J. Symbolic Computation (2001) **32**, 467–473
doi:10.1006/jsco.2001.0481
Available online at http://www.idealibrary.com on IDEAL®

Polynomial Minimum Root Separation

GEORGE E. COLLINS

Department of Computer and Information Sciences, University of Delaware, Newark, DE 19716, U.S.A.

There is a well-known lower bound, due to Mignotte, for the minimum root separation of a squarefree integral polynomial, but no evidence for the sharpness of this bound. This paper provides massive computational evidence for a conjectured much larger bound, one that is approximately the square root of Mignotte's bound.

1. Introduction

Let $A(x) = \sum_{i=0}^{n} a_i x^i = a_n \prod_{i=1}^{n}(x - \alpha_i)$ be a non-zero squarefree polynomial of degree $n \geq 2$ with integer coefficients. The *minimum root separation* of $A(x)$ is defined to be $\mathrm{sep}(A) = \min_{i \neq j} |\alpha_i - \alpha_j|$. We are interested in lower bounds for $\mathrm{sep}(A)$ as a function of the degree n and the size of the coefficients of A. Such a lower bound can be used to obtain an upper bound on the time required by certain algorithms to isolate the roots of A; see, for example, Collins and Akritas (1976). In Collins and Horowitz (1974) the lower bound

$$\mathrm{sep}(A) > \tfrac{1}{2} e^{-n/2} n^{-3n/2} d^{-n} \tag{1}$$

was proved, where d is the max norm $|A| = \max_i |a_i|$. In Mignotte (1982) the lower bound $\sqrt{3} n^{-n/2-1} \parallel A \parallel^{-n+1}$ was proved, using a result of Mahler (1964), where $\parallel A \parallel$ is the Euclidean norm of A. Since $\parallel A \parallel \leq \sqrt{n+1}\, d < \sqrt{2n}\, d$ this implies the slight improvement

$$\mathrm{sep}(A) > \sqrt{6} n^{-n/2-1/2} d^{-n+1}. \tag{2}$$

How good is this bound? Can it be closely approached? Let $A(x) = x^n - 2(ax-1)^2$, $n \geq 3$ and $a \geq 3$. In the same paper, Mignotte showed that the irreducible polynomial A satisfies $\mathrm{sep}(A) < 2a^{-n/2+1/2}$. Here $d = |A| = 2a^2$, so $\mathrm{sep}(A) < 2^{-n/4+5/4} d^{-n/4+1/4}$. Similar examples seem not to be known. Concentrating on the exponent of d, there remains a huge gap between $d^{-n/4}$ and d^{-n+1}. In this paper, we explore this gap by computing $\mathrm{M}(n,d) = \min\{\mathrm{realsep}(A) : A\,\mathrm{irreducible} \wedge \deg(A) = n \wedge |A| = d\}$ for as many (necessarily small) values of n and d as possible. realsep(A) is the minimum distance between any two real roots of A (undefined if A has fewer than two real roots). Analysis of our results leads to a conjecture that $\mathrm{M}(n,d) > n^{-n/4} d^{-n/2}$.

2. Methods

In this section we describe the methods that were used to generate our results. This is important because of the enormous number of polynomials that had to be processed. The programs described next were written in the SACLIB system.

0747–7171/01/110467 + 07 $35.00/0

$A(x)$ and $-A(x)$ have the same roots, so it suffices to consider only polynomials with positive leading coefficients. Also, $A(x)$ and $A(-x)$ have the same separation, so it suffices to consider only polynomials of degree n whose coefficient of x^{n-1} is non-negative. We used a program LEXGEN that generates in lexicographic order all $(n+1)$-tuples of coefficients $(a_n, a_{n-1}, \ldots, a_0)$ such that $a_n > 0$, $a_{n-1} \geq 0$ and $-d \leq a_i \leq d$ for $0 \leq i \leq n$. Our main program, REALSEP, then rejects any such tuple for which there is not some a_i for which $a_i = d$ or $a_i = -d$. Next, REALSEP rejects the tuple if the greatest common divisor of the a_is is not 1. Then REALSEP converts the tuple to an integral polynomial A of degree n that is primitive.

Next A is tested for squarefreeness. The greatest common divisor of A and its first derivative A' is computed modulo a prime number whose size is about one-half of the word length, about 15 bits. If the gcd is 1, then A is known to be squarefree. Otherwise the discriminant of A is computed. Then A is squarefree if and only if the discriminant is non-zero.

Next A is converted to a hardware interval polynomial. Each integer coefficient is converted to the smallest interval with double precision hardware floating point coefficients that contains it. The real roots of the interval polynomial are then isolated using the Descartes method with the SACLIB program HIPRRID. If this fails then the real roots of the integral polynomial are isolated instead, using the SACLIB program IPRRID; but we observed very few failures among millions of cases.

If the polynomial has fewer than two real roots, we go on to the next tuple. Otherwise the SACLIB program HIPIR is used to refine each isolating interval, using interval arithmetic, to a length of 2^{-30}. Then the minimum distance between any two consecutive real roots is computed. If this distance is less than the minimum distance for any previous polynomial, then the polynomial is tested for irreducibility. If the polynomial is reducible then it is rejected and a new minimum is not recorded. Since most polynomials are irreducible and since new minimums are rare, this strategy results in a very small cost for irreducibility testing, a relatively time consuming operation.

For more on the use of interval arithmetic for polynomial real root computation, see Collins *et al.* (2001).

3. Quadratic Polynomials

Using the quadratic formula, we can readily deduce some facts about the minimum root separation of any quadratic polynomial. Let $A(x) = ax^2 + bx + c$ be a squarefree polynomial with $a > 0$ and with $D = b^2 - 4ac \neq 0$. Let $d = \max\{a, b, c\}$. Then $\mathrm{sep}(A) = \sqrt{|D|}/a \geq \sqrt{|D|}/d \geq 1/d$. This is a slight improvement over inequality (2), which for $n = 2$ reduces to $\mathrm{sep}(A) > \sqrt{3}/2d$. If we allow $A(x)$ to be reducible, then the lower bound $1/d$ can actually be attained for infinitely many values of d. Let $d = a(a+1)$, $a \geq 2$, $A(x) = (ax-1)((a+1)x-1) = dx^2 - (2a+1)x + 1$. Then $|A| = d$ and $\mathrm{sep}(A) = 1/a - 1/(a+1) = 1/d$.

Table 1 shows $\mathrm{M}(2,d)$ and $\mathrm{M}(2,d)/d^{-1}$ for $1 \leq d \leq 20$. The discriminant of an irreducible quadratic polynomial $ax^2 + bx + c$ with two real roots is at least 5. Therefore $\mathrm{sep}(A) \geq \sqrt{5}/a \geq \sqrt{5}/d$, and so $\mathrm{M}(2,d) \geq \sqrt{5}/d$ and $\mathrm{M}(2,d)/d^{-1} \geq \sqrt{5}$. Using REALSEP with $n = 2$ and $1 \leq d \leq 200$ we have found that $\mathrm{M}(2,d)/d^{-1} = \sqrt{5}$ for $d = 1, 5, 11, 19, 29, 31, 41, 55, 59, 61, 71, 79, 89, 95, 101, 109, 121, 131, 139, 145, 149, 151, 155, 179, 181, 191$ and 199. Let b be odd and $b \geq 5$, $a = (b^2-5)/4$, $c = 1$, and $A(x) = ax^2 + bx + c$. Then $|A| = a$, the discriminant of A is 5 and $\mathrm{sep}(A) = \sqrt{5}/a$. This

Table 1. Minimum real separations of irreducible quadratic polynomials.

d	$\mathrm{M}(2,d)$	$\mathrm{M}(2,d)/d^{-1}$	d	$\mathrm{M}(2,d)$	$\mathrm{M}(2,d)/d^{-1}$
1	2.23607	2.23607	11	0.20328	2.23608
2	1.41421	2.82842	12	0.31492	3.77904
3	1.15470	3.46410	13	0.26647	3.46411
4	1.03078	4.12312	14	0.20203	2.82842
5	0.44721	2.23605	15	0.20328	3.04920
6	0.57735	3.46410	16	0.25769	4.12304
7	0.40406	2.82842	17	0.16638	2.82846
8	0.40406	3.23248	18	0.26647	4.79646
9	0.40062	3.60558	19	0.11769	2.23611
10	0.48990	4.89900	20	0.20203	4.04060

Table 2. Minimum real separations of irreducible cubic polynomials.

d	$\mathrm{M}(3,d)$	$\mathrm{M}(3,d)/d^{-3/2}$	d	$\mathrm{M}(3,d)$	$\mathrm{M}(3,d)/d^{-3/2}$	d	$\mathrm{M}(3,d)$	$\mathrm{M}(3,d)/d^{-3/2}$
1			13	0.02565	1.202	25	0.01638	2.047
2	0.78348	2.215	14	0.04650	2.435	26	0.00648	0.859
3	0.34730	1.804	15	0.05105	2.965	27	0.01436	2.015
4	0.33513	2.681	16	0.03138	2.008	28	0.01185	1.756
5	0.14367	1.606	17	0.02782	1.950	29	0.01237	1.932
6	0.19273	2.832	18	0.03579	2.733	30	0.01718	2.823
7	0.11263	2.085	19	0.02032	1.683	31	0.00536	0.925
8	0.11813	2.673	20	0.01639	1.465	32	0.00783	1.417
9	0.06662	1.798	21	0.02566	2.469	33	0.01378	2.612
10	0.07701	2.435	22	0.02022	2.099	34	0.01221	2.420
11	0.04765	1.738	23	0.02546	2.807	35	0.00986	2.042
12	0.05813	2.416	24	0.02026	2.382	36	0.00971	2.097

proves that $\mathrm{M}(2,d)/d^{-1}$ assumes its minimum value of $\sqrt{5}$ for infinitely many values of d. The values $b = 5, 7, 9, 11, 13, 15, 17$ and 19 yield the values $d = 5, 11, 19, 29, 41, 55, 71, 89, 109, 131, 155$ and 181. Let $a = 5n^2 + 5n + 1$, $b = 10n + 5$ and $c = 5$. Then the discriminant of $A(x) = ax^2 + bx + c$ is 5, $\mathrm{sep}(A) = \sqrt{5}/a$ and $\mathrm{sep}(A)/d^{-1} = \sqrt{5}$. This accounts for the values $d = 11, 31, 61, 101$ and 151. 11 values of d remain unaccounted for by these two formulae or any other formula. Let $\mathrm{D}(n,d)$ be the discriminant of the polynomial of degree n whose minimum real separation is $\mathrm{M}(n,d)$. Then $\mathrm{M}(2,d) \geq \mathrm{D}(2,d)$. Values of $(d, \mathrm{D}(2,d))$ for which $\mathrm{D}(2,d)$ exceeds $\mathrm{D}(2,d')$ for all $d' < d$ are $(1,5), (2,8), (3,12), (4,17), (10,24), (28,28), (40,41), (110,44)$ and $(144,73)$. We conjecture that $\mathrm{M}(2,d)/d^{-1}$ is unbounded above, but is dominated by $\log d$.

4. Cubic Polynomials

Table 2 shows $\mathrm{M}(3,d)$ and $\mathrm{M}(3,d)/d^{-3/2}$ for $2 \leq d \leq 36$. $\mathrm{M}(3,1)$ is undefined. The minimum value of $\mathrm{M}(3,d)/d^{-3/2}$, 0.859, occurs when $d = 26$; the maximum of 2.965 occurs when $d = 15$. There is no obvious upward or downward trend in the values of $\mathrm{M}(3,d)/d^{-3/2}$.

For $2 \leq d \leq 25$ we also computed $\mathrm{C}(3,d)$, the minimum root separation for irreducible cubic polynomials having only one real root. This was done by dividing the polynomial by the monic linear factor corresponding to its real root and then applying the quadratic formula to the resulting quadratic polynomial. The arithmetic operations were carried out using interval arithmetic. We found that in every case $\mathrm{C}(3,d)$ was the distance between

Table 3. Minimum real separations of reducible cubic polynomials.

d	$\mathrm{M}'(3,d)$	$\mathrm{M}'(3,d)/d^{-3/2}$	d	$\mathrm{M}'(3,d)$	$\mathrm{M}'(3,d)/d^{-3/2}$	d	$\mathrm{M}'(3,d)$	$\mathrm{M}'(3,d)/d^{-3/2}$
2	0.29289	0.828	10	0.02822	0.892	18	0.01257	0.960
3	0.11803	0.613	11	0.03078	1.123	19	0.01549	1.283
4	0.08579	0.686	12	0.01376	0.572	20	0.00693	0.620
5	0.04863	0.544	13	0.00697	0.327	21	0.00265	0.255
6	0.03269	0.480	14	0.00718	0.377	22	0.00239	0.247
7	0.04257	0.788	15	0.01393	0.809	23	0.00660	0.728
8	0.01803	0.408	16	0.00897	0.574	24	0.00742	0.872
9	0.01421	0.384	17	0.00494	0.346	25	0.00300	0.375

Table 4. Minimum real separations of irreducible quartic polynomials.

d	$\mathrm{M}(4,d)$	$\mathrm{M}(4,d)/d^{-2}$	d	$\mathrm{M}(4,d)$	$\mathrm{M}(4,d)/d^{-2}$	d	$\mathrm{M}(4,d)$	$\mathrm{M}(4,d)/d^{-2}$
1	1.14139	1.1414	6	0.04935	1.7766	11	0.00589	0.7127
2	0.38403	1.5361	7	0.02065	1.0118	12	0.01511	2.1758
3	0.16790	1.5111	8	0.01668	1.0675	13	0.00495	0.8365
4	0.07498	1.1997	9	0.01747	1.4151	14	0.00715	1.4014
5	0.06203	1.5507	10	0.01419	1.4190	15	0.00548	1.2330

the two conjugate complex roots of the polynomial with least root separation. Except for $d = 13$ and $d = 25$, $\mathrm{C}(3,d)$ was less than $\mathrm{M}(3,d)$. However the ratios of $\mathrm{M}(3,d)$ to $\mathrm{C}(3,d)$ were mostly less than two, and never exceeded three.

We also computed the minimum real separations of reducible cubic polynomials, denoted by $\mathrm{M}'(3,d)$, for $2 \le d \le 25$. ($\mathrm{M}'(3,1)$ is undefined.) As was the case for quadratics, the minimum separations for reducible polynomials are somewhat smaller than for irreducible polynomials. However, $d^{-3/2}$ again appears to be a good fit. Table 3 shows the values of $\mathrm{M}'(3,d)/d^{-3/2}$, which fluctuate but exhibit no obvious upward or downward trend. For each value of d, the polynomial producing the minimum separation $\mathrm{M}'(3,d)$ is the product of a linear polynomial and a quadratic polynomial with two real roots.

5. Quartic Polynomials

$\mathrm{M}(4,d)$ was computed for $1 \le d \le 15$. The results are shown in Table 4. Once again $d^{-n/2}$ appears to be a very good estimate for $\mathrm{M}(n,d)$. $\mathrm{M}(4,d)/d^{-2}$ varies between 0.7127 and 2.1758 and there is no apparent up or down trend in the values. In every case except $d = 14$, the polynomial achieving the minimum separation had just two real roots. We conjecture that this is just a consequence of the fact that there are fewer polynomials having four real roots than two. For example, for $d = 8$, 26.2% of the polynomials have no real roots, 70.4% have two real roots, and only 3.3% have four real roots.

For $1 \le d \le 12$, we also computed the minimum real separations of reducible quartics with two real roots. In each case the polynomial achieving the minimum separation was the product of a linear polynomial and an irreducible cubic with only one real root. The ratio of the minimum separation to d^{-2} varied between 0.078 and 0.756, with no apparent trend. This is consistent with our observations for minimum separations of reducible cubics.

We also computed the minimum separations of irreducible quartics, defined by the distances between any two roots, real or complex. These did not differ significantly from

Table 5. Minimum real separations of irreducible quintic polynomials.

d	$\mathrm{M}(5,d)$	$\mathrm{M}(5,d)/d^{-5/2}$	d	$\mathrm{M}(5,d)$	$\mathrm{M}(5,d)/d^{-5/2}$	d	$\mathrm{M}(5,d)$	$\mathrm{M}(5,d)/d^{-5/2}$
1	0.80676	0.8068	4	0.02369	0.7581	7	0.00515	0.6676
2	0.20603	1.1655	5	0.01793	1.0023	8	0.00560	1.0137
3	0.03669	0.5719	6	0.00681	0.6005			

Table 6. Minimum real separations of irreducible polynomials of degree 6.

d	$\mathrm{M}(6,d)$	$\mathrm{M}(6,d)/d^{-3}$	d	$\mathrm{M}(6,d)$	$\mathrm{M}(6,d)/d^{-3}$	d	$\mathrm{M}(6,d)$	$\mathrm{M}(6,d)/d^{-3}$
1	0.65808	0.6581	3	0.01673	0.4517	5	0.00190	0.2375
2	0.06656	0.5325	4	0.00618	0.3955	6	0.00245	0.5292

Table 7. Minimum real separations of irreducible polynomials, degrees 7–10.

d	$\mathrm{M}(7,d)$	$\mathrm{M}(7,d)/d^{-7/2}$	d	$\mathrm{M}(7,d)$	$\mathrm{M}(7,d)/d^{-7/2}$	d	$\mathrm{M}(7,d)$	$\mathrm{M}(7,d)/d^{-7/2}$
1	0.15679	0.1568	2	0.03866	0.4374	3	0.00763	0.3568
4	0.00248	0.3174						
d	$\mathrm{M}(8,d)$	$\mathrm{M}(8,d)/d^{-4}$	d	$\mathrm{M}(8,d)$	$\mathrm{M}(8,d)/d^{-4}$	d	$\mathrm{M}(8,d)$	$\mathrm{M}(8,d)/d^{-4}$
1	0.09625	0.0963	2	0.01011	0.1618	3	0.00232	0.1887
d	$\mathrm{M}(9,d)$	$\mathrm{M}(9,d)/d^{-9/2}$	d	$\mathrm{M}(9,d)$	$\mathrm{M}(9,d)/d^{-9/2}$	d	$\mathrm{M}(9,d)$	$\mathrm{M}(9,d)/d^{-9/2}$
1	0.08461	0.0846	2	0.00730	0.1652			
d	$\mathrm{M}(10,d)$	$\mathrm{M}(10,d)/d^{-5}$	d	$\mathrm{M}(10,d)$	$\mathrm{M}(10,d)/d^{-5}$	d	$\mathrm{M}(10,d)$	$\mathrm{M}(10,d)/d^{-5}$
1	0.04950	0.0495	2	0.00352	0.1126			

the minimum real separations. For $d = 1, 9$ and 10 the minimum separations were just slightly smaller than the minimum real separations.

6. Quintic Polynomials

For quintic polynomials the minimum real separations for irreducible polynomials were computed for $1 \leq d \leq 8$. The results are shown in Table 5. Once again $\mathrm{M}(n,d)/d^{-n/2}$ appears to vary modestly, and without a trend, about a constant value slightly less than 1.

7. Higher Degrees

The results for degree 6 are somewhat anomalous. As Table 6 shows, the value of $\mathrm{M}(6,d)/d^{-3}$ decreases steadily as d increases from 1 to 5. However $\mathrm{M}(6,d)/d^{-3}$ for $d = 6$ returns to nearly the same value as for $d = 2$.

Table 7 shows the results that we were able to obtain for degrees 7–10. The values of d are necessarily very small. But, at least, one can say that these results are also consistent with a hypothesis that $\mathrm{M}(n,d)$ dominates $d^{-n/2}$ for every fixed value of n.

8. Separation as a Function of *n*

Our results are supportive of a conjecture that, for every fixed n, there exists $f(n) > 0$ such that $\mathrm{M}(n,d) \geq f(n)d^{-n/2}$. Table 8 summarizes our results and suggests that $f(n) = n^{-n/4}$ may be such a function. In the table, $\mathrm{L}(n)$ denotes the least

Table 8. Least observed values vs. $n^{-n/4}$.

n	L(n)	L(n)/$n^{-n/4}$	n	L(n)	L(n)/$n^{-n/4}$	n	L(n)	L(n)/$n^{-n/4}$
1			5	0.5719	4.276	9	0.0846	11.869
2	2.2361	5.318	6	0.2375	3.491	10	0.0495	15.653
3	0.8590	1.958	7	0.1568	4.724	11	0.0260	18.998
4	0.7127	2.851	8	0.0963	6.163	12	0.0189	32.659

Table 9. Distribution of real root separations, $n = 5$, $d = 6$.

Interval	Number	Percent
$(1, \infty)$	54 159	51.4
(1/2,1)	36 405	34.5
(1/4,1/2)	11 329	10.7
(1/8,1/4)	2693	2.6
(1/16,1/8)	610	0.58
(1/32,1/16)	120	0.11
(1/64,1/32)	11	0.01
(1/128,1/64)	3	0.003

observed value of $\mathrm{M}(n, d)/d^{-n/2}$. We have included $n = 11$ and $n = 12$, for which we computed only $\mathrm{M}(n, 1)$. The values of $\mathrm{L}(n)/n^{-n/4}$ become somewhat larger for $n \geq 9$. This is perhaps to be expected since the values of $\mathrm{L}(n)$ for $n \geq 9$ are based on only one or two values of d.

9. Additional Comments

The data we generated required an enormous amount of computation. Consider just one example, the computation for $n = 7$ and $d = 4$. The number of 8-tuples generated was $4 \cdot 5 \cdot 9^6 = 10\,628\,820$. The number of primitive polynomials produced was 9 124 740. 9 007 485 of the primitive polynomials were squarefree, and their roots were isolated. 5 516 280 polynomials had only one real root, 3 414 054 had three real roots and 77 144 had five real roots. This resulted in refining to a length of 2^{-30} the isolating intervals for $3\,414\,054 \cdot 3 + 77\,144 \cdot 5 = 10\,627\,882$ real roots. The total computation time for this case was 90 min, 43 s.

We also used our computations to explore the frequency of small real root separations. Table 9 gives such frequencies for just one typical example, namely $n = 5, d = 6$. There were 105 330 irreducible quintic polynomials having max norm 6 and three real roots. The table shows how many of these had real separations greater than 1 and how many had real separations in the intervals $(2^{-k-1}, 2^{-k})$ for $k \geq 0$.

We also looked for characteristics of winning polynomials, those polynomials A of degree n and max norm d with $\mathrm{sep}(A) = \mathrm{M}(n, d)$. Knowing such characteristics could be helpful in finding polynomials with small real separations without conducting exhaustive searches. The only characteristic found is that the leading coefficient is likely to be the largest. This was the case for 146 of 200 winning quadratics, 19 of 35 winning cubics, nine of 15 winning quartics, six of eight winning quintics, five of six winning polynomials of degree 6, and four of four winning polynomials of degree 7.

Acknowledgement

Partial support was provided by NSF Grant CCR-9712246.

References

Collins, G. E., Akritas, A. G. (1976). Polynomial real root isolation using Descartes' rule of signs. In Jenks, R. D. ed., *Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation (SYMSAC '76)*, pp. 272–275. ACM Press.

Collins, G. E., Johnson, J. R., Krandick, W. (2001). Interval arithmetic in CAD computation. *J. Symb. Comput.,* submitted.

Collins, G. E., Horowitz, E. (1974). The minimum root separation of a polynomial. *Math. Comp.*, **28**, 589–597.

Mahler, K. (1964). An inequality for the discriminant of a polynomial. *Michigan Math. J.*, **11**, 257–262.

Mignotte, M. (1982). Some useful bounds. In Buchberger, B., Collins, G. E., Loos, R. eds, *Computer Algebra*, pp. 259–263. Springer-Verlag.

Received 21 June 2001
Accepted 7 July 2001