On the Sign of a Real Algebraic Number

Siegfried Rump
Universität Kaiserslautern

March 1976

Abstract

In an ordered algebraic extension field of the rationals algorithms for sign determinations are studied. Two new algorithms are analyzed in detail and shown to be asymptotically and in practice faster than previous algorithms.

1. Introduction

Let Z denote the ring of integers and Q the field of rationals. In a pure algebraic sense an algebraic number α over Q may be represented by its minimal monic polynomial $\psi \in Q[x]$, $\psi(\alpha) = 0$. It is possible [1,2] to perform constructively the four rational operations in $Q(\alpha)$ using only ψ to characterize α and the same holds for operations composed of the four rational operations like greatest common divisor calculation and factorization. There are, however, circumstances where one has to distinguish between an algebraic number α and its conjugates belonging to the same ψ. Very important is the case that the field is ordered like Q and the order relation has to be extended to $Q(\alpha)$. Obviously, ψ is not sufficient to characterize α anymore. Zassenhaus proposed and realized in his real root calculus [3] an indexing from left to right of the real algebraic numbers of a minimal ψ and denotes the roots by $\alpha(\psi,1), \alpha(\psi,2),\ldots,\alpha(\psi,r)$ if ψ has r distinct real roots. The sign determination of an element $\beta \in Q(\alpha)$ as the base for the order relation depends in general on all real roots of φ, $\varphi(\alpha) = \beta$, and ψ. We call such an algorithm based on all real roots of φ a global algorithm for sign determination.

In section 2 we state the problem more formally and discuss global algorithms. Using another indexing method which was introduced by Heindel [4] based on isolating intervals we describe and analyze in section 3 and 4 two new algorithms which are not global in the stated sense. In section 5 we give empirical comparisons and discuss finally applications of the given algorithms for real root isolation of real algebraic polynomials.

2. Global Algorithms

Some of the restrictions we use in the formal statement of the problem will be lifted later for reasons of computational convenience. If ψ is the minimal polynomial over $Q[x]$ such that $\psi(\alpha) = 0$ then every element $\beta \in Q(\alpha)$ can be represented by a polynomial $B \in Q[x]$ of degree $n_B \leq n_\psi - 1$. Let us denote by Ω an interval with rational endpoints r and s such that $\alpha \in \Omega$ but no other real root of ψ is contained in Ω. Ω is called an isolating interval for α with respect to ψ. Since ψ is minimal, $\gcd(\psi,B) = 1$ if $B \neq 0$. Therefore $\beta = 0$ is represented by $B = 0$, the null polynomial, and the problem of sign determination is reduced to the non-zero sign of β, hence to sign $(B(\alpha)) \gtrless 0$ (Figure 1).

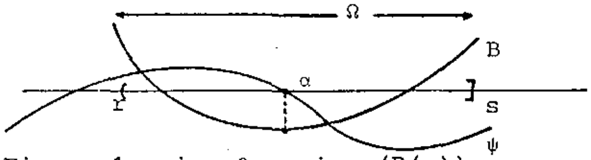

Figure 1 sign β = sign $(B(\alpha))$

For the indexing method of Zassenhaus a solution using Sturm sequences was given by Kempfert [11], and for Collins' method of isolating intervals by Rubald [2]. Rubald's algorithm counts the number of real roots of B in Ω and bisects Ω with respect to α until Ω does not contain a root of B anymore. Then sign (β) = sign $(B(r))$ = sign $(B(s))$. The Sturm sequence is generated once and evaluated repeatedly for each new Ω. We call this algorithm the S-algorithm (for Sturm sequence) which is available in the SAC-1 system [2] for computer algebra.

Recently two algorithms were discovered which can be used as alternatives to Sturm's method. The first one [5] isolates the real roots of a polynomial using the sequence of derivatives, the second one [6] is based on an idea of Uspensky and uses polynomial transformations and Descarte's sign rule. Both algorithms can be easily adapted for an arbitrary interval like Ω. Both algorithms are in general superior to Sturm's algorithm and it can be expected that sign algorithms based on them are also superior to the S-algorithm.

Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation

The global algorithms can be described as follows

```
s ← ASIGNG(α,B)

[Algebraic sign, global algorithm. $\alpha=(\Omega,\psi)$,
 $\beta=B(\alpha)$. s=sign(β)]
(1) [β=0?] if B=0 then set s=0 and stop.
(2) [Isolating intervals] Let $I_1,\ldots,I_{r_B}$ be
     the isolating intervals of B, using
     one of the three mentioned algorithms.
(3) [Bisect] while there are intervals
     $I_n,\ldots,I_m$ such that $I_i \cap \Omega \neq \emptyset$, $n \leq i \leq m$, do
     {bisect Ω with respect to ψ and $I_n,\ldots,$
     $I_m$ with respect to B}.
(4) [Sign] Set s=sign(B(r)), where $\Omega=(l,r)$
     and stop.
```

3. The Interval Algorithm and the Derivative Algorithm

If B≠0 then there exists a lower bound b on (B(α)) which we will give in the next section. Also let us define the interval $Y=B(\Omega)$ by evaluating the polynomial B using interval addition, subtraction and multiplication. A sequence of intervals $\Omega=\Omega_1,\Omega_2,\ldots,\Omega_m$ bisected with respect to ψ such that $\alpha \in \Omega_i$, results by $Y_i=B(\Omega_i)$ in a sequence of intervals $Y_1,\ldots,Y_m$, with $B(\alpha) \in Y_i$ and $\Omega_{i+1} \subset \Omega_i$, $Y_{i+1} \subset Y_i$ for $i=1,\ldots,m-1$. Since the width of the intervals in both sequences decreases monotonically m can be choosen such that the width of Y_m is less then the bound b. Hence $0 \notin Y_m=(l,r)$ and sign (B(α))=sign(r). This leads to the following algorithm [7]

```
s ← ASIGNI(α,B)

[Algebraic sign using interval arithmetic.
 $\alpha=(\psi,\Omega)$, $\beta=B(\alpha)$. **s=sign(β)**]  ,
(1)[β=0?] if B=0 then set s=0 and stop.
(2)[Bisect] Y←B(Ω); while $0 \in Y$ do {bisect
    Ω with rεspect to ψ and set Y←B(Ω)
    using interval arithmetic}.
(3)[Sign] Let Y=(l,r); Set S=sign(l) and
    stop
```

Although ASIGNI turns out to be asymptotically and in practice faster than the S-algorithm there is still another method empirically more attractive.

The algorithm is based on the following observation. If the derivative $B'(x)=dB/dx$ has no real root in Ω , then B has by Rolle's Theorem at most one real root in Ω , which is of multiplicity 1 if it exists. Then the sign of B is different on the endpoints of Ω. (The case that Ω is of width 0 means that $\alpha \in Q$ ans may be trivially excluded). Bisecting Ω with respect to ψ until the signs of B at the endpoints agree results in an interval Ω on which B is of the same sign. It remains to enforce the hypothesis. This can easily be accomplished inductively because the n_B-th derivative of B is a non-zero constant.

```
s ← ASIGND(α,B)
[Algebraic sign using derivatives.$\alpha=(\psi,\Omega)$,
 $\beta=B(\alpha)$. s=sign(β)]
(1) [β=0?]if B=0 then set s=0 and stop.
(2) [Derivative sequence] Let $B^{(o)}$
     $B^{(1)},\ldots,B^{(n_B)}$ be the derivative
     sequence of B.
(3) [Induction] for $k=n_B,n_B-1,\ldots,0$ do
     with $\Omega=(l,r)$ {while sign
     $(B^{(k)}(l)) \neq$ sign $(B^{(k)}(r))$
     bisect Ω with respect to ψ}.
(4) [Sign] Set s = sign(B(r)) and stop.
```

The algorithm as stated is only correct for minimal ψ. This restriction can easily be lifted.

4. Theoretical Analysis

The assumptions made in the actual implementation are the following. ψ is not assumed to be irreducible since there exists no complete factorization algorithm with a polynomial bound on the computing **time**. Instead ψ is assumed to be squarefree, and primitive since $\psi \in Z[x]$. B is assumed to be relatively prime to ψ, otherwise B=0. B is split into a rational number r_B and a primitive polynomial $\overline{B} \in Z[x]$. Since $r_B > 0$ only $\overline{B}$ is of interest in the algorithm.

We denote by L(a) the length of the integer a, by L(r)=max{L(a),L(b)} the length of the rational r=a/b reduced to lowest terms and by L(I)=max{L(l),L(r)} the length of the interval Ω=(l,r) with rational endpoints l and r. The width $W(\Omega)=|r-l|$ is distinguished from L(Ω). Finally, the integral polynomial A is characterized by its degree n_A and its sum norm $d_A=\Sigma_{0 \leq i \leq n_A} |a_i|$ where the a_i are the coefficients of A.

Let the interval (-a,a] contain all real roots of $B \in Z[x]$. If a is an integer all intervals occuring in the algorithms generated by bisection of such an initial interval have binary rational endpoints,i.e. the denominator is a power of 2. Binary rational arithmetic is much cheaper than rational arithmetic. For the bisection of the intervals Collins' [5] method of minimizing the length of the numerators and denominators is employed.

The analysis of algorithm ASIGNG gives for step 2

$$t_2 \precsim n_B^{10} + n_B^7 \, L(d_B)^3$$

for Sturm and derivate sequence [4,5].

and $t_3 \preceq t_2$ by the argument in [5] for algorithm R if $L(d)=\max\{L(d_B),L(d_\psi)\}$. Hence, for $n_\psi = n > n_B$,

$$t_{ASIGNG} \preceq n^{10} + n^7 L(d)^3.$$

In practice, one does not have to generate all isolating intervals in step 2 in the S-algorithm, if one bisects Ω until it contains only the nearest root of B to α. Then only one applies step 3. With this improvement Rubald´s S-algorithm has the time

$$t_S \preceq n^9 + n^6 L(d)^3.$$

The use of the stronger result of Mignotte [12], [13] does not affect this time.

If in step 2 the modified Uspensky algorithm is used we have

$$t_{ASING} \preceq n^8 + n^6 L(d)^2 + n^5 L(d)^3.$$

where the second term is due to step 3.

The analysis of the interval algorithm ASIGNI is based on Theorem 5 of [5] which gives the lower bound

$$|B(\alpha)| > \frac{1}{2}\,(d_B+1)^{-n_\psi} d_\psi^{-n_B}$$

and on the relation between the width of $Y = B(\Omega)$ and of Ω

$$W(Y) < n_B \omega^{n_B-1} d_B \cdot W(\Omega)$$

where $\omega = \max\{|r|,|l|\} + W(\Omega) + 1, \Omega=(l,r]$.

<u>Theorem</u> Let $\alpha = (\psi,\Omega), \beta = B(\alpha) \neq 0$,
$n = n_\psi > n_B$, $d = \max\{d_\psi,d_B\}$
Then $t\ (ASIGNI,\alpha,B) \preceq n^5 L(d)^3$ and
$t\ (ASIGND,\alpha,B) \preceq n^8 + n^5 L(d)^3$.

For algorithm ASIGND it is not obvious that no root of the derivatives coincides with α. This cannot happen if ψ is minimal; otherwise by calculating the $\gcd(\psi,B^{(k)})$ ψ can always be made relatively prime to $B^{(k)}$, $0 < k < n_B$. Even without assuming a minimal ψ we get the stated result for ASIGND. Collins and Horowitz [14] have shown, that a square free polynomial with degree n and sumnorm d_1 have a minimum root separation λ with $L(\lambda^{-1}) \preceq n \cdot L(d)$. One can show, that this result still holds for the distinct roots of a polynomial with possibly multiple roots. It is conjectured, that the minimum real root separation of a polynomial as given by the formula is also a minimum real root separation for all the derivatives. This has not yet been proved and in the derivation of the computing time of ASIGND a λ, with $L(\lambda^{-1}) \preceq n^2 + nL(d)$, is used as a minimum root separation for all derivatives contributing to the term n^8 in the result. Detailed proofs will be contained in [8].

<u>5. Empirical Analysis</u>

For Rubald´s S-algorithm, ASIGNI and ASIGND we give in the following tables in columns S, I and D times in seconds of a TR 440 computer using SAC-1 [9]. For each algorithm we give also under B the number of bisections. Since we took the average of three randomly generated polynomials for each entry B is a fraction. With the exception that Ω is initially sufficient small that no bisections are needed at all, algorithm ASIGND is clearly superior to ASIGNI and both are faster than the Sturm sequence algorithm. The efficient modification of Uspensky´s algorithm became only known while this note was written. Therefore, no tests could be included. b denotes the length of the coefficients in bits, n the degree of the polynomials, ψ has always 44 bit (1 word on TR 440) coefficients and degree n + 1.

Table 1 - Random Polynomials, b = 44

n	S	B	I	B	D	B
5	2.8	10.3	2.6	10.6	1.0	13.6
10	21.2	12.3	6.1	12.0	1.5	12
10 ⁎)	9.7	0	0.6	0	1.09	2
15	46.0	3	7.5	11.7	3.3	15.3
20	-	-	13.4	15.3	4.4	15.3
20 ⁎)	140	1.3	4.63	3.1	4.60	3.3

⁎) Ω three orders of magnitude smaller

Table 2 - Random Polynomials, n = 10

b	S	B	I	B	D	B
44	12.8	10.3	4.8	11	1.4	12.3
88	38	12	5.7	12.3	1.7	13.3
132	66	8.3	6.0	11	1.4	11
176	97	7.7	6.6	12.7	1.9	13

Table 3 - Random Resultants

n	S	B	I	B	D	B
8	5.4	8	2.7	8	0.86	11
18	179	10	9.6	10	4.1	18

Table 4 - Random Products, b = 44

n	S	B	I	B	D	B
5	4.7	13	3.3	16	0.75	13
10	26	12	6.3	15	1.48	13
15	85	13	20.1	31	3.1	18

Table 5 - Chebyshev Polynomials

n	S	B	I	B	D	B
5	2.9	12	2.2	14	0.68	14
10	10.9	11	3.6	11	0.83	11
15	25	10	7.1	14	1.73	13

6. Conclusion

We have shown that two new algorithms are theoretically and practically faster than previous known algorithms, based on Sturm sequences. We expect this also being true compared to Zassenhaus´ method of indexing because Kempfert´s algorithm relies also on Sturm sequences. The main attraction to study the sign determination for real algebraic numbers is its application for real root isolation of real algebraic polynomials [8]. In particular the real root isolation algorithms based on derivative sequences or Descarte´s sign rule make havily use of sign calculations and can easily be extended from $Z[x]$ to $Q(\alpha)[x]$. In contrast, the calculation of Sturm sequences over $Q(\alpha)$ is even worse than over Z.

References

[1] G. E. Collins, Computer Algebra of Polynomials and Rational Functions, Amer. Math. Monthly 80, (Aug.-Sept. 1973), 725-754

[2] C. R. Rubald, Algorithms for Polynomials over a Real Algebraic Number Field, Computer Sciences Dep., University of Wisconsin, Madison Techn. Report No. 206, Jan. 1974

[3] H. Zassenhaus, A Real Root Calculus, Proceedings of a Conference held at Oxford, (Aug.-Sept. 1967), 383-393

[4] L. E. Heindel, Integer Arithmetic Algorithms for Polynomial Real Zero Determination, J. ACM, 18 (Oct.1971), 533-548

[5] G. E. Collins, R. Loos, Polynomial Real Root Isolation by Differentiation, Proceedings of 1976 ACM Symposium on Symbolic and Algebraic Computation

[6] G. E. Collins, A. Akritas, Polynomial Real Root Isolation Using Descarte´s Rule of Signs, Proceedings of 1976 ACM Symposium on Symbolic and Algebraic Computation

[7] R. Loos, private communication

[8] S. Rump, Diplomarbeit, Kaiserslautern 1976

[9] G. E. Collins, a list of SAC-1 reports is contained in the KWIC-Index, SIGSAM Bulletin of the ACM, 8 (1974), 17-44

[10] G. E. Collins, Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition, Lecture Notes in Computer Science, Vol. 33, pp. 134-183, Springer Verlag, Berlin, 1975

[11] H. Kempfert, On Sign Determinations in Real Algebraic Numbers Fields, Num. Math. 11, (1968) 170-174

[12] M. Mignotte, An Inequality About Factors of Polynomials, Mathematics of Computation, Vol. 28, No. 128 (October 1974), pp. 1153-1157

[13] M. Mignotte, Sur la complexité certains algorithmes ou intervient la séparation des racines d'un polynôme

[14] G. E. Collins and E. Horowitz, The Minimum Root Seperation of a Polynomial, Math. of Comp., Vol. 28, No. 126(1974) 589-597