# REAL ROOT ISOLATION FOR ALGEBRAIC POLYNOMIALS

Siegfried M. Rump
University of Karlsruhe
Fakultät Informatik

7500 Karlsruhe

Several algorithms are known to separate the real zeros of a polynomial. In his thesis Heindel [He70] showed, that the computing time of his algorithm using Sturm sequences is polynomially bounded in the length of the coefficients. The polynomials are assumed to have integral coefficients. In his Diplomarbeit [Lü76] Lüdicke gave a modified Sturm algorithm for real algebraic polynomials with a polynomially bounded, but very high computing time. He described and analyzed the algorithm, but did not implement it. In the present paper we extend the Collins/Loos - algorithm [CL76] from integral to real algebraic coefficients and gain empirical computing times.

To achieve a real algebraic number field $Q(\alpha)$ over the rationals we assume an integral polynomial $\Psi \in Z[x]$ with $\Psi(\alpha)=0$ and an interval $\Omega$ with rational endpoints to be given, which contains exactly one real root of $\Psi$, namely $\alpha$. Every real algebraic number $A \in Q(\alpha)$ can be represented by

$$A = \sum_{i=0}^{n_\Psi -1} a_i \cdot \alpha^i, \qquad a_i \in Q.$$

From now on an indexed n like $n_\Psi$ denotes the degree, an indexed d the size of the index-polynomial. We note, that $\Psi$ is not assumed to be irreducible and therefore the representation need not to be unique.

For arithmetical operations in $Q(\alpha)$ and $Q(\alpha)[y]$ Rubald gave several algorithms [Rb74] including gcd-operations. Our main algorithm relies heavily on sign determinations, which are of course trivial over the integers but by no means over an algebraic number field $Q(\alpha)$ if one insists on infallability in all cases. We give a sequence of algorithms for algebraic sign calculation where the maximum computing time of

$$t_{ASIGN}(\alpha,A) \lesssim n_\Psi^5 \cdot \{\log(d_A)^3 + \log(d_\Psi)^3\} + 1$$

is better than the result

$$t \lesssim n_\Psi^9 + n_\Psi^6 \cdot \{\log(d_A)^3 + \log(d_\Psi)^3\} + 1$$

of Rubald. For one of the sign-algorithms interval arithmetic is used.

Several algorithms are written to get coercions of algebraic types.

A binary rational is a rational number, where the denominator is a power of 2. It turned out, that throughout the main-algorithm only binary rationals are needed. So a special binary arithmetic is given with essential improvements in theoretical and practical (up to factor 6) computing times over rational arithmetic.

Algorithms are given for efficient evaluation of $P(r)$, $P \in Q(\alpha)[y]$ and $r \in Q$.

Some improvements in estimating the

minimum root separation of an integral polynomial $P \in Z[x]$ were made. The asymptotically best result for not necessarily squarefree polynomials was

$$\log\{sep(P)^{-1}\} = O(n_P^2 + n_P \cdot \log(d_P)),$$

see [CH73], [Mi76]; we proved

$$\log\{sep(P)^{-1}\} = O\{n_P \cdot \log(n_P) + n_P \cdot \log(d_P)\}.$$

Such estimates are crucial for a tight time analysis of root isolation algorithms. For $P \in Q(\alpha)[y]$ we found

$$\log\{sep(P)^{-1}\} =$$

$$O\{n_\psi \cdot n_P \cdot (\log(n_P) + n_\psi \log(d_\psi) + n_\psi \log(d_P)\},$$

and a root bound

$$|\beta| < d_\psi^{n_\psi} \cdot d_P^{2n_\psi} \quad \text{for } P(\beta) = 0.$$

The last estimation is not trivial, because the leading coefficient of P may be very small.

All algorithms are described and analyzed in detail. The main algorithm could be improved in some aspects. One gcd and one division of polynomials over $Q(\alpha)$ were saved, and, in case $P^{(i)}$ has only simple zeros one more gcd operation is saved; and this for each derivative, i.e. $n_P$ times. These operations are very time consuming. Moreover an improvement of the theoretical computing time was possible.

The main algorithm has a maximum computing time of

$$t \preceq n_\psi^{13} \cdot n_P^{9} \cdot \max\{\log(d_P), \log(d_\psi)\}^4 + 1$$

compared with

$$t \preceq n_\psi^{38} \cdot n_P^{24} \cdot \log(d_P)^{19} \cdot \log(d_\psi)^{22} + 1$$

of Lüdicke [Lü76].

Furthermore several computing examples are given showing how the computing time depends on the various input parameters. Here a high dependence was observed on the degree of P, a smaller dependence on the degree of $\psi$ and $(d_P, d_\psi)$.

A detailed description, the Diplomarbeit and all algorithms as FORTRAN-card deck or on magnetic tape are available from the author. The algorithms can be used as a subsystem of SAC-1.

Acknowledgement. I thank Prof. R. Loos for several discussions.

REFERENCES

[CH73] Collins, G.E. and Horowitz, E., Minimum Root Separation of a Polynomial, Math. Comp., Vol.28, Nr.126, 1976

[CL76] Collins, G.E. and Loos, R.G.K., Polynomial Real Root Isolation by Differentiation, Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation, p. 15, New York 1976

[He70] Heindel, L.E., Algorithms for exact Polynomial Root Calculation, Ph.D. Thesis, Computer Science Department, University of Wisconsin, Madison, Wisconsin 1970

[Lo76] Loos, R.G.K., private communication

continued on page 13

## RADICAL SIMPLIFICATION MADE EASY

Richard E.B. Zippel

Abstract: In this paper we summarize some of the major results of the author's thesis concerning the simplification of radicals. We present techniques which permit linearly independent bases for fields involving nested radicals to be constructed and present results which may be used to de-nest expressions involving nested radicals.

## SYMBOLIC MANIPULATION TECHNIQUES FOR VIBRATION ANALYSIS OF LAMINATED ELLIPTIC PLATES

C.M. Andersen and Ahmed K. Noor

Abstract: A vibration analysis of laminated anisotropic plates of elliptic planform is carried out using a Rayleigh-Ritz technique implemented with the aid of the MACSYMA algebraic manipulation system. For this problem MACSYMA analytically performs a large number of differentiations and integrations and outputs its results in the form of Fortran code for defining the elements of two large matrices. The block of Fortran code so generated is used for determining both the vibration frequencies and the derivatives of the vibration frequencies with respect to various material and geometric parameters. Symmetries play a significant role in reducing the amount of symbolic computation needed.

Continued from page 3

[Lü76] Lüdicke, L., Diplomarbeit, Frankfurt 1976

[Mi76] Mignotte, M., Some Problems about Polynomials, Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation, August 1976, p.227

[Rb74] Rubald, C.M., Algorithms for Polynomials over Real Algebraic Number Field, Ph.D. Thesis, Computer Science Technical Report Nr. 206, January 1974

[Ru76] Rump, S., On the Sign of a Real Algebraic Number, Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation, p. 238, New York 1976

[Ru76] Rump, S., Isolierung der Reellen Nullstellen algebraischer Polynome, Bericht der Arbeitsgruppe Computer Algebra, 10, Fachbereich Informatik Kaiserslautern, November 1976, 121 Seiten