128 Palaiseau Cedex
France

Email: vdhoeven@lix.polytechnique.fr
Web: http://lix.polytechnique.fr/~vdhoeven

August 2, 2011

In this note, we present a variant of an algorithm by Schönhage for counting the number of zeros of a complex polynomial in a disk. Our algorithm implements a few optimizations and also applies to more general analytic functions.

Keywords: Root counting, reliable computation, Graeffe method
A.M.S. subject classification: 68W25, 68W30, 65G20, 30B10, 42-04

1. Introduction

Many algorithms have been proposed for the reliable computation of zeros of complex polynomials [Sch82, Gou96, KvB00, Pan02], assuming multiple precision arithmetic. A slightly less ambitious problem is to count the number of zeros in a given disk; see also [Rum10, Sections 13.2 and 13.3]. In this paper, we present a variant of Schönhage's method [Sch82], based on iterated Graeffe transforms, but with a few advantages.

We present our algorithm in the setting of ball arithmetic [vdH09], which is our preferred variant of interval arithmetic [Moo66, AH83, MKC09, Rum10]. In this framework, a large part of the burden of bound computations is taken away from our shoulders and moved to the underlying arithmetic. Moreover, the algorithm naturally applies for analytic functions, which are represented by an approximating polynomial and a bound for the error. Finally, during the iterated application of Graeffe transforms, some coefficients of the polynomial become very small. Ball arithmetic allows us to move such coefficients to a global error term and reduce the degree of the polynomial, thereby speeding up the overall algorithm.

Our algorithm is presented for analytic functions whose power series expansion is given explicitly up to a given order, together with an error bound for the tail. In practice, we are often given a program which may compute the expansion (and tail bound) up to any required order. If we are expecting a k-fold multiple root, then it is a good practice to compute the expansion up to order $O(z^{\tau k})$ for some $1<\tau<2$: this is usually only a constant times more expensive than the computation of an expansion up to order $O(z^{k+1})$, but greatly improves the quality of the error bounds and the probability that our root counting algorithm will be successful.

*. This work has been supported by the ANR-09-JCJC-0098-01 MaGiX project, as well as a Digiteo 2009-36HD grant and Région Ile-de-France.

2. BALL ARITHMETIC

2.1. Basic principles

Let us briefly recall the principles behind ball arithmetic, while referring to [vdH09] for details. Given a normed vector space $\mathbb{K}$, we will denote by $\mathbb{IK}$ or $\mathcal{B}(\mathbb{K}, \mathbb{R})$ the set of closed balls with centers in $\mathbb{K}$ and radii in $\mathbb{R}^{\geqslant} = \{x \in \mathbb{R} : x \geqslant 0\}$. Given such a ball $\boldsymbol{z} \in \mathcal{B}(\mathbb{K}, \mathbb{R})$, we will denote its center by $\operatorname{cen}(\boldsymbol{z})$ and its radius by $\operatorname{rad}(\boldsymbol{z})$. Conversely, given $z \in \mathbb{K}$ and $r \in \mathbb{R}$, we will denote by $z + \mathcal{B}(r)$ the closed ball with center z and radius r.

A continuous operation $f : \mathbb{K}^r \to \mathbb{K}$ is said to *lift* into an operation $\boldsymbol{f} : \mathbb{IK}^r \to \mathbb{IK}$ on balls, which is usually also denoted by f, if the *inclusion property*

$$f(x_1, ..., x_r) \ \in \ f(\boldsymbol{x}_1, ..., \boldsymbol{x}_r) \tag{1}$$

is satisfied for any $\boldsymbol{x}_1, ..., \boldsymbol{x}_r \in \mathbb{IK}$ and $x_1 \in \boldsymbol{x}_1, ..., x_r \in \boldsymbol{x}_r$. For instance, if $\mathbb{K}$ is a Banach algebra, then we may take

$$\begin{aligned}
\boldsymbol{x} + \boldsymbol{y} &= \operatorname{cen}(\boldsymbol{x}) + \operatorname{cen}(\boldsymbol{y}) + \mathcal{B}(\operatorname{rad}(\boldsymbol{x}) + \operatorname{rad}(\boldsymbol{y})) \\
\boldsymbol{x} - \boldsymbol{y} &= \operatorname{cen}(\boldsymbol{x}) - \operatorname{cen}(\boldsymbol{y}) + \mathcal{B}(\operatorname{rad}(\boldsymbol{x}) + \operatorname{rad}(\boldsymbol{y})) \\
\boldsymbol{x}\, \boldsymbol{y} &= \operatorname{cen}(\boldsymbol{x}) \operatorname{cen}(\boldsymbol{y}) + \mathcal{B}(\operatorname{rad}(\boldsymbol{x}) \, (|\operatorname{cen}(\boldsymbol{y})| + \operatorname{rad}(\boldsymbol{y})) + |\operatorname{cen}(\boldsymbol{y})| \operatorname{rad}(\boldsymbol{x})).
\end{aligned}$$

Similar formulas can be given for division and elementary functions.

2.2. Floating point arithmetic

In concrete machine computations, numbers are usually approximated by floating point numbers with a finite precision. Let $\tilde{\mathbb{R}} = \mathbb{R}_p$ be the set of floating point numbers at a working precision of p bits. It is customary to include the infinities $\pm\infty$ in $\tilde{\mathbb{R}}$ as well. The IEEE754 standard [ANS08] specifies how to perform basic arithmetic with floating point numbers in a predictable way, by specifying a rounding mode $\mathsf{R} \in \{\downarrow, \uparrow, \updownarrow\}$ among "down", "up" and "nearest". A multiple precision implementation of this standard is available in the MPFR library [HLRZ00]. Given an operation $f : \mathbb{R}^r \to \mathbb{R}$, we will denote by $f^{\mathsf{R}} : \tilde{\mathbb{R}}^r \to \tilde{\mathbb{R}}$ its approximation using floating pointing arithmetic with rounding mode R. This notation extends to the case when $\mathbb{R}$ and $\tilde{\mathbb{R}}$ are replaced by their complexifications $\mathbb{C}$ and $\tilde{\mathbb{C}} = \tilde{\mathbb{R}}[\mathrm{i}]$.

Setting $\tilde{\mathbb{C}} = \tilde{\mathbb{R}}[\mathrm{i}]$, we will denote by $\tilde{\mathbb{C}}$ or $\mathcal{B}(\tilde{\mathbb{C}}, \tilde{\mathbb{R}})$ the set of closed balls in $\mathbb{C}$ with centers in $\tilde{\mathbb{C}}$ and radii in $\tilde{\mathbb{R}}^{\geqslant}$. In this case, we will also allow for balls with an infinite radius. A continuous operation $f : \mathbb{C}^r \to \mathbb{C}$ is again said to lift to an operation $f : \tilde{\mathbb{C}}^r \to \tilde{\mathbb{C}}$ on balls if (1) holds for any $\boldsymbol{x}_1, ..., \boldsymbol{x}_r \in \tilde{\mathbb{C}}$ and $x_1 \in \boldsymbol{x}_1, ..., x_r \in \boldsymbol{x}_r$. The formulas for the ring operations may now be adapted to

$$\begin{aligned}
\boldsymbol{x} + \boldsymbol{y} &= \operatorname{cen}(\boldsymbol{x}) +^{\updownarrow} \operatorname{cen}(\boldsymbol{y}) + \mathcal{B}(\operatorname{rad}(\boldsymbol{x}) +^{\uparrow} \operatorname{rad}(\boldsymbol{y}) +^{\uparrow} \epsilon_{+,\boldsymbol{x},\boldsymbol{y}}) \\
\boldsymbol{x} - \boldsymbol{y} &= \operatorname{cen}(\boldsymbol{x}) -^{\updownarrow} \operatorname{cen}(\boldsymbol{y}) + \mathcal{B}(\operatorname{rad}(\boldsymbol{x}) +^{\uparrow} \operatorname{rad}(\boldsymbol{y}) +^{\uparrow} \epsilon_{-,\boldsymbol{x},\boldsymbol{y}}) \\
\boldsymbol{x}\, \boldsymbol{y} &= \operatorname{cen}(\boldsymbol{x}) \times^{\updownarrow} \operatorname{cen}(\boldsymbol{y}) + \\
&\quad \mathcal{B}(\operatorname{rad}(\boldsymbol{x}) \times^{\uparrow} (|\operatorname{cen}(\boldsymbol{y})| +^{\uparrow} \operatorname{rad}(\boldsymbol{y})) +^{\uparrow} |\operatorname{cen}(\boldsymbol{y})| \times^{\uparrow} \operatorname{rad}(\boldsymbol{x}) +^{\uparrow} \epsilon_{\times,\boldsymbol{x},\boldsymbol{y}}),
\end{aligned}$$

where $\epsilon_{+,\boldsymbol{x},\boldsymbol{y}}$, $\epsilon_{-,\boldsymbol{x},\boldsymbol{y}}$ and $\epsilon_{\times,\boldsymbol{x},\boldsymbol{y}}$ are reliable bounds for the rounding errors induced by the corresponding floating point operations on the centers; see [vdH09] for more details. Given $\boldsymbol{z} \in \tilde{\mathbb{C}}$, it will be convenient to denote by $\lfloor \boldsymbol{z} \rfloor$ and $\lceil \boldsymbol{z} \rceil$ certified lower and upper bounds for $|\boldsymbol{z}|$.

2.3. Balls of polynomials and analytic functions

Let $\mathbb{B} = \mathcal{B}(1) \subseteq \mathbb{C}$ denote the closed unit disk and $\mathbb{S} \subseteq \mathbb{C}$ the closed unit circle. Let $\mathcal{A}_{\mathbb{B}}$ and $\mathcal{A}_{\mathbb{S}}$ denote the rings of analytic functions on $\mathbb{B}$ resp. $\mathbb{S}$. We define norms on $\mathcal{A}_{\mathbb{B}}$ and $\mathcal{A}_{\mathbb{S}}$ by

$$\begin{aligned} \|f\| &= \sup_{z \in \mathbb{B}} |f(z)| \qquad (f \in \mathcal{A}_{\mathbb{B}}) \\ \|f\| &= \sup_{z \in \mathbb{S}} |f(z)| \qquad (f \in \mathcal{A}_{\mathbb{S}}). \end{aligned}$$

By the maximum modulus principle, the inclusion $\mathcal{A}_{\mathbb{B}} \hookrightarrow \mathcal{A}_{\mathbb{S}}$ preserves norms. Since our criterion for root counting will be based on a variant of Rouché's theorem, we will mainly consider analytic functions on $\mathbb{S}$ in what follows. In order to avoid confusion with $\mathcal{B}(r)$, we will denote by $\mathcal{B}_{\mathbb{S}}(r)$ the closed ball of radius r in $\mathcal{A}_{\mathbb{S}}$:

$$\mathcal{B}_{\mathbb{S}}(r) = \{f \in \mathcal{A}_{\mathbb{S}} \colon \|f\| \leqslant r\}.$$

In view of section 2.1, we may then consider the space $\mathcal{B}(\mathbb{C}[z], \mathbb{R})$ of balls with centers in $\mathbb{C}[z]$ and radii in $\mathbb{R}^{\geqslant}$. Any such ball can be written $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r)$ for $P \in \mathbb{C}[z]$ and $r \in \mathbb{R}^{\geqslant}$. For concrete machine computations, and in a similar way as in section 2.2, we may also consider the space $\mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$ of balls with centers in $\tilde{\mathbb{C}}[z]$ and radii in $\tilde{\mathbb{R}}^{\geqslant}$. Given $\boldsymbol{f} \in \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$, we will denote by $\mathbb{[\![} \boldsymbol{f} \mathbb{]\!]}$ a certified upper bound for $\boldsymbol{f}(z)$ on $\mathbb{S}$. If $\boldsymbol{f} = P_0 + \cdots + P_n z^n + \mathcal{B}_{\mathbb{S}}(r)$, then we may for instance take $\mathbb{[\![} \boldsymbol{f} \mathbb{]\!]} = \lceil P_0 \rceil +^{\uparrow} \cdots +^{\uparrow} \lceil P_n \rceil +^{\uparrow} r$.

2.4. Simplification

Consider a ball $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r) \in \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$ with $n = \deg P \geqslant 0$ and let e_P be the maximum of the exponents of the coefficients of P. Let $q \leqslant p$ be maximal such that

$$2^{e_P - q} \geqslant \frac{r}{256\,(n+1)}$$

and take $q = 0$ if $256\,(n+1)\,2^{e_P} < r$. Denote $\mathbb{Z}_q = \pm\{0, \ldots, 2^q - 1\}$. Truncation of the mantissas of the coefficients of P leads to a decomposition

$$P = P_{\text{head}} + P_{\text{tail}},$$

where

$$\begin{aligned} P_{\text{head}} &\in \mathbb{Z}_q[\mathrm{i}][z]\, 2^{e_P + 1 - q} \\ \mathbb{[\![} P_{\text{tail}} \mathbb{]\!]} &\leqslant \max\left\{\tfrac{r}{64}, 2^{e_P + 2 - p}\right\}. \end{aligned}$$

We define the simplification $\sigma(\boldsymbol{f})$ of $\boldsymbol{f}$ by

$$\sigma(\boldsymbol{f}) = P_{\text{head}} + \mathcal{B}_{\mathbb{S}}(\mathbb{[\![} P_{\text{tail}} + \mathcal{B}_{\mathbb{S}}(r) \mathbb{]\!]})$$

and notice that $\boldsymbol{f} \subseteq \sigma(\boldsymbol{f})$.

2.5. Efficient multiplication

Assume now that we want to multiply two balls $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r)$ and $\boldsymbol{g} = Q + \mathcal{B}_{\mathbb{S}}(s)$ in an efficient way. Modulo simplification, we may assume without loss of generality that $\boldsymbol{f} = \sigma(\boldsymbol{f})$ and $\boldsymbol{g} = \sigma(\boldsymbol{g})$. For some common $q \leqslant p$, we thus have

$$\begin{aligned} P &\in \mathbb{Z}_q[\mathrm{i}][z]\, 2^{e_P + 1 - q} \\ Q &\in \mathbb{Z}_q[\mathrm{i}][z]\, 2^{e_Q + 1 - q} \end{aligned}$$

We may multiply the integer polynomials $P^* = P/2^{e_P+1-q}$ and $Q^*/2^{e_Q+1-q}$ using any fast classical algorithm, such as Kronecker substitution [PB94, GG02]. When truncating $(P^*\,Q^*)\,2^{e_P+e_Q+2-2q}$ back to a complex floating polynomial $R \in \tilde{\mathbb{C}}[z]$, we have

$$\left\lVert R - (P^*\,Q^*)\,2^{e_P+e_Q+2-2q} \right\rVert \;\leqslant\; 2^{e_R+2-p}.$$

Consequently, we may take

$$\boldsymbol{f}\boldsymbol{g} \;=\; R + \mathcal{B}_{\mathbb{S}}(2^{e_R+2-p} +^{\uparrow} r \times^{\uparrow} \left\lVert Q \right\rVert +^{\uparrow} s \times^{\uparrow} \left\lVert P \right\rVert +^{\uparrow} r \times^{\uparrow} s).$$

3. The algorithm

Given an analytic function $f \in \mathcal{A}_{\mathbb{S}}$ with no zeros on $\mathbb{S}$, we will denote

$$\kappa(f) \;=\; \frac{1}{2\,\pi\,\mathrm{i}} \oint_{\mathbb{S}} \frac{f'(z)}{f(z)}\,\mathrm{d}\,z.$$

If $f \in \mathcal{A}_{\mathbb{B}}$, then $\kappa(f)$ counts the number of zeros of f in the open unit disk. Now consider a ball $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r) \in \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$ of analytic functions. Whenever no $f \in \boldsymbol{f}$ admits a zero on $\mathbb{S}$, then $\kappa(\boldsymbol{f}) := \kappa(f)$ does not depend on the choice of $f \in \boldsymbol{f}$. The aim of this paper is to compute $\kappa(\boldsymbol{f})$ in this case. If some $f \in \boldsymbol{f}$ admit zeros which are too close to $\mathbb{S}$, then the algorithm is allowed to fail.

3.1. Rouché's theorem

The method that we will use for certifying the number of roots relies on the following variant of Rouché's theorem.

THEOREM 1. *Let $f(z)$ and $g(z)$ be two analytic functions on $\mathbb{S}$, such that*

$$|f(z) - g(z)| \;<\; |g(z)|.$$

Then $\kappa(f) = \kappa(g)$.

Proof. We will use a similar argument as in [Lan76, page 158]. Let γ be the path on $\mathbb{S}$ which turns one time around the origin and let $F = f/g$. By our assumption, the path $F \circ \gamma$ is contained in the open disk with center one and radius one. Since this disk does not contain the origin, we have [Lan76, Lemma 3, page 116]

$$W(F \circ \gamma, 0) \;:=\; \frac{1}{2\,\pi\,\mathrm{i}} \int_{F\circ\gamma} \frac{\mathrm{d}\,z}{z} = 0.$$

But

$$W(F \circ \gamma, 0) \;=\; \frac{1}{2\,\pi\,\mathrm{i}} \int_{\gamma} \frac{F'(z)}{F(z)}\,\mathrm{d}\,z = \kappa(f) - \kappa(g),$$

whence $\kappa(f) = \kappa(g)$. □

Given a polynomial $P = P_0 + \cdots + P_n\,z^n \in \tilde{\mathbb{C}}[z]$ and $k \in \mathbb{N}$, let us denote by $P_{\bar{k}}$ the polynomial $P_0 + \cdots + P_{k-1}\,z^{k-1} + P_{k+1}\,z^{k+1} + \cdots + P_n\,z^n$.

PROPOSITION 2. *Consider a ball $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r) \in \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$ and let k be the index for which $\lceil P_k \rceil$ is maximal. If*

$$\left\lVert P_{\bar{k}} + \mathcal{B}(r) \right\rVert \;<\; \lfloor P_k \rfloor,$$

then $\kappa(\boldsymbol{f}) = k$.

Proof. Let $f = P + \varepsilon$ with $\|\varepsilon\| \leqslant r$. Setting $g = f_k z^k$, our assumption implies

$$|f(z) - g(z)| \;<\; |g(z)|,$$

for all $z \in \mathbb{S}$. By theorem 1, we conclude that $\kappa(f) = \kappa(f_k z^k) = k$. □

3.2. Graeffe transforms

The second ingredient for our algorithm is the Graeffe transform, which we will use for analytic functions. Given $f \in \mathcal{A}_{\mathbb{S}}$, we define its *Graeffe transform* $g = \mathrm{Gr}(f) \in \mathcal{A}_{\mathbb{S}}$ by

$$\begin{aligned} f_{\mathrm{even}}(z^2) &= \tfrac{1}{2}(f(z) + f(-z)) \\ f_{\mathrm{odd}}(z^2) &= \tfrac{1}{2z}(f(z) - f(-z)) \\ g(z) &= f_{\mathrm{odd}}(z)^2 z - f_{\mathrm{even}}(z)^2 \\ &= \tfrac{1}{4}((f(\sqrt{z}) - f(-\sqrt{z}))^2 - (f(\sqrt{z}) + f(-\sqrt{z}))^2) \end{aligned}$$

If f is actually a polynomial, then we notice that g has the same degree as f. The fundamental property of Graeffe transforms is:

PROPOSITION 3. *On a small annulus containing* $\mathbb{S}$*, the roots of* g *are precisely the squares of the roots of* f*, when counting with multiplicities.*

Proof. By continuity under small deformations, it suffices to consider the case when g has only simple zeros z near $\mathbb{S}$. Now

$$\begin{aligned} g(z) = 0 &\Leftrightarrow f(\sqrt{z}) - f(-\sqrt{z}) = \pm(f(\sqrt{z}) + f(-\sqrt{z})) \\ &\Leftrightarrow f(\sqrt{z}) = 0 \vee f(-\sqrt{z}) = 0, \end{aligned}$$

for all z near $\mathbb{S}$. □

Let us show that the Graeffe transform can be lifted to an operation $\mathrm{Gr}: \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}}) \to \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$ which satisfies the inclusion property

$$f \in \boldsymbol{f} \;\Rightarrow\; \mathrm{Gr}(f) \in \mathrm{Gr}(\boldsymbol{f}),$$

for all $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r) \in \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$ and $f \in \mathcal{A}_{\mathbb{S}}$. If $r = 0$, then we may directly use the formula $\mathrm{Gr}(\boldsymbol{f}) = P_{\mathrm{odd}}^2 z - P_{\mathrm{even}}^2$, assuming that the squares are computed using the algorithm for ball multiplication in section 2.5. In general, we take

$$\mathrm{Gr}(\boldsymbol{f}) \;=\; \mathrm{Gr}(P + \mathcal{B}_{\mathbb{S}}(0)) + \mathcal{B}_{\mathbb{S}}(2\,(\lceil\!\lceil P_{\mathrm{odd}} \rceil\!\rceil + \lceil\!\lceil P_{\mathrm{even}} \rceil\!\rceil)\, r + 2\, r^2)$$

and claim that this definition satisfies the inclusion property. Indeed, given $f \in \boldsymbol{f}$, there exists an $\varepsilon \in \mathcal{B}_{\mathbb{S}}(r)$ with $f = P + \varepsilon$. Hence,

$$\mathrm{Gr}(f) \;=\; \mathrm{Gr}(P) + 2\, P_{\mathrm{odd}}\, \varepsilon_{\mathrm{odd}}\, z + \varepsilon_{\mathrm{odd}}^2\, z - 2\, P_{\mathrm{even}}\, \varepsilon_{\mathrm{even}} - \varepsilon_{\mathrm{even}}^2.$$

Since $\|\varepsilon_{\mathrm{even}}\| \leqslant \|\varepsilon\|$ and $\|\varepsilon_{\mathrm{odd}}\| \leqslant \|\varepsilon\|$, we thus have

$$\begin{aligned} \|\mathrm{Gr}(f) - \mathrm{Gr}(P)\| &= \|2\, P_{\mathrm{odd}}\, \varepsilon_{\mathrm{odd}}\, z + \varepsilon_{\mathrm{odd}}^2\, z - 2\, P_{\mathrm{even}}\, \varepsilon_{\mathrm{even}} - \varepsilon_{\mathrm{even}}^2\| \\ &\leqslant 2\, \|P_{\mathrm{odd}}\|\, r + r^2 + 2\, \|P_{\mathrm{even}}\|\, r + r^2 \\ &\leqslant 2\, (\lceil\!\lceil P_{\mathrm{odd}} \rceil\!\rceil + \lceil\!\lceil P_{\mathrm{even}} \rceil\!\rceil)\, r + 2\, r^2. \end{aligned}$$

This proves our claim.

3.3. Root counting

Putting together the various pieces, we now have the following algorithm for root counting. Optionally, one may add an extra integer parameter in order to limit the number of recursive calls to, say, $\lceil 2 \log_2 p \rceil$.

Algorithm root-count(f)
INPUT: $\boldsymbol{f} \in \mathcal{B}(\tilde{\mathbb{C}}[z], \tilde{\mathbb{R}})$
OUTPUT: $\kappa(\boldsymbol{f})$ or failure

Let $\boldsymbol{f} := \sigma(\boldsymbol{f})$ and write $\boldsymbol{f} = P + \mathcal{B}_{\mathbb{S}}(r)$
If $P = 0$, then **abort**
Let $v := \mathrm{val}(P)$ and $P := P z^{-v}$
Let k be such that $|P_k|$ is maximal
If $r \geqslant |P_k|$, then **abort**
If $\llbracket P_{\bar{k}} + \mathcal{B}_{\mathbb{S}}(r) \rrbracket < \lfloor P_k \rfloor$, then return $k + v$
Return root-count($\mathrm{Gr}(P + \mathcal{B}_{\mathbb{S}}(r))$)

One nice property of this algorithm is that the degree of P often quickly decreases during successive recursive calls. More precisely, let $z_1, \ldots, z_n$ be the zeros of P, ordered such that $|z_1| < \cdots |z_k| < 1 < |z_{k+1}| < \cdots < |z_n|$. Then

$$\frac{\mathrm{Gr}^i(p)}{\mathrm{Gr}^i(p)_k} \;=\; (z - z_k^{2^i}) \cdots (z - z_1^{2^i})\, (1 - z_{k+1}^{-2^i} z) \cdots (1 - z_n^{-2^i} z).$$

In the right hand size, all coefficients which smaller than 2^{-p} are discarded via simplification. Roughly speaking, for $j < k$, the j-th coefficient therefore only survives as long as $(z_j \cdots z_k)^{2^i} > 2^{-p}$.

3.4. Alternative termination strategies

In our algorithm, satisfaction of the condition $\llbracket P_{\bar{k}} + \mathcal{B}_{\mathbb{S}}(r) \rrbracket < \lfloor P_k \rfloor$ enabled us to produce a final certified root count. It may be possible to design quick certified root counts for other favourable cases. Any alternative root counting strategy may actually be tried before applying our algorithm, or even at every stage as a replacement of the default strategy based on the condition $\llbracket P_{\bar{k}} + \mathcal{B}_{\mathbb{S}}(r) \rrbracket < \lfloor P_k \rfloor$.

One natural alternative root counting strategy is based on the evaluation of $\boldsymbol{f}$ at many points on $\mathbb{S}$. Let N to be the smallest power of two which is larger than $\pi\, n$ and take $\omega = \mathrm{e}^{2\pi \mathrm{i}/N}$. Then we may efficiently evaluate P at 1, ω, ..., ω^{N-1} using the FFT. Furthermore, the distance between two successive powers of ω is bounded by $1/n$. Now assume that

$$\frac{\llbracket P' \rrbracket}{2\, n} \;<\; \lfloor P(\omega^k) \rfloor - r \tag{2}$$

for all k. Then it is guaranteed that $\boldsymbol{f}$ admits no zeros on $\mathbb{S}$. Hence,

$$\kappa(\boldsymbol{f}) \;=\; \frac{1}{2\,\pi} \sum_{k=0}^{n-1} \arg \frac{P(\omega^{k+1})}{P(\omega^k)}.$$

When multiplying the number of points N by a constant K, we may replace $2\, n$ by $2\, K\, n$ in the denominator of (2). We may also consider the second order condition

$$\frac{\llbracket P'' \rrbracket}{4\, n^2} + \frac{\lceil P'(\omega^k) \rceil}{2\, n} \;<\; \lfloor P(\omega^k) \rfloor - r \tag{3}$$

instead of (2), which requires the additional evaluation of P' at the powers ω^k. The conditions (2) and (3) have a reasonable chance of being satisfied if the closest root of $\boldsymbol{f}$ with respect to $\mathbb{S}$ is at distance at least n^{-1}.

Bibliography

[AH83] G. Alefeld and J. Herzberger. *Introduction to interval analysis*. Academic Press, New York, 1983.

[ANS08] ANSI/IEEE. IEEE standard for binary floating-point arithmetic. Technical report, ANSI/IEEE, New York, 2008. ANSI-IEEE Standard 754-2008. Revision of IEEE 754-1985, approved on June 12, 2008 by IEEE Standards Board.

[GG02] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2-nd edition, 2002.

[Gou96] X. Gourdon. *Combinatoire, algorithmique et géométrie des polynômes*. PhD thesis, École polytechnique, 1996.

[HLRZ00] G. Hanrot, V. Lefèvre, K. Ryde, and P. Zimmermann. MPFR, a C library for multiple-precision floating-point computations with exact rounding. `http://www.mpfr.org`, 2000.

[KvB00] P. Kravanja and M. van Barel. *Computing the zeros of analytic functions*, volume 1727 of *Lecture Notes in Mathematics*. Springer-Verlag, 2000.

[Lan76] S. Lang. *Complex analysis*. Addison-Wesley, 1976.

[MKC09] R.E. Moore, R.B. Kearfott, and M.J. Cloud. *Introduction to Interval Analysis*. SIAM Press, 2009.

[Moo66] R.E. Moore. *Interval Analysis*. Prentice Hall, Englewood Cliffs, N.J., 1966.

[Pan02] V. Y. Pan. Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding. *J. Symbolic Comput.*, 33(5):701–733, 2002.

[PB94] V. Pan and D. Bini. *Polynomial and matrix computations*. Birkhauser, 1994.

[Rum10] S.M. Rump. Verification methods: Rigorous results using floating-point arithmetic. *Acta Numerica*, 19:287–449, 2010.

[Sch82] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Technical report, Math. Inst. Univ. of Tübingen, 1982.

[vdH09] J. van der Hoeven. Ball arithmetic. Technical report, HAL, 2009. `http://hal.archives-ouvertes.fr/hal-00432152/fr/`.