

COMPUTING THE DISTANCE FROM A POINT TO AN ALGEBRAIC HYPERSURFACE

J.P. DEDIEU, X. GOURDON AND J.C. YAKOUBSOHN

ABSTRACT. We generalize the Dandelin-Graeffés method to the multivariate case and apply it to compute the distance from a point to an algebraic surface. For that we introduce the positive root of a certain concave which is a good lower bound of this distance. We also illustrate this theoretical fact by a numerical example.

1. INTRODUCTION

This paper is devoted to the problem of computing the distance in \mathbb{C}^n from a point u to an algebraic hypersurface $\mathcal{Z} = \{z \in \mathbb{C}^n : P(z) = 0\}$ where $P(z)$ is a polynomial in $\mathbb{C}[z_1, \dots, z_n]$, the distance in \mathbb{C}^n corresponding to the norm

$$\|z\| = \max_{1 \leq k \leq n} |z_k|.$$

By shifting the variable z , we can restrict in the case $u = 0$. In fact we compute a sequence of lower bounds converging to $d(0, \mathcal{Z})$. Such lower bounds for the distance from u to \mathcal{Z} are particularly useful to give an approximation of \mathcal{Z} via an exclusion-bisection algorithm. In the univariate case such lower bounds, also called proximity tests, are given by Weyl [8], Henrici-Gargantini [4], Schönhage [6], Turan [7]. One may consult about this subject the recent survey written by Pan [5]. In the multivariate case a proximity test based on Taylor's formula is studied by Dedieu-Yakoubsohn [2].

The test presented here is based on both Taylor's formula and a generalization of Dandelin-Graeffe's process to the multivariate case (see [1] or [6] for the univariate case). It consists essentially in computing the N -th Graeffe iterate of $P(z)$ (see Definition 1), which has the form

$$P^{[N]}(z) = \sum_{j \geq 0} B_j(z)$$

where the $B_j(z)$ are homogeneous polynomials of degree $2^N j$, and then computing the non negative root ρ_N of the equation in ρ

$$\|B_0\| = \sum_{j \geq 1} \|B_j\| \rho^j,$$

1991 *Mathematical Subject Classification*. Primary 65H05, 12D10; Secondary 26C10.

© 1996 American Mathematical Society

the norms $\|B_j\|$ being the sum of the absolute values of coefficients of B_j . Then $r_N = \rho_N^{2^{-N}}$ tends rapidly to $d(0, \mathcal{Z})$.

More precisely the following theorem is proved :

Theorem 1. Let ρ_N be the unique nonnegative solution of

$$(1) \quad |P^{[N]}(0)| = \sum_{j=1}^d \|B_j^{[N]}\| \rho^j$$

The distance from 0 to \mathcal{Z} satisfies

$$(2) \quad r_N \leq d(0, \mathcal{Z}) \leq \kappa_N r_N,$$

where

$$r_N = \rho_N^{2^{-N}} \quad \text{and} \quad \kappa_N = \left(\frac{1}{2^{1/d} - 1} \sqrt{\frac{2^N + n - 1}{n - 1}} \right)^{1/2^N}.$$

Moreover $\lim_{N \rightarrow \infty} \kappa_N = 1$, which implies $\lim_{N \rightarrow \infty} r_N = d(0, \mathcal{Z})$.

2. THE GRAEFFE PROCESS.

The purpose of this part is to generalize the classical univariate Graeffe process to the multivariate case. In the univariate case, the Graeffe iterate of polynomial $P(z)$ is defined as the unique polynomial $Q(z)$ such that $Q(z^2) = P(z)P(-z)$. In the multivariate case, the polynomial $P(z)P(-z)$ can not be written as $Q(z^2)$ where $Q(z)$ is a polynomial, thus we need to slightly modify the definition.

Definition 1. We call the N -th Graeffe iterate of $P(z) \in \mathbb{C}[z_1, \dots, z_n]$ the polynomial $P^{[N]}(z)$ defined by

$$(3) \quad P^{[N]}(z) = \prod_{j=0}^{2^N-1} P(\omega^j z), \quad \omega = \exp\left(\frac{2i\pi}{2^N}\right), \quad i^2 = -1.$$

When $P(z)$ is a univariate polynomial, we have $P^{[1]}(z) = P(z)P(-z) = P^{(1)}(z^2)$ where $P^{(1)}(z)$ is the classical Graeffe iterate of $P(z)$. More generally, the N -th classical univariate Graeffe iterate satisfy $P^{(N)}(z) = P^{[N]}(z^{2^N})$ for all N . Remember that $P^{(N)}(z)$ has the same degree as $P(z)$ and its roots are the 2^N powers of roots of $P(z)$ (see [Ba]).

Graeffe iterates satisfy several properties which make them easy to compute.

Proposition 1. For all non negative integer N , the N -th Graeffe iterate of $P(z)$ writes as

$$P^{[N]}(z) = \sum_{j \geq 0} B_j^{[N]}(z),$$

where the $B_j^{[N]}$'s are homogeneous polynomials of degree $2^N j$. The $(N+1)$ -st Graeffe iterate can be computed from the N -th thanks to the formula

$$(4) \quad P^{[N+1]}(z) = P_0^{[N]}(z)^2 - P_1^{[N]}(z)^2, \quad P_k^{[N]}(z) = \sum_{j \equiv k \pmod{2}} B_j^{[N]}(z).$$

Proof. Since the degrees of all the monomials in $P_0^{[N]}(z)^2$ and $P_1^{[N]}(z)^2$ are multiples of 2^{N+1} , we need only to prove formula (2). For this, we notice that

$$P^{[N+1]}(z) = P^{[N]}(z)P^{[N]}(\omega z), \quad \omega = \exp\left(\frac{2i\pi}{2^{N+1}}\right),$$

and since $P_0^{[N]}(\omega z) = P_0^{[N]}(z)$ and $P_1^{[N]}(\omega z) = -P_1^{[N]}(z)$, this implies

$$P^{[N+1]}(z) = \left(P_0^{[N]}(z) + P_1^{[N]}(z)\right) \left(P_0^{[N]}(z) - P_1^{[N]}(z)\right) = P_0^{[N]}(z)^2 - P_1^{[N]}(z)^2,$$

proving the result. \square

3. THE UNIVARIATE CASE

In the univariate case, the distance $d(0, \mathcal{Z})$ from 0 to the set \mathcal{Z} of zeros of $P(z)$ is also the smallest modulus of the roots of $P(z)$. Computing this distance is a classical task. It usually consists in using the Graeffe process together with a result giving an upper and a lower bound for $d(0, \mathcal{Z})$. Classical bounds are given in the following theorem, which can be found in [3] Theorems 6.4.d and 6.4.i.

Theorem 2. Let $P(z) = \sum_{k=0}^d b_k z^k$ be a univariate complex polynomial, and $\rho(P)$ the nonnegative root of the equation

$$|b_0| = \sum_{j=1}^d |b_j| \rho^j.$$

Then

$$\rho(P) \leq d(0, \mathcal{Z}) \leq \frac{1}{2^{1/d} - 1} \rho(P).$$

The value $\rho(P)$ is easily computable. When we apply this result to the N -th classical Graeffe iterate of $P(z)$, we obtain

$$\rho(P^{(N)}) \leq d(0, \mathcal{Z}_N) \leq \frac{1}{2^{1/d} - 1} \rho(P^{(N)}),$$

where \mathcal{Z}_N is the set of roots of $P^{(N)}(z)$. Since the roots of $P^{(N)}(z)$ are the 2^N -th powers of the roots of $P(z)$, we have $d(0, \mathcal{Z}_N) = d(0, \mathcal{Z})^{2^N}$, thus

$$(5) \quad r_N \leq d(0, \mathcal{Z}) \leq \left(\frac{1}{2^{1/d} - 1}\right)^{2^{-N}} r_N, \quad r_N = \rho(P^{(N)})^{2^{-N}}.$$

The upper bound tends rapidly to the lower bound as N increases, thus we have obtained an effective process to compute $d(0, \mathcal{Z})$.

4. THE MULTIVARIATE CASE

Thanks to the multivariate Graeffe process, we easily generalize the univariate algorithm to compute $d(0, \mathcal{Z})$ to the multivariate case.

Theorem 3. Let $P(z)$ be a polynomial in $\mathbb{C}[z_1, \dots, z_n]$ of total degree d . Let $P^{[N]}(z) = \sum_{j \geq 0} B_j^{[N]}(z)$ be its N -th Graeffe iterate and R_N the non-negative solution R of the equation

$$(6) \quad |P^{[N]}(0)| = \sum_{j \geq 1} \|B_j^{[N]}\|_{\infty} R^j,$$

where $\|B_j^{[N]}\|_{\infty} = \sup_{\|z\|=1} \|B_j(z)\|$. Then we have

$$(7) \quad r_N \leq d(0, \mathcal{Z}) \leq \left(\frac{1}{2^{1/d} - 1} \right)^{2^{-N}} r_N, \quad r_N = R_N^{2^{-N}}$$

Proof. If $P(0) = 0$, there is nothing to prove since $r_N = 0$. Otherwise, we have $P^{[N]}(0) \neq 0$. We prove first the left part of the inequality. Let $z \in \mathbb{C}^n$, $\|z\| < r_N = R_N^{2^{-N}}$. We have

$$|P^{[N]}(z)| \geq |P^{[N]}(0)| - \sum_{j \geq 1} \|B_j^{[N]}\|_{\infty} \|z\|^{2^N j} > |P^{[N]}(0)| - \sum_{j \geq 1} \|B_j^{[N]}\|_{\infty} R_N^j = 0,$$

thus $P^{[N]}(z)$ does not vanish in the open ball centered in zero with radius r_N , and since $P(z)$ is a factor of $P^{[N]}(z)$, this is also the case for $P(z)$. Thus $r_N \leq d(0, \mathcal{Z})$.

Now we prove the right inequality of 7. For all $y \in \mathbb{C}^n$ such that $\|y\| = 1$, we define the univariate polynomial $P_y(t) = P(ty)$. We have

$$(8) \quad P_y^{(N)}(t) = \sum_{j=0}^d B_j^{[N]}(y) t^j.$$

Let $\mathcal{Z}_N(y)$ denotes the set of zeros of $P_y^{(N)}(t)$. Since

$$d(0, \mathcal{Z}_N(y)) = d(0, \mathcal{Z}_0(y))^{2^N} \geq d(0, \mathcal{Z})^{2^N},$$

formula 8 together with Lemma 1 below yield for all j

$$(9) \quad |B_j^{[N]}(y)| \leq |P^{[N]}(0)| \binom{d}{j} \frac{1}{d(0, \mathcal{Z})^{2^N j}}.$$

The right side of the inequality is independent of y such that $\|y\| = 1$, thus inequality 9 remains valid with $|B_j^{[N]}(y)|$ replaced by $\|B_j^{[N]}\|_{\infty}$. Plugging this information into equation 6 defining R_N , we obtain

$$|P^{[N]}(0)| \leq \sum_{j \geq 1} |P^{[N]}(0)| \binom{d}{j} \frac{R_N^j}{d(0, \mathcal{Z})^{2^N j}},$$

that is

$$1 \leq \left(1 + \frac{R_N}{d(0, \mathcal{Z})^{2^N}} \right)^d - 1,$$

leading to

$$\frac{d(0, \mathcal{Z})^{2^N}}{R_N} \leq \frac{1}{2^{1/d} - 1},$$

proving the right inequality of 7. \square

The following lemma was needed in the proof of Theorem 3. Its proof can be found in [3] chap. 6, 6.4-8.

Lemma 1. *Let $P(z) = \sum_{j=0}^d b_j z^j$ be a univariate complex polynomial, $\mathcal{Z}(P)$ the set of its roots, $b_0 \neq 0$. Then*

$$|b_j| \leq |b_0| \binom{d}{j} \frac{1}{d(0, \mathcal{Z}(P))^j}.$$

Theorem 3 can not be applied directly to approach $d(0, \mathcal{Z})$ in the practice, since the norms $\| \cdot \|_\infty$ are difficult to compute. Instead, we make use of the norm

$$\left\| \sum_{\alpha} a_{\alpha} z^{\alpha} \right\| = \sum |a_{\alpha}|,$$

easy to compute. Our main result is stated using this norm. We now shall prove the theorem 1.

5. PROOF OF THE THEOREM 1

For the left part of inequality 2, we proceed as in the proof of Theorem 3 replacing the norm $\| \cdot \|_\infty$ with $\| \cdot \|$. We can do that because $\| \cdot \|_\infty \leq \| \cdot \|$ (see Lemma 2 below).

Now we prove the right part of 2. Lemma 2 and Lemma 3 below give for all j ,

$$\|B_j^{[N]}\| \leq \sqrt{\binom{j2^N + n - 1}{n - 1}} \|B_j^{[N]}\|_\infty \leq \alpha^j \|B_j^{[N]}\|_\infty, \quad \alpha = \sqrt{\binom{2^N + n - 1}{n - 1}}$$

thus

$$|P^{[N]}(0)| = \sum_{j=1}^d \|B_j^{[N]}\| \rho_N^j \leq \sum_{j=1}^d \|B_j^{[N]}\|_\infty (\alpha \rho_N)^j.$$

This implies

$$R_N \leq \alpha \rho_N,$$

where R_N satisfies equation 6. The inequality 7 satisfied by R_N now entails

$$d(0, \mathcal{Z}) \leq \left(\frac{1}{2^{1/d} - 1} \right)^{2^{-N}} R_N^{2^{-N}} \leq \left(\frac{\alpha}{2^{1/d} - 1} \right)^{2^{-N}} \rho_N^{2^{-N}},$$

proving the result.

In order to prove Theorem 1, we needed a lemma comparing the norm $\| \cdot \|$ on polynomials with the intrinsic norm $\| \cdot \|_\infty$.

Lemma 2. *Let $A \in \mathbb{C}[z_1, \dots, z_n]$ be an homogeneous polynomial of degree k , $z \in \mathbb{C}^n$. Then*

$$\max_{\|z\|=1} |A(z)| = \|A\|_\infty \leq \|A\| \leq \sqrt{\binom{k + n - 1}{n - 1}} \|A\|_\infty.$$

Proof. The left inequality is trivial. Let us show the right inequality. Let $A(z) = \sum_{|\alpha|=k} a_\alpha z^\alpha$ and $\|A\|_2 = \left(\sum_{|\alpha|=k} |a_\alpha|^2\right)^{1/2}$. The Parseval identity

$$\|A\|_2^2 = \left(\frac{1}{2\pi}\right)^n \int_{[0,2\pi]^n} |A(e^{i\theta_1}, \dots, e^{i\theta_n})|^2 d\theta_1 \dots d\theta_n$$

implies $\|A\|_2 \leq \|A\|$. To conclude, we use Cauchy-Schwarz inequality

$$\|A\| \leq \sqrt{K} \|A\|_2,$$

where K is the total number of $\alpha \in \mathbb{N}^n$ such that $|\alpha| = k$, that is $K = \binom{k+n-1}{n-1}$. \square

The following combinatorial lemma was also needed in the proof of Theorem 1.

Lemma 3. *For all positive integer j , K and p , we have*

$$\binom{jK+p}{p} \leq \binom{K+p}{p}^j.$$

Proof. The inequality

$$\binom{jK+p}{p} \binom{K+p}{p}^{-j} = \prod_{\ell=1}^p \frac{(jK+\ell)\ell^{j-1}}{(K+\ell)^j} \leq 1,$$

holds because each term in the product is ≤ 1 , this being true because $(jK + \ell)\ell^{j-1} = \ell^j + jK\ell^{j-1}$ represents the first two terms in the binomial expansion of $(K + \ell)^j$. \square

6. CONVERGENCE OF THE PROCESS

The sharpness of inequality 2 depends essentially of the rate of convergence of κ_N to 1. In fact, this convergence appears to be fast. As an illustration, Table 1 shows, for different values of n and d , $1 \leq n \leq 10$ and $2 \leq d \leq 10$, the minimal value of N such that

$$\rho_N \leq d(0, \mathcal{Z}) \leq 2\rho_N.$$

$d \setminus n$	1	2	3	4	5	6	7	8	9	10
2	2	2	3	3	3	3	4	4	4	4
3	2	3	3	3	3	4	4	4	4	4
4	2	3	3	3	3	4	4	4	4	4
5	2	3	3	3	4	4	4	4	4	4
6	3	3	3	3	4	4	4	4	4	4
7	3	3	3	3	4	4	4	4	4	4
8	3	3	3	4	4	4	4	4	4	4
9	3	3	3	4	4	4	4	4	4	4
10	3	3	3	4	4	4	4	4	4	4

Table 1.

The following result also gives an idea of how fast does κ_N tend to 1.

Proposition 2. *The error coefficient κ_N satisfies, for $N \geq 1$,*

$$1 \leq \kappa_N \leq (2d)^{1/2^N} 2^{N(n-1)/2^{N+1}}.$$

Proof. The inequality $1 \leq \kappa_N$ is trivial. For the other, we first write

$$\binom{2^N + n - 1}{n - 1} = \frac{2^N + 1}{1} \cdot \frac{2^N + 2}{2} \cdots \frac{2^N + n - 1}{n - 1},$$

thus

$$\binom{2^N + n - 1}{n - 1} = 2^{N(n-1)} (2^{-N} + 1) \left(2^{-N} + \frac{1}{2}\right) \cdots \left(2^{-N} + \frac{1}{n-1}\right),$$

and since $N \geq 1$, this implies

$$\binom{2^N + n - 1}{n - 1} \leq 2^{N(n-1)} (2^{-N} + 1) \leq 1.5 \cdot 2^{N(n-1)}.$$

Now, we have $2^{1/d} - 1 = e^{\log 2/d} - 1 \geq \log 2/d$, thus

$$\frac{1}{2^{1/d} - 1} \leq \frac{d}{\log 2}.$$

This finally gives

$$\kappa_N \leq \left(\frac{d}{\log 2} \sqrt{1.5} \cdot 2^{N(n-1)/2}\right)^{1/2^N} \leq \left((2d) 2^{N(n-1)/2}\right)^{1/2^N},$$

yielding the result. \square

In the practice, when n is large, computation of r_N becomes very expensive when N gets large. The following result gives a bound on κ_N for a reasonable value of N .

Proposition 3. *Let N be such that $2^N \leq n < 2^{N+1}$. Then the error coefficient κ_N satisfies*

$$1 \leq \kappa_N \leq 4(1.45d)^{2/n}.$$

Proof. We need to prove the second inequality. First, we notice that

$$\binom{2^N + n - 1}{n - 1} \leq \binom{2n - 1}{n - 1} \leq \binom{2n}{n} \leq 2^{2n},$$

and since $2^{1/d} - 1 \geq \log 2/d$ and $1/2^N \leq 2/n$, we obtain

$$\kappa_N \leq \left(\frac{d}{\log 2} \sqrt{2^{2n}}\right)^{1/2^N} \leq \left(\frac{d}{\log 2} \sqrt{2^{2n}}\right)^{2/n} \leq 4(1.45d)^{2/n},$$

proving the result. \square

7. EXAMPLES

Theorem 1 provides an efficient way of computing the distance from a point to an algebraic hypersurface. We illustrate this result by computing the distance from 0 to a family of algebraic hypersurface $\mathcal{Z}_{n,d}$ for positive integer n and d , defined by

$$\mathcal{Z}_{n,d} = \{z \in \mathbb{C}^n : P_{n,d}(z) = 0\}, \quad \text{where } P_{n,d}(z) = \sum_{j=1}^n (1 - z_j)^d - 1.$$

The set $\mathcal{Z}_{n,d}$ is a sphere associated to the d -norm centered in $(1, \dots, 1)$, and its distance from 0 is found to be

$$(10) \quad d(0, \mathcal{Z}_{n,d}) = 1 - n^{-1/d}.$$

Let us prove this formula. If $\|z\| < 1 - n^{-1/d}$, then we have for all j the inequality $|z_j| < 1 - n^{-1/d}$, thus

$$|P_{n,d}(z)| \geq \sum_{j=1}^n |1 - z_j|^d - 1 \geq \sum_{j=1}^n (1 - |z_j|)^d - 1 > \sum_{j=1}^n \frac{1}{n} - 1 = 0,$$

which proves that $P_{n,d}(z)$ does not vanish in the open ball centred in zero of radius $1 - n^{-1/d}$. Thus $d(0, \mathcal{Z}_{n,d}) \geq 1 - n^{-1/d}$. Since the point $z = (1 - n^{-1/d}, \dots, 1 - n^{-1/d})$ belongs to $\mathcal{Z}_{n,d}$, we have finally proved formula 10.

Below are tables giving for several values of n the value of the ratio $r_N/d(0, \mathcal{Z}_{n,d})$ of Theorem t.principal for several values of d and N . The computations were made in Maple.

d	r_0/d	r_1/d	r_2/d	r_3/d	r_4/d
2	0.7673	0.9725	0.9996	1.0000	1.0000
5	0.6525	0.9479	0.9973	1.0000	1.0000
7	0.6325	0.9400	0.9960	0.9999	1.0000
15	0.6067	0.9271	0.9938	0.9999	1.0000

Table 2. Some values of $r_N/d(0, \mathcal{Z}_{n,d})$ for $n = 2$.

d	r_0/d	r_1/d	r_2/d	r_3/d	r_4/d
2	0.6885	0.9386	0.9752	0.9785	0.9910
5	0.5453	0.6859	0.8546	0.9357	0.9610
7	0.5212	0.6475	0.8307	0.9270	0.9535

Table 3. Some values of $r_N/d(0, \mathcal{Z}_{n,d})$ for $n = 3$.

d	r_0/d	r_1/d	r_2/d	r_3/d
2	0.6457	0.7847	0.8759	0.9326
5	0.4891	0.5612	0.7640	0.8311
7	0.4632	0.5268	0.7437	0.8117

Table 4. Some values of $r_N/d(0, \mathcal{Z}_{n,d})$ for $n = 4$.

d	r_0/d	r_1/d	r_2/d	r_3/d
2	0.6180	0.7101	0.8384	0.8831
5	0.4533	0.4970	0.7031	0.7661

Table 5. Some values of $r_N/d(0, \mathcal{Z}_{n,d})$ for $n = 5$.

d	r_0/d	r_1/d	r_2/d	r_3/d
2	0.5832	0.6338	0.8108	0.8224
3	0.4802	0.5108	0.6478	0.7561

Table 6. Some values of $r_N/d(0, \mathcal{Z}_{n,d})$ for $n = 7$.

d	r_0/d	r_1/d	r_2/d	r_3/d
2	0.5534	0.5796	0.6779	0.7561

Table 7. Some values of $r_N/d(0, \mathcal{Z}_{n,d})$ for $n = 10$ and $d = 2$.

These examples show that the bound is quite good for a small value N of Graeffe iterates.

REFERENCES

1. E.H. Bareiss, *Resultant Procedure and the Mechanization of the Graeffe Process*, ACM, **7** (1960), 346-386.
2. J.P. Dedieu, J.C. Yakoubsohn, *Localization of an Algebraic Hypersurface by the Exclusion Algorithm*, AAECC **2** (1992), 239-256.
3. P. Henrici, *Applied and Computational Complex Analysis*, Vol.1, Wiley, New-York, 1974.
4. P. Henrici, I. Gargantini, *Uniformly Convergent Algorithm for the Simultaneous Approximation of all Zeros of a Polynomial*, in *Aspects of the Fundamental Theorem of Algebra*, B. Dejon, P. Henrici editors, Wiley, New-York, 1969.
5. V. Pan, *Solving a Polynomial Equation: Some History and Recent Progress*, Preprint, (1995).
6. A. Schönhage, *The Fundamental Theorem of Algebra in Terms of Computational Complexity*, Manuscript, (1982).
7. P. Turan, *On a New Method of Analysis and its Applications*, Wiley, New-York, (1984).
8. H. Weyl, *Randbemerkungen zu hautproblem der Mathematik 2. Fundamentalsatz der algebra und Grundlagen der Mathematik*, Math. Z. **20** (1924) 131-150.

LAO, Université Paul Sabatier, 31062, Toulouse Cedex, France.

E-mail address: dedieu@cict.fr

INRIA Rocquencourt, 78153, Le Chesnay Cedex, France.

E-mail address: Xavier.Gourdon@inria.fr

LAO, Université Paul Sabatier, 31062, Toulouse Cedex, France.

E-mail address: yak@cict.fr