


Polynomial root separation

Andrej Dujella

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

*Joint work with Yann Bugeaud, Tomislav Pejković and
Bruno Salvy*

Supported by the Croatian Science Foundation under the project

no. 6422. 

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.

We may consider also the absolute variant of the problem, where we ask for the minimal nonzero distance between absolute values of the roots.

Remark: The computing times required by algorithms for isolating the zeros of a separable polynomial P depend inversely on the minimal distance between its roots.

Algorithms for determining the asymptotic expansion of solution of linear recurrences depend on the distance between moduli of two dominant roots (roots with the largest modulus).

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

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

Similarly, we define $e_{\text{irr}}(d)$ if the 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 .

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

Trivial results: $e_{\text{irr}}(2) = e(2) = 1$, $e_{\text{irr}}^*(2) = e^*(2) = 0$.

$$\boxed{d = 3}$$

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. (2014):

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

Bugeaud & D. (2014):

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

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, i.e.

$$e_{\text{red}}^*(4) = 2.$$

p -adic version

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

Pejković (2016):

- quadratic polynomials: $\text{sep}_p(P_k) \asymp H(P_k)^{-1}$
(best possible)
- reducible cubic polynomials: $\text{sep}_p(P_k) \asymp H(P_k)^{-2}$
(best possible)
- irreducible cubic polynomials: $\text{sep}_p(P_k) \asymp H(P_k)^{-25/14}$

Bugeaud & Mignotte (2004,2010):

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

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

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

Beresnevich, Bernik & Götze (2010):

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

Bugeaud & Mignotte (2010):

$$e^*(d) \geq d/2, \quad \text{for even } d \geq 4,$$

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

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

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

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

Let $d = 4$. 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 tends to infinity we get $e_{\text{irr}}(4) \geq 13/6$.

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

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

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 polynomial $T_{4,a}(x)$.

It follows from the recurrence 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.

Bugeaud & D. (2014):

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

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

Bugeaud & D. (2014):

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

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

Bugeaud & D. (2014):

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

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

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

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

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

D. & Pejković (2017):

$$7/3 \leq e^*(5) \leq 3, \quad 17/5 \leq e^*(7) \leq 5, \quad 31/7 \leq e^*(9) \leq 7$$

$$T_{5,n} = (x^2 + n^2x - n)(x^3 + nx - 1)$$

close roots: $1/n - 1/n^4 + (2, 3)/n^7 + \dots$

$$T_{7,n} = (x^2 + n^3x - n)(x^5 + nx^3 + n^2x - 1)$$

roots: $1/n^2 - 1/n^7 + 2/n^{12} + (-4, -5)/n^{17} + \dots$

$$T_{9,n} = (x^2 + n^4x - n)(x^7 + nx^5 + n^2x^3 + n^3x - 1)$$

roots: $1/n^3 - 1/n^{10} + 2/n^{17} - 5/n^{24} + (14, 15)/n^{31} + \dots$

Can be generalized to $(d^2 - 2d - 1)/(2d - 4) \leq e^*(d) \leq d - 2$; the lower bound is asymptotically weaker than Theorem 2.

Theorem 3: $e_{\text{irr}}^*(d) \geq \frac{d}{2} - \frac{1}{4}$ 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

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

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

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

The **absolute** variant of the problem: the minimal nonzero distance between absolute values of the roots:

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

Gourdon & Salvy (1996), Dubickas & Sha (2015):

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

Bugeaud, D., Pejković & Salvy (2017): Let $\alpha_1 = \alpha, \alpha_2 = \beta, \alpha_3, \dots, \alpha_d \in \mathbb{C}$ 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 $i, j \in \{1, \dots, d\}$. If α and β are real then

$$\left| |\alpha| - |\beta| \right| \geq 2^{(-d^2+2)/2} (d+1)^{(-d+1)/2} H(P)^{-d+1}.$$

Moreover, the exponent of $H(P)$ is best possible.

Families of polynomials that reach the exponent $-d + 1$:

The construction starts from $Mx^2 - 1$ which has two real roots $\pm 1/\sqrt{M}$. By perturbing $Mx^2 - 1$ in appropriate ways we get polynomials of the form $(Mx^2 - 1)u(x) + v(x)$ with roots very close to $\pm 1/\sqrt{M}$ and whose sum is small.

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:

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

If M tends to infinity, then the polynomial $P_{d,M}(x)$ has height M and two roots $\alpha, \beta \in \mathbb{R}$ satisfying

$$0 < ||\alpha| - |\beta|| = \alpha + \beta \sim M^{-d+1} = H(P_{d,M})^{-d+1}.$$

The polynomial $P_{3,M}$ has two roots α_3, β_3 satisfying

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

This can be proved by giving small enough intervals where the polynomial $P_{d,M}(x)$ changes sign:

$$\begin{aligned}P_{3,M}(-M^{-1/2} + \frac{1}{2}M^{-2} - M^{-3}) &= -2M^{-5/2} + O(M^{-3}) < 0, \\ P_{3,M}(-M^{-1/2} + \frac{1}{2}M^{-2}) &= \frac{5}{4}M^{-3} + O(M^{-4}) > 0,\end{aligned}$$

for M large enough, and similarly for the other root.

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

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

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

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

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

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

For $d \geq 3$, these polynomials are monic and irreducible over \mathbb{Q} .

Indeed, 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 the following result then implies that $P_{d,M}(x)$ is irreducible for M large enough in terms of d .

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

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