

Root separation for integer polynomials

Andrej Dujella

Department of Mathematics
University of Zagreb, Croatia
e-mail: duje@math.hr
URL: <http://web.math.hr/~duje/>

Question: How close to each other can be two distinct roots of a polynomial $P(X)$ with integer coefficients and degree d ?

We compare the distance between two distinct roots of $P(X)$ with its (naïve) height $H(P)$, defined as the maximum of the absolute values of its coefficients.

Mahler (1964): $|\alpha - \beta| \gg H(P)^{-d+1}$

for any distinct roots α and β of the integer polynomial $P(X)$ of degree d (the constant implied by \gg is an explicit constant depending only on the degree d).

For an integer polynomial $P(x)$ of degree $d \geq 2$ and with distinct roots $\alpha_1, \dots, \alpha_d$, we set

$$\text{sep}(P) = \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|$$

and define $e(P)$ by $\text{sep}(P) = H(P)^{-e(P)}$.

For $d \geq 2$, we set

$$e(d) := \limsup_{\deg(P)=d, H(P) \rightarrow +\infty} e(P),$$

$$e_{\text{irr}}(d) := \limsup_{\deg(P)=d, H(P) \rightarrow +\infty} e(P),$$

where the latter limsup is taken over all irreducible integer polynomials $P(x)$ of degree d .

We further define $e^*(d)$ and $e_{\text{irr}}^*(d)$ by restricting to monic, respectively, monic irreducible integer polynomials, of degree d .

Obviously, we have

$$e(d) \geq e_{\text{irr}}(d) \quad \text{and} \quad e^*(d) \geq e_{\text{irr}}^*(d).$$

Mahler (1964): $e(d) \leq d - 1$ for all d

$$\boxed{d = 2}$$

$$P(X) = aX^2 + bX + c,$$

$$\Delta = b^2 - 4ac, \text{ sep}(P) = \sqrt{|\Delta|}/a$$

$$e_{\text{irr}}(2) = e(2) = 1, \quad e_{\text{irr}}^*(2) = e^*(2) = 0$$

$$\text{E.g. } a = k^2 + k - 1, \quad b = 2k + 1, \quad c = 1, \quad \Delta = 5$$

$$\boxed{d = 3}$$

Evertse (2004), Schönhage (2006):

$$e_{\text{irr}}(3) = e(3) = 2$$

Bugeaud & Mignotte (2010):

$$e_{\text{irr}}^*(3) = e^*(3) \geq 3/2$$

(the equality here is equivalent to Hall's conjecture)

$$d = 4$$

Bugeaud & D. (2011):

$$e_{\text{irr}}(4) \geq 13/6$$

Bugeaud & D. (2013):

$$e(4) \geq 7/3$$

Bugeaud & D. (2013):

$$e_{\text{irr}}^*(4) \geq 7/4$$

Bugeaud & Mignotte (2010):

$$e^*(4) \geq 2$$

D. & Pejković (2011):

explicit family with exponent 2:

$$P_n(x) = (x^2 + x - 1)(x^2 + (1 + F_{n+1})x - (F_n + 1))$$

There is no such family with coefficients which grow polynomially in n , but we can find such families with exponent arbitrary close to 2.

$\limsup e(P) = 2$, where \limsup is taken over all reducible monic integer polynomials $P(x)$ of degree 4.

Bugeaud & Mignotte (2004,2010):

$$e_{\text{irr}}(d) \geq d/2, \quad \text{for even } d \geq 4,$$

$$e(d) \geq (d+1)/2, \quad \text{for odd } d \geq 5,$$

$$e_{\text{irr}}(d) \geq (d+2)/4, \quad \text{for odd } d \geq 5,$$

Beresnevich, Bernik, & Götze (2010):

$$e_{\text{irr}}(d) \geq (d+1)/3, \quad \text{for every } d \geq 2.$$

Bugeaud & Mignotte (2010):

$$e_{\text{irr}}^*(d) \geq (d - 1)/2, \quad \text{for even } d \geq 4,$$

$$e_{\text{irr}}^*(d) \geq (d + 2)/4, \quad \text{for odd } d \geq 5,$$

Beresnevich, Bernik, & Götze (2010):

$$e_{\text{irr}}^*(d) \geq d/3, \quad \text{for every } d \geq 3.$$

Bugeaud & D. (2011):

$$e_{\text{irr}}(d) \geq \frac{d}{2} + \frac{d-2}{4(d-1)} \quad \text{for every } d \geq 4.$$

This result improves all previously known lower bounds for $e_{\text{irr}}(d)$ when $d \geq 4$.

Bugeaud & D. (2011):

$$e_{\text{irr}}^*(d) \geq \frac{d}{2} + \frac{d-2}{4(d-1)} - 1 \quad \text{for odd } d \geq 7.$$

Bugeaud & D. (2013):

$$e(d) \geq \frac{2d}{3} - \frac{1}{3} \quad \text{for every } d \geq 4.$$

This is first result of the form $e(d) \geq C \cdot d$ with $C > \frac{1}{2}$.

Bugeaud & D. (2013):

$$e^*(d) \geq \frac{2d}{3} - 1 \quad \text{for even } d \geq 6$$

$$e^*(d) \geq \frac{2d}{3} - \frac{5}{3} \quad \text{for odd } d \geq 7$$

Bugeaud & D. (2013):

$$e_{\text{irr}}^*(d) \geq \frac{d}{2} - \frac{1}{4} \quad \text{for every } d \geq 4.$$

Theorem 1: $e_{\text{irr}}(d) \geq \frac{d}{2} + \frac{d-2}{4(d-1)}$ for every $d \geq 4$.

To prove this result, we construct explicitly, for any given degree $d \geq 4$, a one-parametric family of irreducible integer polynomials $T_{d,a}(x)$ of degree d .

Examples of small degree:

For $a \geq 1$, the roots of the polynomial

$T_{4,a}(x) = (20a^4 - 2)x^4 + (16a^5 + 4a)x^3 + (16a^6 + 4a^2)x^2 + 8a^3x + 1$,
are approximately equal to:

$$\begin{aligned} r_1 &= -1/4a^{-3} - 1/32a^{-7} - 1/256a^{-13} + \dots, \\ r_2 &= -1/4a^{-3} - 1/32a^{-7} + 1/256a^{-13} + \dots, \\ r_3 &= -2/5a + 11/100a^{-3} + 69/4000a^{-7} + 4/5ai + \dots, \\ r_4 &= -2/5a + 11/100a^{-3} + 69/4000a^{-7} - 4/5ai + \dots \end{aligned}$$

$H(T_{4,a}) = O(a^6)$, $\text{sep}(T_{4,a}) = |r_1 - r_2| = O(a^{-13})$, by letting a tend to infinity we get $e_{\text{irr}}(4) \geq 13/6$.

A similar construction for degree five:

$$T_{5,a}(x) = (56a^5 - 2)x^5 + (56a^6 + 4a)x^4 + (80a^7 + 4a^2)x^3 \\ + (100a^8 + 8a^3)x^2 + 20a^4x + 1$$

with two close roots

$$1/10a^{-4} + 1/250a^{-9} + 3/25000a^{-14} - 3/250000a^{-19} \\ \pm \sqrt{10}/500000a^{-43/2} + \dots,$$

and we obtain that $e_{\text{irr}}(5) \geq 43/16$.

Our construction is applicable as well for $d = 3$. It gives the family

$$T_{3,a}(x) = (8a^3 - 2)x^3 + (4a^4 + 4a)x^2 + 4a^2x + 1$$

with close roots $-1/2a^{-2} - 1/4a^{-5} \pm \sqrt{2}/8a^{-13/2}$, showing that $e_{\text{irr}}(3) \geq 13/8$.

This is weaker than the known result $e_{\text{irr}}(3) = 2$, but in the examples showing that $e_{\text{irr}}(3) = 2$ the coefficients of the polynomials involved have exponential growth, while in our example the coefficients have polynomial growth, only.

We discovered these examples by forcing the discriminant to be as small as possible (as a polynomial in the parameter a). The discriminant $\Delta(P)$ of $P(X)$ is defined by

$$\Delta(P) = |a_d|^{2d-2} \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)^2,$$

where a_d is the leading coefficient of $P(X)$. Recall that $\Delta(P)$ is a (rational) integer and is nonzero if, and only if, $P(X)$ has no multiple roots. In the latter case, we have the following refinement of Mahler's estimate:

$$\text{sep}(P) \gg |\Delta(P)|^{1/2} H(P)^{-d+1}.$$

The constant term of every polynomial $T_{d,a}(x)$ is equal to 1. This means that the reciprocal polynomial of $T_{d,a}(x)$ is monic. Therefore, our result gives also a lower bound for the quantity $e_{\text{irr}}^*(d)$.

Observe that if α and β denote the two very close roots of a polynomial $T_{d,a}(x)$, then α and β satisfy

$$|\alpha|^{-1}, |\beta|^{-1} = O(a^{d-1}) = O(H(T_{d,a})^{1/2}),$$

and

$$\left| \frac{1}{\alpha} - \frac{1}{\beta} \right| = \frac{|\alpha - \beta|}{\alpha\beta}$$

is very small, where $1/\alpha$ and $1/\beta$ are roots of the reciprocal polynomial of $T_{d,a}(x)$.

For $i \geq 0$, let c_i denote the i th Catalan number defined by

$$c_i = \frac{1}{i+1} \binom{2i}{i}.$$

The sequence of Catalan numbers $(c_i)_{i \geq 0}$ begins as

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, \dots$$

and satisfies the recurrence relation

$$c_{i+1} = \sum_{k=0}^i c_k c_{i-k}, \quad \text{for } i \geq 0. \quad (1)$$

For integers $d \geq 3$ and $a \geq 1$, consider the polynomial

$$\begin{aligned} T_{d,a}(x) = & (2c_0 a x^{d-1} + 2c_1 a^2 x^{d-2} + \dots + 2c_{d-2} a^{d-1} x)^2 \\ & - (4c_1 a^2 x^{2d-2} + 4c_2 a^3 x^{2d-3} + \dots + 4c_{d-2} a^{d-1} x^{d+1}) \\ & + (4c_1 a^2 x^{d-2} + 4c_2 a^3 x^{d-3} + \dots + 4c_{d-2} a^{d-1} x) \\ & + 4a x^{d-1} - 2x^d + 1, \end{aligned}$$

which generalizes the polynomials $T_{3,a}(x)$, $T_{4,a}(x)$, $T_{5,a}(x)$.

It follows from the recurrence (1) that $T_{d,a}(x)$ has degree exactly d , and not $2d - 2$, as it seems at a first look. Furthermore, height of $T_{d,a}(x)$ is given by the coefficient of x^2 , that is,

$$H(T_{d,a}) = 4c_{d-2}^2 a^{2d-2} + 4c_{d-3} a^{d-2}.$$

By applying the Eisenstein criterion with the prime 2 on the reciprocal polynomial $x^d T_{d,a}(1/x)$, we see that the polynomial $T_{d,a}(x)$ is irreducible. Indeed, all the coefficients of $T_{d,a}(x)$ except the constant term are even, but its leading coefficient, which is equal to $4c_{d-1} a^d - 2$, is not divisible by 4.

Writing

$$g = g(a, x) = 2c_0ax^{d-1} + 2c_1a^2x^{d-2} + \dots + 2c_{d-2}a^{d-1}x,$$

we see that

$$T_{d,a}(x) = (1 + g)^2 + x^d(4ax^{d-1} - 2(1 + g)).$$

Clearly, $(1 + g)^2$ has a double root, say x_0 , close to $-1/(2c_{d-2}a^{d-1})$. More precisely, we have

$$x_0 = -a^{-d+1}/(2c_{d-2}) + O(a^{-2d+1}).$$

The numerical constants implied in O is independent of a .

The polynomial $T_{d,a}(x)$ has two distinct roots close to x_0 , since the term $x^d(4ax^{d-1} - 2(1 + g))$ is a small perturbation when x is near x_0 .

Let $\delta_0 = \frac{1}{2^{d-1/2}c_{d-2}^{d+1/2}}$. Then for every sufficiently small $\varepsilon > 0$ and sufficiently large a , $T_{d,a}(x)$ has a root x_1 in the interval

$$(x_0 - (\delta_0 + \varepsilon)a^{-d^2+d/2+1}, x_0 - (\delta_0 - \varepsilon)a^{-d^2+d/2+1})$$

and a root x_2 in the interval

$$(x_0 + (\delta_0 - \varepsilon)a^{-d^2+d/2+1}, x_0 + (\delta_0 + \varepsilon)a^{-d^2+d/2+1}).$$

This yields

$$\text{sep}(T_{d,a}) \leq \frac{1}{2^{d-3/2}c_{d-2}^{d+1/2}a^{d^2-d/2-1}}.$$

Since $H(T_{d,a}) = O(a^{2d-2})$, this gives

$$e_{\text{irr}}(d) \geq \frac{2d^2 - d - 2}{4(d-1)} = \frac{d}{2} + \frac{d-2}{4(d-1)},$$

as claimed.

Theorem 2: $e(d) \geq \frac{2d}{3} - \frac{1}{3}$ for every $d \geq 4$.

We want to construct a one-parametric sequence of integer polynomials $p_{d,n}(x)$ of degree d having a root very close to the rational number $x_n = (n+2)/(n^2+3n+1)$. Then the polynomials

$$P_{d,n}(x) = ((n^2 + 3n + 1)x - (n + 2))p_{d-1,n}(x)$$

will have two roots very close to each other. We define the sequence $p_{d,n}(x)$ recursively by

$$p_{0,n}(x) = -1, \quad p_{1,n}(x) = (n+1)x - 1,$$

$$p_{d,n}(x) = (1+x)p_{d-1,n}(x) + x^2p_{d-2,n}(x).$$

It holds

$$p_{d,n}\left(\frac{n+2}{n^2+3n+1}\right) = \frac{(-1)^{d-1}}{(n^2+3n+1)^d}.$$

This allows us to show for sufficiently large n the polynomial $p_{d,n}(x)$ has a root between x_n and

$$z_{d,n} = x_n + \frac{(-1)^d}{n(n^2 + 3n + 1)^d}.$$

Therefore, the polynomial $P_{d,n}(x)$ has two close roots: x_n and $y_{d,n}$, which is between x_n and $z_{d-1,n}$. This yields

$$\text{sep}(P_{d,n}) \leq |x_n - y_{d,n}| \leq \frac{1}{n(n^2 + 3n + 1)^{d-1}} \leq \frac{1}{n^{2d-1}},$$

when n is large enough. Since the height of $P_{d,n}(x)$ is bounded from above by n^3 times a number depending only on d , this gives

$$e(d) \geq \frac{2d-1}{3},$$

by letting n tend to infinity.

Theorem 3: $e^*(d) \geq \frac{2d}{3} - 1$ for even $d \geq 6$,
 $e^*(d) \geq \frac{2d}{3} - \frac{5}{3}$ for odd $d \geq 7$.

In order to get a family of monic polynomials with similar separation properties as the family $P_{d,n}(x)$, we replace the linear non-monic polynomial $L_n(x) = (n^2 + 3n + 1)x - (n + 2)$ by the monic quadratic polynomial

$$K_n(x) = x^2 - (n^2 + 3n + 1)x + (n + 2).$$

Thus, we want to construct a one-parametric sequence of integer polynomials $q_{d,n}(x)$ of degree d having a root very close to the root $y_n = 1/n + O(1/n^2)$ of $K_n(x)$. Then the polynomials

$$Q_{d,n}(x) = (x^2 - (n^2 + 3n + 1)x + (n + 2))q_{d-2,n}(x)$$

will have two roots very close to each other.

For $d \geq 0$ even, we define the sequence $q_{d,n}(x)$ recursively by

$$q_{0,n}(x) = 1, \quad q_{2,n}(x) = x^2 - (n+1)x + 1,$$

$$q_{d,n}(x) = (2x^2 + x + 1)q_{d-2,n}(x) - x^4 q_{d-4,n}(x).$$

Note that $q_{d,n}(x) - q_{d-2,n}(x)q_{2,n}(x)$ is divisible by $K_n(x)$. This yields that

$$q_{d,n}(y_n) = q_{d-2,n}(y_n)q_{2,n}(y_n) = (q_{2,n}(y_n))^{d/2},$$

for $d \geq 2$ even. From

$$y_n = 1/n - 1/n^2 + 2/n^3 - 4/n^4 + 8/n^5 + O(1/n^6),$$

we get $q_{2,n}(y_n) = 1/n^4 + O(1/n^5)$ and hence

$$q_{d,n}(y_n) = 1/n^{2d} + O(1/n^{2d+1}).$$

It can be shown that for sufficiently large n the polynomial $q_{d,n}(x)$ has a root between y_n and $w_{d,n} = y_n + \frac{2}{n^{2d+1}}$. Thus, the polynomial $Q_{d,n}(x)$ has two close roots: y_n and $v_{d,n}$, which is between y_n and $w_{d-2,n}$. This yields

$$\text{sep}(Q_{d,n}) \leq \frac{2}{n^{2d-3}},$$

when n is large enough. Since $H(Q_{d,n}) = O(n^3)$, this gives

$$e^*(d) \geq \frac{2d-3}{3},$$

by letting n tend to infinity.

Let now d be odd. Then we define

$$Q_{d,n}(x) = x(x^2 - (n^2 + 3n + 1)x + (n + 2))q_{d-3,n}(x).$$

This polynomial has two close roots: y_n and a root lying between y_n and $w_{d-3,n}$. Thus we get

$$\text{sep}(Q_{d,n}) \leq \frac{2}{n^{2d-5}},$$

for n large enough, and

$$e^*(d) \geq \frac{2d-5}{3}.$$

Theorem 4: $e_{\text{irr}}^*(d) \geq \frac{d}{2} - \frac{1}{4}$ for every $d \geq 4$.

We use the polynomials $p_{d,n}(x)$ to construct irreducible monic polynomials having two very close roots.

Let F_k denote the k th Fibonacci number. Note that Fibonacci numbers appear in the asymptotic expansion of $x_n = (n + 2)/(n^2 + 3n + 1)$, namely

$$x_n = 1/n - 1/n^2 + 2/n^3 - 5/n^4 + \cdots - (-1)^k F_{2k-3}/n^k + \cdots$$

For $d \geq 0$, we first define monic polynomials $s_{d,n}(x)$ with a root close to x_n by

$$s_{d,n}(x) = (-1)^{d-1}(F_{d-1}p_{d,n}(x) - F_d x p_{d-1,n}(x)),$$

and then monic polynomials with two close roots by

$$r_{2d+1,n}(x) = x s_{d,n}^2(x) + F_d^2 p_{d,n}^2(x),$$

$$r_{2d,n}(x) = s_{d,n}^2(x) + F_{d-1}^2 x p_{d-1,n}^2(x).$$

We claim that these polynomials are monic. It suffices to show that this is true for $s_{d,n}(x)$. Since the leading coefficient of $p_{d,n}(x)$ is $F_d n + F_{d-2}$, we deduce that the leading coefficient of $s_{d,n}(x)$ is equal to

$$\begin{aligned} & (-1)^{d-1}(F_{d-1}(F_d n + F_{d-2}) - F_d(F_{d-1}n + F_{d-3})) \\ &= (-1)^{d-1}(F_{d-1}F_{d-2} - F_d F_{d-3}) = 1. \end{aligned}$$

We have

$$r_{d,n}(x_n) = F_{[(d-1)/2]}^2/n^{2d-3} + O(1/n^{2d-2}).$$

Observe that the degree of the polynomial $r_{d,n}(x)$ is d and $H(r_{d,n}) = O(n^2)$.

It can be shown that $r_{d,n}(x)$ has two complex conjugate roots $v_{d,n}$ and $\overline{v_{d,n}}$ close to x_n , more precisely they are equal to

$$\begin{aligned} &1/n - 1/n^2 + 2/n^3 - 5/n^4 + 13/n^5 - \dots + \\ &+ (-1)^d F_{2d-5}/n^{d-1} \pm i/n^{(2d-1)/2} + O(1/n^d). \end{aligned}$$

It is not straightforward, but it can be shown that for sufficiently large positive integer n the polynomial $r_{d,n}(x)$ is irreducible over $\mathbb{Z}[x]$. The argument uses estimates for the resultant of the polynomials $R_{d,n}(x)$ and $L_n(x)$, where $R_{d,n}(x)$ denotes the irreducible factor of $r_{d,n}(x)$ having roots $v_{d,n}$ and $\overline{v_{d,n}}$. These estimates give that the degree of $R_{d,n}(x)$ is either d or $d - 1$, and it is possible to exclude the later possibility for sufficiently large n .

Since

$$\text{sep}(r_{d,n}) = O(n^{-(d-1/2)}),$$

we obtain

$$e_{\text{irr}}^*(d) \geq \frac{2d - 1}{4}.$$

Hall's conjecture: For any $\varepsilon > 0$, there exists a constant $c(\varepsilon) > 0$ such that if x and y are positive integers such that $x^3 - y^2 \neq 0$, then

$$|x^3 - y^2| > c(\varepsilon)x^{1/2-\varepsilon}.$$

It is known that Hall's conjecture follows from the *abc*-conjecture (there is a stronger version of Hall's conjecture which is equivalent to the *abc*-conjecture).

Consider a cubic polynomial

$$P(X) = X^3 + pX + q.$$

Its discriminant is $\Delta(P) = -4p^3 - 27q^2$. Thus, we are interested how small can be the quantity $4p^3 + 27q^2$ compared with $\max\{|p|, |q|\}$. And by taking $p = -3x$, $q = 2y$ we actually ask how small can be the quantity $|x^3 - y^2|$, so this explains connection of root separation problem for monic irreducible cubic polynomials with Hall's conjecture.

Let us mention our recent result concerning Hall's conjecture for polynomials.

Davenport (1965): For non-constant complex polynomials x and y , such that $x^3 \neq y^2$, we have

$$\deg(x^3 - y^2) / \deg(x) > 1/2.$$

Zannier (1995): For any positive integer δ there exist complex polynomials x and y such that $\deg(x) = 2\delta$, $\deg(y) = 3\delta$ and $\deg(x^3 - y^2) = \frac{1}{2} \deg(x) + 1$.

Birch, Chowla, Hall and Schinzel (1965), Elkies (2000): There exist polynomials with integer coefficients such that $\deg(x^3 - y^2) / \deg(x) = 0.6$.

D. (2011): For any $\varepsilon > 0$ there exist polynomials x and y with integer coefficients such that $x^3 \neq y^2$ and $\deg(x^3 - y^2) / \deg(x) < 1/2 + \varepsilon$.

More precisely, for any even positive integer δ there exist polynomials x and y with integer coefficients such that $\deg(x) = 2\delta$, $\deg(y) = 3\delta$ and $\deg(x^3 - y^2) = \delta + 5$.

Here is part of an explicit example which improves the quotient $\deg(x^3 - y^2)/\deg(x) = 0.6$ from the above mentioned examples by Birch, Chowla, Hall, Schinzel and Elkies, as

$$\deg(x^3 - y^2)/\deg(x) = 31/52 = 0.5961\dots :$$

$$\begin{aligned} x &= 281474976710656t^{52} + 3799912185593856t^{50} + \\ &\quad \dots \\ &\quad + 496080t^5 + 130625t^4 + 15750t^3 + 629t^2 + 150t + 4, \end{aligned}$$

$$\begin{aligned} y &= 4722366482869645213696t^{78} + \\ &\quad \dots \\ &\quad + 11812545t^5 + 642429t^4 + 94050t^3 + 6591t^2 + 225t + 19, \end{aligned}$$

$$\begin{aligned} x^3 - y^2 &= -905969664t^{31} - 8380219392t^{29} - 35276193792t^{27} \\ &\quad - 89379569664t^{25} - 151909171200t^{23} - 182680289280t^{21} \\ &\quad - 159752355840t^{19} - 102786416640t^{17} - 48661447680t^{15} \\ &\quad - 16772918400t^{13} - 4116359520t^{11} - 692649360t^9 \\ &\quad - 75171510t^7 - 297t^6 - 4749570t^5 - 891t^4 - 144450t^3 \\ &\quad - 891t^2 - 1350t - 297. \end{aligned}$$