On the separation of the roots of a polynomial

(extended abstract)

by Maurice MIGNOTTE
University of Strassbourg

In a recent paper COLLINS and HOROWITZ [1] considered the following problem: Let P be a polynomial with rational integer coefficients. If sep (P) is the minimum distance between distinct roots of P, find a good lower bound for sep (P). This question is important for the algorithms which calculate the roots of a polynomial (see [1] for a more detailed discussion).

Our first result in [2] is:

THEOREM 1. - If $P = a_0 X^d + \dots + a_1$ is a Polynomial over $\mathbb{Z}$, without multiple roots, then

$$\text{sep}(P) > \sqrt{3}\, d^{-(d+2)/2} \left(|a_0|^2 + \dots + |a_d|^2\right)^{-(d-1)/2}.$$

The proof uses the following important inequality. If $z_1, \dots, z_d$ are the roots of P then

$$\max(|z_1|, 1) \dots \max(|z_d|, 1) \le \left(|a_0|^2 + \dots + |a_d|^2\right)^{1/2}.$$

(A proof of it can be found for example in [3].)

Next we study another function defined in [1]

$$L(d, H) = \operatorname{Min}\{\text{sep}(P);\ P \in \mathbb{Z}[X] \text{ without multiple roots, } \deg P = d,\ H(P) \le H\},$$

where $H(P) = \max |a_i|$.

It is easy to see that $L(2, H)$ satisfies

$$H^{-1} \ll L(2, H) \ll H^{-1}$$

(where $f(x) \ll g(x)$ means that there is a positive constant C such that $f(x) \le C\, g(x)$).

We prove the relations

$$H^{-2} \ll L(3, H) \ll H^{-2},$$

which settle a problem of [1].

This leads us to consider the function

$$L(d) = \limsup\, (-\operatorname{Log} L(d, H)/\operatorname{Log} H).$$

Using a deep result of W. SCHMIDT ([4], th. 7.I) about approximation of algebraic numbers by algebraic numbers of smaller degree we prove

THEOREM 2. - The function $L(d)$ satisfies

$$[(d+1)/2] \le L(d) \le d-1.$$

But, as Professor COLLINS pointed out to me, it is more interesting to consider the function $L_0(d)$, similar to $L(d)$, where only irreductible polynomials are considered. We are unable to prove a non trivial lower bound of $L_0(d)$.

When we consider only reducible plynomials the function $L_1(d)$ (similar to $L(d)$) satisfies

$$L_1(d) = [(d+1)/2].$$

(We use another theorem of W. SCHMIDT ([4], th. 7. H.). This result is not proved in [2].)

REFERENCES

[1] G. E. COLLINS, E. HOROWITZ. - The minimum root separation of a polynomial, Math. Comp., 28, Nr. 126, 1974, 589-597

[2] M. MIGNOTTE.- Sur la complexité de certains algorithmes où intervient la séparation des racines d'un polynôme (to appear in the Revue d'Automatique, Informatique, Recherche Opérationelle).

[3] M. MIGNOTTE.- An inequality about factors of polynomials, Math. Comp. 28, 1974, 1153-1157.

[4] W.M. SCHMIDT.- Approximation to algebraic numbers, Monographie Nr. 19 de l'Enseignement Mathématique, Genève, 1972.

Abstracts

ANALYSIS OF THE SUBTRACTIVE ALGORITHM FOR GREATEST COMMON DIVISORS, by C.C. Yao, D.E. Knuth, Computer Science Department, Stanford University, STAN-CS-75-510, Sept. 1975

Abstract

The sum of all partial quotients in the regular continued fraction expansions of m/n, for $1 \le m \le n$, is shown to be $6\pi^{-2}\, n(\ln n)^2 + O(n \log n(\log \log n)^2)$. This result is applied to the analysis of what is perhaps the oldest nontrivial algorithm for number-theoretic computations.

ON COMPUTING THE TRANSITIVE CLOSURE OF A RELATION, by James Eve, Computer Science Department, Stanford University, STAN-CS-75-508, September 1975

Abstract

An algorithm is presented for computing the transitive closure of an arbitrary relation which is based upon a variant of Tarjan's algorithm [4] for finding the strongly connected components of a directed graph. This variant leads to a more compact statement of Tarjan's algorithm.

If V is the number of vertices in the directed graph representing the relation than the worst case behavior of the proposed algorithm involves $O(V^3)$ operations. In this respect it is inferior to existing algorithms [1,2] wich require $O(V^3/\log V)$ and $O(V^{\log_2 7} \log V)$ operations respectively. The best case behavior involves only $O(V^2)$ operations.

FAST ALGORITHMS FOR MANIPULATING FORMAL POWER SERIES, by R.P. Brent, H.T. Kung, Department of Computer Science, Carnegie-Mellon University, January 1976

Abstract

The classical algorithms require $O(n^3)$ operations to compute the first n terms in the reversion of a power series or the composition of two series, and $O(n^2 \log n)$ operations if the fast Fourier transform is used for power series multiplication. In this paper we show that the composition and reversion problems are equivalent (up to constant factors), and we give algorithms which require only $O((n \log n)^{3/2})$ operations. In many cases of practical importance only $O(n \log n)$ operations are required. An application to root-finding methods which use inverse interpolation is described, some results on multivariate power series are stated, and several open questions are mentioned.