Absolute real root separation

Yann Bugeaud, Andrej Dujella,

Tomislav Pejković, and Bruno Salvy

Abstract

While the separation (the minimal nonzero distance) between roots of a polynomial is a classical topic, its absolute counterpart (the minimal nonzero distance between their absolute values) does not seem to have been studied much. We present the general context and give tight bounds for the case of real roots.

1 Separation and absolute separation

The polynomials $14x^3 + 17x^2 - 13x + 2$ and $17x^3 - 9x^2 - 7x + 8$ hold records in the set of polynomials with integer coefficients in $\{-20, \ldots, 20\}$ and degree at most 3. The first one has two roots α_1, α_2 with

$$0 < |\alpha_1 - \alpha_2| < 0.005,$$

while the second one has two roots β_1, β_2 with

$$0 < \big||\beta_1| - |\beta_2|\big| < 0.000015.$$

Apart from those obtained by multiplying these polynomials by -1 or changing x into $-x$ in them, no other polynomial in that set has roots satisfying any of these inequalities. More generally, we are interested in understanding how close can the nonzero difference between two roots (or the absolute values of two roots) of a polynomial with integer coefficients be in terms of its degree and a bound on its coefficients.

The first quantity is classically called the *root separation* of a polynomial P with at least two distinct roots and denoted by $\text{sep}(P)$:

$$\text{sep}(P) := \min_{\substack{P(\alpha)=P(\beta)=0, \\ \alpha \neq \beta}} |\alpha - \beta|.$$

By analogy, we define the *absolute root separation* by

$$\text{abs sep}(P) := \min_{\substack{P(\alpha)=P(\beta)=0, \\ |\alpha| \neq |\beta|}} \big| |\alpha| - |\beta| \big|.$$

This quantity arises in the computation of the asymptotic behavior of sequences satisfying linear recurrence equations, where it governs the precision required in computing the roots of the characteristic polynomial.

The *height* of a polynomial P, denoted $\text{H}(P)$, is the maximum of the absolute values of its coefficients. In 1964, Mahler proved the following lower bound relating separation, degree and height [9, 1].

Proposition 1 (Mahler, 1964). *If α, β are two roots of a separable polynomial (i.e., with no multiple roots) of degree $d \geq 2$ with integer coefficients, then*

$$|\alpha - \beta| > \sqrt{3}(d+1)^{-(2d+1)/2} \max\{1, |\alpha|, |\beta|\} \, \text{H}(P)^{-d+1}. \tag{1}$$

This implies in that case

$$\text{sep}(P) \gg \text{H}(P)^{-d+1}, \tag{2}$$

where, here and below, the constant implicit in the '$\gg$' sign depends only on the degree d. The tightness of the exponent $-d+1$ of $\text{H}(P)$ in this inequality is still unknown. The best known upper bound on this exponent is $-(2d-1)/3$ for general d (see [3]) and -2 for $d = 3$ [6, 11], which is the only case where we thus know the bound of (2) to be optimal. (Restricting further the set of polynomials under consideration so that only monic or irreducible polynomials enter the contest leads to even larger upper bounds [4, 2, 3, 5].)

Concerning the absolute separation, not much appears to be known. A consequence of Mahler's result (1) yields the following [7]:

$$\text{abs sep}(P) \gg \text{H}(P)^{-d(d^2+2d-1)/2}. \tag{3}$$

The exponent of $\text{H}(P)$ does not seem to be the best possible, but no improvement in this general case seems to be known. However, restricting to the absolute root separation of two *real* roots, our main result completely solves the problem:

Theorem 1. *Let $\alpha_1 = \alpha, \alpha_2 = \beta, \alpha_3, \ldots, \alpha_d \in \mathbb{C}$ be the roots of a separable polynomial $P(x) \in \mathbb{Z}[x]$ of degree d such that $\alpha_i + \alpha_j \neq 0$ for any $i, j \in \{1, \ldots, d\}$. If α and β are real then*

$$\big||\alpha| - |\beta|\big| \geq 2^{(-d^2+2)/2}(d+1)^{(-d+1)/2} \, \mathrm{H}(P)^{-d+1}. \qquad (4)$$

Moreover, the exponent of $\mathrm{H}(P)$ is best possible.

In the next section, we give a proof of the first part of this theorem, which is a variant of Mahler's proof. Next, we prove that for reducible polynomials, the exponent can be increased to $-d+2$ (Theorem 2 below). Finally, we give explicit families of polynomials reaching the bound $-d+1$. We show that, furthermore, the bound is still tight when restricting to monic polynomials of arbitrary degree $d \geq 3$.

2 Bounds from resultants

Since Mahler's result (1) implies (4) if α and β have the same sign, we need to prove a comparable result for $|\alpha + \beta|$ as well. Our proof, like Mahler's, relies on the use of a resultant. Recall that the resultant $\mathrm{Res}(P, Q)$ of two univariate polynomials P and Q of degree d_1 and d_2 is the determinant of their Sylvester matrix, which is the transposed matrix of the map $(U, V) \mapsto UP + VQ$ in the bases $((1, 0), (x, 0), \ldots, (x^{d_2-1}, 0), (0, 1), (0, x), \ldots, (0, x^{d_1-1})), (1, x, \ldots, x^{d_1+d_2-1})$. We refer to the literature (e.g., [8, 10]) for the definition and properties of resultants and recall only the following.

Lemma 1 (Poisson's formula)**.** *The resultant of the polynomials $P = a_{d_1} \prod_{i=1}^{d_1}(x - \alpha_i)$ and $Q = b_{d_2} \prod_{i=1}^{d_2}(x - \beta_i)$ satisfies*

$$\mathrm{Res}(P, Q) = a_{d_1}^{d_2} b_{d_2}^{d_1} \prod_{i,j}(\alpha_i - \beta_j).$$

The special case when $Q = P'$ gives the discriminant (up to a simple constant), that was used by Mahler in his proof.

We thus obtain the products of pairwise sums of roots of $P(x) = a_d x^d +$

$\cdots + a_1 x + a_0$ by considering the resultant $r = \mathrm{Res}(P(x), P(-x))$,

$$r = \begin{vmatrix} a_d & \cdots & a_1 & a_0 & & & \\ & \ddots & & & & \ddots & \\ & & a_d & a_{d-1} & \cdots & & a_0 \\ (-1)^d a_d & \cdots & -a_1 & a_0 & & & \\ & \ddots & & & & \ddots & \\ & & (-1)^d a_d & (-1)^{d-1} a_{d-1} & \cdots & & a_0 \end{vmatrix}.$$

Factoring out a_d from the first column and a_0 from the last, we see that r is an integer divisible by $a_0 a_d$. Thus, if $r \neq 0$, then we have

$$|r| \geq |a_0 a_d|. \tag{5}$$

On the other hand, Poisson's formula gives

$$r = (-1)^d a_d^{2d} \prod_{1 \leq i \leq d} (2\alpha_i) \prod_{1 \leq i < j \leq d} (\alpha_i + \alpha_j)^2,$$
$$= a_0 a_d^{2d-1} 2^d \prod_{1 \leq i < j \leq d} (\alpha_i + \alpha_j)^2.$$

since $\prod_{i=1}^d \alpha_i = (-1)^d a_0 / a_d$.

Bounds will follow from the simple upper bound

$$|\alpha_i + \alpha_j| \leq 2 \max\{1, |\alpha_i|\} \max\{1, |\alpha_j|\}, \quad \text{for all } i, j.$$

Then, with our notation $\alpha = \alpha_1$, $\beta = \alpha_2$, we get

$$|r| \leq 2^{d^2 - 2} |a_0| |a_d|^{2d-1} |\alpha + \beta|^2 \prod_{1 \leq i \leq d} \max\{1, |\alpha_i|\}^{2d-2}. \tag{6}$$

This last quantity is related to the height of P thanks to the following.

Lemma 2 (Landau's inequality). *The* Mahler measure $\mathrm{M}(P)$, *defined as*

$$\mathrm{M}(P) := |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\},$$

is bounded by:

$$\mathrm{M}(P) \leq \sqrt{a_0^2 + \cdots + a_d^2} \leq \sqrt{d+1}\, \mathrm{H}(P). \tag{7}$$

Sketch of proof. See, for instance, [1, 10]. If all the roots have modulus smaller than 1, then the property is obvious. If $P(\alpha) = 0$ with $|\alpha| > 1$ then the polynomial $(1 - \alpha x)P(x)/(x - \alpha)$ can be checked to have the same Mahler measure and the same L_2-norm as P. This construction is repeated till no root has modulus larger than 1. $\qquad\square$

When no $\alpha_i + \alpha_j$ is 0, then Landau's bound (7) together with (6) and (5) give

$$|\alpha + \beta| \geq 2^{(-d^2+2)/2}(d + 1)^{(-d+1)/2} \operatorname{H}(P)^{-d+1},$$

which finishes the proof of the first part of Theorem 1.

3 The case of reducible polynomials

It turns out that the exponent of $\operatorname{H}(P)$ can be improved for irrational roots of reducible polynomials.

Theorem 2. *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial of degree d reducible over $\mathbb{Q}$. Then for any two irrational real roots α, β of $P(x)$, either $|\alpha| = |\beta|$ or*

$$\big||\alpha| - |\beta|\big| \geq 2^{-3d^2/2+3d-1}d^{(-d+2)/2} \operatorname{H}(P)^{-d+2}. \tag{8}$$

Proof. We assume $|\alpha| \neq |\beta|$. Any irreducible factor Q of P has degree at most $d-1$ and Gelfond's lemma (see e.g., [1, Lemma A.3]) implies $\operatorname{H}(Q) \leq 2^d \operatorname{H}(P)$.

We distinguish two cases depending on whether α and $\pm\beta$ are roots of the same irreducible factor of P or not. When α and either one of $\pm\beta$ are roots of the same irreducible factor Q, Theorem 1 applies to Q if moreover it has no pair of opposite roots. Then, we get

$$\begin{aligned}
\big||\alpha| - |\beta|\big| &\geq 2^{(-d^2+2d+1)/2}d^{(-d+2)/2} \operatorname{H}(Q)^{-d+2} \\
&\geq 2^{-3d^2/2+3d+1/2}d^{(-d+2)/2} \operatorname{H}(P)^{-d+2}.
\end{aligned} \tag{9}$$

If two roots of Q sum to 0, the gcd of $Q(x)$ and $Q(-x)$ is nontrivial and since Q is irreducible, this means that $Q(x)$ is even, so that $\pm\beta$ are both roots of Q and Mahler's bound applies both to $|\alpha - \beta|$ and $|\alpha + \beta|$, leading to

$$\big||\alpha| - |\beta|\big| = |\alpha - (\pm\beta)| > \sqrt{3}d^{-(2d-1)/2} \operatorname{H}(Q)^{-d+2}, \tag{10}$$

which leads to the result since $\sqrt{3}d^{-(2d-1)/2} > 2^{(-d^2+2d-2)/2}d^{(-d+2)/2}$ for $d \geq 0$.

Otherwise, if α and $\pm\beta$ are not roots of the same irreducible factor of P, let $Q_\alpha(x)$ and $Q_\beta(x)$ be minimal polynomials of α and β over $\mathbb{Z}$ with respective degrees a and b. Arguing in a similar manner as in the proof of Theorem 1, we deduce

$$1 \leq |\operatorname{Res}(Q_\alpha(x), Q_\beta(\pm x))| \leq 2^{ab} \operatorname{M}(Q_\alpha)^b \operatorname{M}(Q_\beta)^a |\alpha \pm \beta|.$$

5

Gauss's lemma and multiplicativity of Mahler's measure give $\mathrm{M}(Q_\alpha Q_\beta) \leq \mathrm{M}(P)$. Furthermore, the condition that α and β are not rational gives $a, b \in [2, d-2]$, so that

$$\mathrm{M}(Q_\alpha)^b \, \mathrm{M}(Q_\beta)^a \leq \mathrm{M}(Q_\alpha Q_\beta)^{\max\{a,b\}} \leq \mathrm{M}(P)^{d-2} \leq (d+1)^{(d-2)/2} \, \mathrm{H}(P)^{d-2}$$

and finally $2^{ab} \leq 2^{d^2/4}$, leading to

$$\bigl||\alpha| - |\beta|\bigr| \geq 2^{-d^2/4}(d+1)^{(-d+2)/2} \, \mathrm{H}(P)^{-d+2}$$

which is stronger than (8) since α, β being both irrational forces $d \geq 4$. $\qquad\square$

4 Families with small absolute root separation

We now exhibit families of polynomials that reach the exponent $-d+1$ of Theorem 1, thereby concluding its proof. The construction starts from $Mx^2 - 1$ which has two real roots $\pm 1/\sqrt{M}$. For M sufficiently large, these are small so that higher powers of the roots will be even smaller. By perturbing $Mx^2 - 1$ in appropriate ways we thus get polynomials with roots very close to $\pm 1/\sqrt{M}$ and whose sum is minute.

Theorem 3. *Let $d \geq 2$ be an integer and M be a positive integer. Consider the polynomials $P_{d,M}(x)$ of degree d and height M defined by:*

$$P_{d,M}(x) = \begin{cases} Mx^2 - x - 1 & \text{if } d = 2; \\ x^3 + Mx^2 - 1 & \text{if } d = 3; \\ x^d - (Mx^2 - 1)(1 - x^{d-3}) & \text{if } d \geq 4 \text{ even;} \\ x^d - (M-1)x^{d-1} + x^{d-3} - Mx^3 - Mx^2 + x + 1 & \text{if } d \geq 5 \text{ odd.} \end{cases}$$

If M is sufficiently large in terms of d, then the polynomial $P_{d,M}(x)$ has two roots $\alpha, \beta \in \mathbb{R}$ such that $||\alpha| - |\beta|| = |\alpha + \beta|$ and

$$0 < |\alpha + \beta| \ll \mathrm{H}(P_{d,M})^{-d+1}. \tag{11}$$

For $d \geq 3$, these polynomials are monic and irreducible over the field of rational numbers.

Note that for any odd integer $d \geq 5$ the polynomial $x^{d-1} - (Mx^2 - 1)(1 - x^{d-2})$ has also two real roots satisfying (11). However, $P_{d,M}$ has the extra advantage of being monic.

Proof of Theorem 3. The case of quadratic polynomials is trivial. The only thing left to discuss for $d = 2$ is monicity and irreducibility. With monic quadratic polynomials, we can only achieve the exponent 0 in (11). The given polynomial is irreducible if and only if $4M + 1$ is not a square, which happens for infinitely many M. Therefore, from now on, we take $d \geq 3$.

Direct asymptotic computations give roots α and β of $P_{d,M}$ such that (11) holds. For instance, the polynomial $P_{3,M}$ has two roots α_3, β_3 satisfying

$$\alpha_3 = -M^{-1/2} - \frac{1}{2}M^{-2} + \mathcal{O}(M^{-7/2}),$$
$$\beta_3 = M^{-1/2} - \frac{1}{2}M^{-2} + \mathcal{O}(M^{-7/2}).$$

The conclusion of the proof is computational too and consists in giving small enough intervals where the polynomial $P_{d,M}(x)$ changes sign. For the first root for instance,

$$P_{3,M}\left(-M^{-1/2} - \frac{1}{2}M^{-2} - M^{-3}\right) = 2M^{-5/2} + \mathcal{O}(M^{-3}) > 0,$$
$$P_{3,M}\left(-M^{-1/2} - \frac{1}{2}M^{-2}\right) = -\frac{5}{4}M^{-3} + \mathcal{O}(M^{-4}) < 0,$$

for M large enough and similarly for the other root. Of course, the lengths of the intervals can be adjusted to the required precision.

Correspondingly, for $d \geq 4$ even, $P_{d,M}(x)$ has roots

$$\alpha = -M^{-1/2} - \frac{1}{2}M^{-(d+1)/2} + \frac{1}{2}M^{-d+1} + \mathcal{O}(M^{-(2d+1)/2}),$$
$$\beta = M^{-1/2} + \frac{1}{2}M^{-(d+1)/2} + \frac{1}{2}M^{-d+1} + \mathcal{O}(M^{-(2d+1)/2}).$$

For $d \geq 5$ odd, $P_{d,M}(x)$ has roots

$$\alpha = -M^{-1/2} - \frac{1}{2}M^{-d/2} + \frac{1}{2}M^{-(2d-3)/2} + \frac{1}{2}M^{-d+1} + \mathcal{O}(M^{-(2d-1)/2}),$$
$$\beta = M^{-1/2} + \frac{1}{2}M^{-d/2} - \frac{1}{2}M^{-(2d-3)/2} + \frac{1}{2}M^{-d+1} + \mathcal{O}(M^{-(2d-1)/2}).$$

Inequalities showing that actual roots with these expansions exist are obtained by straightforward computations.

For $d \geq 3$ and $M \geq 3$, the leading coefficient of the polynomial $P_{d,M}(x)$ is 1 and its constant coefficient is ± 1. It is easily checked that 1 and -1 are not roots of $P_{d,M}(x)$, thus this polynomial has no rational roots. Gauss' lemma together with Theorem 2 then implies that $P_{d,M}(x)$ is irreducible for M large enough in terms of d. $\qquad \square$

Acknowledgements

References

[1] Y. Bugeaud, Approximation by algebraic numbers. Cambridge Tracts in Mathematics, Cambridge, 2004.

[2] Y. Bugeaud and A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244.

[3] Y. Bugeaud and A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403.

[4] Y. Bugeaud and M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.

[5] A. Dujella and T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova **126** (2011), 63–72.

[6] J.-H. Evertse, *Distances between the conjugates of an algebraic number*, Publ. Math. Debrecen **65** (2004), 323–340.

[7] X. Gourdon and B. Salvy, *Effective asymptotics of linear recurrences with rational coefficients*, Discrete Math. **153** (1996), 145–163.

[8] S. Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

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

[10] M. Mignotte, Mathematics for computer algebra. Springer-Verlag, New York, 1992.

[11] A. Schönhage, *Polynomial root separation examples*, J. Symbolic Comput. **41** (2006), 1080–1090.

Yann Bugeaud
Université de Strasbourg
Mathématiques
7, rue René Descartes
F-67084 Strasbourg cedex, France
E-mail address: bugeaud@math.unistra.fr

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: duje@math.hr

Tomislav Pejković
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: pejkovic@math.hr

Bruno Salvy
INRIA and LIP – ENS Lyon
46, allée d'Italie
69364 Lyon Cedex 07, France
E-mail address: Bruno.Salvy@inria.fr