Vol. 3 No. 2 JOURNAL OF COMPUTATIONAL MATHEMATICS April 1985

THE COMPUTATIONAL COMPLEXITY OF THE RESULTANT METHOD FOR SOLVING POLYNOMIAL EQUATIONS*[1)]

XUAN XIAO-HUA (宣晓华)

(Hangzhou University, Hangzhou, China)

Abstract

Under an assumption of distribution on zeros of the polynomials, we have given the estimate of computational cost for the resultant method. The result is that, in probability $1-\mu$, the computational cost of the resultant method for finding ε-approximations of all zeros is at most

$$cd^2\left(\log d+\log\frac{1}{\mu}+\log\log\frac{1}{\varepsilon}\right),$$

where the cost is measured by the number of f-evaluations. The estimate of cost can be decreased to $c\left(d^2\log d+d^2\log\frac{1}{\mu}+d\log\log\frac{1}{\varepsilon}\right)$ by combining resultant method with parallel quasi-Newton method.

§ 1. Introduction

Generally, search algorithms such as Lehmer's or Kuhn's[1,2] only converge linearly, whereas iterative methods with high order demand an initial approximation which is sufficiently close to the zero. The resultant procedure[3] based on root-squaring process not only converges rapidly, but imposes no restriction on the initial approximation. In the light of this, we estimate the cost of the resultant method for finding all zeros in the sense of probability. To be precise, we shall prove

Main Theorem. *Suppose* $f(z)=a_0z^d+a_1z^{d-1}+\cdots+a_d$ $(a_0\neq 0)$ *is a random polynomial whose zeros are independently uniform random variables on* $[0;R]$[2)]. *Then, for* $0<\varepsilon<\frac{1}{4}$, $0<\mu<\frac{1}{2}$, *in probability* $1-\mu$, *the computational cost of the resultant method for finding* ε*-approximations of all zeros is at most*

$$cd^2\left(\log_2 d+\log_2\frac{1}{\mu}+\log_2\log_2\frac{1}{\varepsilon}\right),$$

where c *only depends on* R, *and the unit of cost is defined as an* f*-evaluation which is turned into* d *multiplications and additions.*

From the theorem, we see that the cost of the method is of loglog ε type, and is a low-degree polynomial in d. As the cost is relatively low, the resultant method is tractable and worth notice.

---

* Received July 21, 1984.

1) Projects supported by the Science Fund of the Chinese Academy of Sciences.

2) $[z;r]$ is the disk with center z and radius r.

§ 2. Elementary Assumption and Computation of Probability

Let C be a complex field. We define the following polynomial set

$$\mathfrak{B}(R)=\{f:\ \partial f=d,\ \text{all zeros } \zeta_i (i=1,\ 2,\ \cdots,\ d) \text{ of } f \text{ satisfy } |\zeta_i|\leqslant R\} \tag{2.1}$$

as a probability space, and propose the following

Elementary Assumption The zeros $(\zeta_1,\ \zeta_2,\ \cdots,\ \zeta_d)$ of a polynomial equation are uniformly independent random variables on $[0,\ R]^d$.

Conventionally, one always supposes that the coefficient of the first term of a polynomial is 1 and other coefficients are independent uniformly random variables on $[0;\ R]^d$, see [4—6]. In practical computation, it is difficult to consider the distribution of the coefficients or zeros of the polynomials to be solved. The study of computational complexity is to give some information about the tractability of the method, the cost function in degree d and approximation error ε.

Assume G is a Lebesgue measurable subset of $\{(z_1,\ z_2,\ \cdots,\ z_d):\ z_i\in\mathbb{C},\ |z_1|<\cdots<|z_d|,\ i=1,\ \cdots,\ d\}$, $\mathfrak{B}(G)$ is a set of the polynomials in $\mathfrak{B}(R)$ whose zero vector, after proper arrangement of the orders of components, is in G. Define the volume of G in a complex field as the volume of the relative set $\mathfrak{B}(G)$, and the probability of $\{f\in\mathfrak{B}(G)\}$ as

$$P\{f\in\mathfrak{B}(G)\}=\frac{\text{vol } G}{\text{vol } \mathfrak{B}(R)}=\frac{\text{vol } G}{(\pi R^2)^a/d!}.$$

Let

$$\mathfrak{D}_\rho(R)=\{f:\ f\in\mathfrak{B}(R),\ \exists\zeta_1\neq\zeta_2,\ f(\zeta_1)=f(\zeta_2)=0,\ \big||\zeta_1|-|\zeta_2|\big|<R\rho\},$$

$$\mathfrak{R}_\lambda(R)=\left\{f:\ f\in\mathfrak{B}(R),\ \exists\zeta_1\neq\zeta_2,\ |\zeta_1|<|\zeta_2|,\ f(\zeta_1)=f(\zeta_2)=0,1-\left|\frac{\zeta_1}{\zeta_2}\right|<\lambda\right\},$$

$$\mathfrak{U}_\alpha(R)=\left\{f:\ f\in\mathfrak{B}(R),\ \exists\zeta_1,\ f(\zeta_1)=0,\ \left|\arg\zeta_1-\frac{k\pi}{2}\right|<\alpha,\ k=1 \text{ or } 3\right\}.$$

From the definition of polynomial sets and a simple computation of volume, the following lemmas can be proved easily.

Lemma 2.1. *Suppose* $\lambda>0$. *Then*

$$\mathfrak{D}_{R\lambda}(R)\supset\mathfrak{R}_\lambda(R).$$

Lemma 2.2.

$$P\{f\in\mathfrak{D}_\rho(R)\}\leqslant 2d^2\rho,\quad P\{f\in\mathfrak{U}_\alpha(R)\}\leqslant\frac{d\alpha}{\pi}.$$

§ 3. The Resultant Method for Solving the Polynomial Equation

Let $f(z)=a_0z^d+a_1z^{d-1}+\cdots+a_d$. Define

$$Tf(z)=f(z)\cdot f^*(z), \tag{3.1}$$

where $f^*(z)=\bar{a}_0z^d+\cdots+\bar{a}_d$. Obviously $Tf(z)$ becomes a polynomial with real coefficients. For convenience, we also write $f(z)$ for $Tf(z)$.

The resultant procedure is divided in two steps: First, compute the moduli of all zeros; second, compute all real zeros and all quadratic factors. Now we are going to give the detail.

Suppose that the zeros $\zeta_1, \bar{\zeta}_1, \zeta_2, \bar{\zeta}_2, \cdots, \zeta_d, \bar{\zeta}_d$ of $f(z)=a_0z^{2d}+a_1z^{2d-1}+\cdots+a_{2d}$ satisfy $|\zeta_1|>|\zeta_2|>\cdots>|\zeta_d|$.

1) Construct the polynomial sequence $\{f^{(i)}(z)\}$, where the zero of $f^{(i)}(z)$ is the 2^i-th power of the relative zero of $f(z)$, that is

$$\zeta_j^{(i)}=\zeta_j^{2^i},\ \bar{\zeta}_j^{(i)}=\bar{\zeta}_j^{2^i},\ f(\zeta_j)=0,\ f^{(i)}(\zeta_j^{(i)})=0,\quad j=1, 2, \cdots, d,\ i=1, 2, \cdots.$$

From the Graeffe process, the coefficients of $f^{(i+1)}(z)$ could be taken as

$$a_j^{(0)}=a_j,\ (-1)^j a_j^{(i+1)}=(a_j^{(i)})^2+2\sum_{l=0}^{\min(2d-j,j)}(-1)^l a_{j-l}^{(i)}\cdot a_{j+l}^{(i)}. \tag{3.2}$$

From the connection between coefficients and zeros, it can be easily proved that

$$\lim_{i\to\infty} 2^{i+1}\sqrt{\frac{a_{2j}^{(i)}}{a_{2j-2}^{(i)}}}=|\zeta_j|,\quad j=1, 2, \cdots, d.$$

So, when i is large enough, we take $q_{i,j}=2^{i+1}\sqrt{\dfrac{a_{2j}^{(i)}}{a_{2j-2}^{(i)}}}$ as the approximation of $|\zeta_j|$ within required precision. We write $q_j=\lim\limits_{i\to\infty} q_{i,j}$.

2) First we check whether $\pm q_j$ are zeros or not. Then determine the quadratic factors. From the algebraic theorem, use the root-square process again to compute all possible approximations of the moduli of zeros for the following equations

$$\Re(p, q_j)=\begin{vmatrix} a_0 & a_1 & \cdots & a_{2d} & 0 \\ 0 & a_0 & \cdots & a_{2d-1} & a_{2d} \\ 1 & p & q_j^2 & & \\ & & \cdots\cdots\cdots & & \\ & & 1 & p & q_j^2 \end{vmatrix}=0,\quad j=1, 2, \cdots, d. \tag{3.3}$$

By some decomposition of the possible quadratic factors and checking, the approximations of all complex zeros can be obtained.

For the convergence, rate of the resultant method the following proposition is given in [7].

Proposition 3.1. Assume the zeros $\zeta_1, \bar{\zeta}_1, \zeta_2, \bar{\zeta}_2, \cdots, \zeta_d, \bar{\zeta}_d$ of $f(z)=a_0z^{2d}+\cdots+a_{2d}$ satisfy $|\zeta_1|>|\zeta_2|>\cdots>|\zeta_d|$ and define

$$|\zeta_j|=q_j,\ \lambda=\max\left|\frac{\zeta_{j+1}}{\zeta_j}\right|,\ \gamma^{(m)}=\frac{2^{2d+1}}{\sqrt{4\pi d}}\lambda^{2^m},\quad j=1, 2, \cdots, d.$$

Then

$$\left|\frac{q_{m,j}-q_j}{q_j}\right|\leqslant\left(\frac{1+\gamma^{(m)}}{1-\gamma^{(m)}}\right)^{\frac{1}{2^{m+1}}}-1,\quad j=1, 2, \cdots, d,\ m\in N.$$

§ 4. The Proof of Theorem

Lemma 4.1. *Under the same hypothesis on $f(z)$ and λ, as in Proposition 3.1, for $0<\varepsilon<\frac{1}{2}$, if*

$$m\geqslant\bar{m}(\varepsilon, d, \lambda)=\left[\log_2\log_2\frac{2^{2d+1}}{\varepsilon\sqrt{4\pi d}}+\left|\log_2\left|\log_2\frac{1}{\lambda}\right|\right|\right], \tag{4.1}$$

then

$$\left|\frac{q_{m,j}-q_j}{q_j}\right|\leqslant\varepsilon,\quad j=1,2,\cdots,d. \tag{4.2}$$

Proof. If m satisfies inequality (4.1), then

$$m\geqslant\log_2\log_\lambda\frac{\varepsilon\sqrt{4\pi d}}{2^{2d+1}},$$

$$\lambda^{2^m}\leqslant\frac{\varepsilon\sqrt{4\pi d}}{2^{2d+1}},\quad 1+\frac{2^{2^m+1}}{\sqrt{4\pi d}}\leqslant 1+\varepsilon.$$

So

$$\left(\frac{1+\gamma^{(m)}}{1-\gamma^{(m)}}\right)^{\frac{1}{2^{m+1}}}\leqslant\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{\frac{1}{2^{m+1}}}\leqslant\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{\frac{1}{8}}\leqslant 1+\varepsilon. \tag{4.3}$$

Combining it with Proposition 3.1, we have

$$\left|\frac{q_{m,j}-q_j}{q_j}\right|\leqslant\varepsilon,\quad j=1,2,\cdots,d.$$

Lemma 4.2. *Suppose the zeros of $f(z)$ satisfy $\theta_j=\min_i|\cos\arg\zeta_i|>0$ and an approximation $q_{m,j}$ of the modulus of a zero satisfies (4.2). Then the total number of Graeffe transformations for finding a $\frac{2\varepsilon}{\theta_j}$ approximation $p_{n,k}$ of $|p|$ of a relative factor is at most $\overline{m}(\frac{\varepsilon}{\varepsilon+\theta_j},d,\lambda')$, where $|p_1|>|p_2|>\cdots>|p_d|$ and $\lambda'=\max_i\left|\frac{p_{i+1}}{p_i}\right|$.*

Proof. Because $q_{m,j}$ satisfies (4.2), from equations $\Re(p',q_{m,j})=0$ (3.3) we can determine some p'. For any p'_k, assume that $\zeta=q_je^{i\varphi}$ is a zero of $f(z)$ which makes the best approximation to $-p'_k$ by $\zeta+\bar{\zeta}$, and write

$$q_{m,j}=(1+\varepsilon)q_j,\quad p=\zeta+\bar{\zeta}.$$

Then (see (7))

$$|p-p'_k|\leqslant\frac{\varepsilon(1+\varepsilon)}{(1+\varepsilon)^2}|\zeta|,$$

$$\left|\frac{p'_k-p}{p}\right|\leqslant\frac{\varepsilon(1+\varepsilon)}{2(1+\varepsilon)^2\theta_j}\leqslant\frac{\varepsilon}{\theta_j},$$

and when $n\geqslant\overline{m}\left(\frac{\varepsilon}{\varepsilon+\theta_j},d,\lambda'\right)$, we have

$$\left|\frac{p'_k-p_{n,k}}{p'_k}\right|\leqslant\frac{\varepsilon}{\theta_j+\varepsilon}.$$

Because $\left|\frac{p'}{p}\right|\leqslant 1+\frac{\varepsilon}{\theta_j}$, combining it with (4.5), we have

$$\left|\frac{p'_k-p_{n,k}}{p}\right|\leqslant\frac{\varepsilon}{\theta_j+\varepsilon}\cdot\frac{\theta_j+\varepsilon}{\theta_j}=\frac{\varepsilon}{\theta_j},\quad\left|\frac{p-p_{n,k}}{p}\right|\leqslant\frac{2\varepsilon}{\theta_j}.$$

Lemma 4.3. *Suppose $q_{m,j}$ is an approximation of q_j and define*

$$\mathfrak{M}_{\varepsilon,j}(R)=\Big\{f:\ f\in\mathfrak{B}(R),\ \text{there exist two zeros } p_1,p_2 \text{ of equation (3.3)},\ \text{satisfy } |p_1|>|p_2|,\ 1-\left|\frac{p_2}{p_1}\right|<\delta\Big\}.$$

Then

$$\frac{\text{vol } \mathfrak{M}_{\delta,J}(R)}{\text{vol } \mathfrak{B}(R)} \leqslant 20\, d^2 |p|^{\frac{1}{2}} \delta^{\frac{1}{4}} (1+R^{-1}), \tag{4.6}$$

where $|p| = \max_i \left(|\zeta_i| + \frac{R^2}{|\zeta_i|} \right)$.

Proof. Because p_1, p_2 are two zeros of equation (3.3), there exist two zeros ζ_1, ζ_2 of $f(z)$ which satisfy

$$p_1 = \zeta_1 + \frac{q_{m,J}^2}{\zeta_1}, \quad p_2 = \zeta_2 + \frac{q_{m,J}^2}{\zeta_2}.$$

For a fixed ζ_1, write $\zeta_2 = x+yi$. Then from $|p_2| = (1-\sigma)|p_1| (\sigma < \delta)$, we have a plane algebraic curve

$$P_\sigma: \qquad (x^2-y^2+q_{m,J}^2)^2 + 4x^2y^2 - |p_1|(x^2+y^2) = 0. \tag{4.7}$$

From the theory of algebraic geometry, the length $l(P_0 \cap [0; R])$ of $P_0 \cap [0; R]$ is less than $5\pi R$. From the effect of coefficients on zeros, it is known that for any $\sigma < \delta$, all points of $P_\sigma \cap [0; R]$ are in the region

$$\{(x, y): \max(|x-x_0|, |y-y_0|) \leqslant \{3(1+R)^4 \delta |p_1|^2\}^{\frac{1}{4}}, (x_0, y_0) \in P_0 \cap [0; R]\},$$

and the volume of the region is at most $10\pi R(R+1)\delta^{\frac{1}{4}} |p|^{\frac{1}{2}}$. Because there are at most d zeros whose moduli are different, it is easy to get (4.6).

Proof of the main theorem. Suppose $0 < \mu < \frac{1}{2}$, $0 < \varepsilon < \frac{1}{4}$. Define

$$\mathfrak{M}_{\rho_0, \alpha_0}(R) = \mathfrak{D}_{\rho_0}(R) \cup \mathfrak{U}_{\alpha_0}(R),$$

where $\rho_0 = \frac{\mu}{8d}$, $\alpha_0 = \frac{\pi\mu}{4d}$. From Lemma 2.2, it follows that

$$P\{f \in \mathfrak{M}_{\rho_0, \alpha_0}(R)\} = \frac{\text{vol } \mathfrak{M}(R)}{\text{vol } \mathfrak{B}(R)} \leqslant \frac{\mu}{4} + \frac{\mu}{4} = \frac{\mu}{2},$$

and when $f \in \mathfrak{M}_{\rho_0, \alpha_0}(R)$, we have $|\lambda| < 1-\rho_0$. Combining Lemmas 4.1, 4.2 with 4.3 and $\left| \log \frac{1}{1-\mu} \right| \leqslant \frac{2\mu}{1-\mu}$, it is true that

i) the total number of Graeffe processes for computing $\frac{\varepsilon}{1+\varepsilon}$-relative approximations of the moduli of zeros is at most

$$O\left(\log_2 d + \log_2 \frac{1}{\mu} + \log_2 \log_2 \frac{1}{\varepsilon} \right);$$

ii) for a $\frac{\varepsilon}{1+\varepsilon}$-approximation of the modulus of a zero, define

$$\delta_0 = \left\{ \frac{\mu}{80\, d^4 (1+R)\left(1+\sqrt{\frac{4d}{\mu R^2}}\right)} \right\}^4.$$

When

$$f \in \left\{ f: f \in \bigcup_J \mathfrak{M}_{\delta_0, J} \text{ or } \exists \zeta_1, f(\zeta_1) = 0, |\zeta_1| < \sqrt{\frac{\mu R^2}{4d}} \right\} \triangleq \mathfrak{N}_{\delta_0},$$

then $\lambda' < 1-\delta_0$ (see Lemma 4.2). So the total number for computing an ε-relative approximation of a $|p|$ is at most $O\left(\log_2 d + \log_2 \frac{1}{\mu} + \log_2 \log_2 \frac{1}{\varepsilon} \right)$, and $P\{f \in \mathfrak{N}_{\delta_0}\} \leqslant \frac{\mu}{2}$;

iii) the amount of arithmetic operation of a Graeffe transformation equals c_1d^2, and that of writing in general form the polynomial defined by a determinant (see (3.3)) equals c_2d^2; the evalution takes less operations. Besides, the test of the zeros requires at most c_3d^2 arithmetic opration.

In summary, in probability $1-\mu$, the computational cost for obtaining ε-relative approximations of all moduli of zeros and $|p|$ by the resultant method is at most

$$cd^2\left(\log_2 d+\log_2\frac{1}{\mu}+\log_2\log_2\frac{1}{\varepsilon}\right).$$

Because the order of the cost in d, $\frac{1}{\mu}$, $\frac{1}{\varepsilon}$ in the above estimate gives the order of d, $\frac{1}{\mu}$, $\frac{1}{\varepsilon}$ of the cost for computing all ε-approximations of zeros, only the constants c depending on R are different. So the main theorem holds readily.

Remark. If one thinks that d^2 loglog $\frac{1}{\varepsilon}$ in the estimate of the cost increases too fast as d increases, one may combine the resultant method with the parallel quasi-Newton method[8,9], with the estimate of the cost at most

$$c\left(d^2\log d+d^2\log_2\frac{1}{\mu}+d\log_2\log_2\frac{1}{\varepsilon}\right).$$

Under the assumption of uniform distribution on the coefficients of the polynomials, the estimate of the cost for the Lehmer-Newton method is relatively low the estimate is $c\left(d^3+d^2\log\frac{1}{\mu}+d\,\text{loglog}\frac{1}{\varepsilon}\right)$.

Acknowledgment. The author wishes to thank Prof. Wang Xing-hua for his useful suggestions and Prof. Wu Shao-ping for her help during the preparation of this paper.

References

[1] D. H. Lehmer, A machine method for solving polynomial equations, *J. Assoc. Comp. Math.*, **8** (1961), 151—162.

[2] H. W. Kuhn, Fixed Point Algorithms and Applications (edited by S. Karamadian), Academic Press, New York, 1977, 11—40.

[3] E. H. Bareiss, Resultant procedure and the mechanization of Graeffe process, *Journal ACM*, **7** (1960), 346—386.

[4] S. Smale, The fundamental theorem of algebra and computational complexity theory, *Bulletin AMS*, **4** (1981), 1—36.

[5] Wang Ze-ke, Xu Sen-lin, Approximation zercs and computational complexity theory, *Scientia Sinica*, **27** (1984), 566—575.

[6] Wang Xing-hua, Xuan Xiao-hua, Random polynomial space and computational complexity theory (to appear).

[7] A. Ralston, H. S. Wilf, Mathematical Methods for Digital Computer, Vol. 2, John Wiley & Sons Inc., 1968, 223—258.

[8] K. Weierstrass, Neuer Beweis des Satzess, dass jede Garze Rationale Function einer Veräderlichen dargestellt werden Kanr als ein Product aus Lineare Function dersellben Veränderlichen, Ges. Werke, Vol. 3, 1903, 251—269.

[9] Wang Xing-hua, Zhen Shi-ming, The quasi-Newton method in parallel circular iteration (to appear).