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 $\Psi \in \mathbb{Z}[x]$ with $\Psi(\alpha) = 0$ and an interval $I$ 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

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

For arithmetical operations in $Q(\alpha)$ and $Q(\alpha)[y]$ Kubald gave several algorithms [Ku74] 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 infallibility in all cases. We give a sequence of algorithms for algebraic sign calculation where the maximum computing time of

$$t_{\text{ASIGN}}(\alpha, A) \leq n_\Psi^5 \cdot \log(\delta_A)^3 + \log(\delta_\Psi)^3 + 1$$

is better than the result

$$t \leq n_\Psi^9 + n_\Psi^6 \cdot \log(\delta_A)^3 + \log(\delta_\Psi)^3 + 1$$

of Kubald. 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 $r \in \mathbb{Q}$.

Some improvements in estimating the
minimum root separation of an integral polynomial \( p \in \mathbb{Z}[x] \) were made. The asymptotically best result for non-necessarily squarefree polynomials was

\[
\log(\text{sep}(p)^{-1}) = O\left(n_p^2 \log(d_p)\right),
\]

see [Ch73], [Hi76]; we proved

\[
\log(\text{sep}(r)^{-1}) = O\left(n_p \log(n_p) + n_p \log(d_p)\right).
\]

Such estimates are crucial for a tight time analysis of root isolation algorithms. For \( p \in \mathbb{C}[x] \) we found

\[
\log(\text{sep}(p)^{-1}) = O\left(n_p \cdot \log(n_p) + n_p \log(d_p) + n_p \log(d_p)\right),
\]

and a root bound

\[
|\alpha| < d_p^{n_p} \cdot 2^{n_p} \quad \text{for} \quad p(\alpha) = 0.
\]

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 idea and one division of polynomials over \( \mathbb{C}[x] \) were saved, and, in case \( p(1) \) 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

\[
t \leq n_p^{13} \cdot \min\{\log(d_p), \log(d_p)\}^4 + 1
\]

cmpared with

\[
t \leq n_p^{24} \cdot \log(d_p)^{19} \cdot \log(d_p)^{22} + 1
\]

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 \( q \) and \( (d_p, \omega) \).

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


[Lo76] Loos, R.C.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 platform 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


[Ru76] Rump, S., Isolierung der Reellen Nullstellen algebraischer Polynome, Bericht der Arbeitsgruppe Computer Algebra, 18, Fachbereich Informatik Kaiserslautern, November 1976, 121 Seiten