Root separation for reducible integer polynomials

Andrej Dujella

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

Joint work with Yann Bugeaud

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 $\alpha_1, \ldots, \alpha_d$, we set

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

and define $e(P)$ by $\mathrm{sep}(P) = H(P)^{-e(P)}$.
For $d \geq 2$, we set

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

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

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

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

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

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

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

$\boxed{d = 3}$

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)

$\boxed{d = 4}$

Bugeaud & D. (2011):

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

Bugeaud & D. (2014):

$e(4) \geq 7/3$

Bugeaud & D. (2014):

$e^*_{\mathrm{irr}}(4) \geq 7/4$

Bugeaud & Mignotte (2010):

$e^*(4) \geq 2$

D. & Pejković (2011):
explicit family with exponent 2:

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

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

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

Pejković (2012):

- quadratic polynomials: $\mathrm{sep}_p(P_k) \asymp H(P_k)^{-1}$ (best possible)

- reducible cubic polynomials: $\mathrm{sep}_p(P_k) \asymp H(P_k)^{-2}$ (best possible)

- irreducible cubic polynomials: $\mathrm{sep}_p(P_k) \asymp H(P_k)^{-25/14}$

Bugeaud & Mignotte (2004,2010):

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

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

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

Beresnevich, Bernik, & Götze (2010):

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

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):

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

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

Bugeaud & D. (2011):

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

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):

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

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

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

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

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

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

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

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

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

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

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

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

for n large enough, and

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

Work in progress:

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

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

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

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

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

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

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

Might be generalized to $e^*(d) \geq (d^2 - 2d - 1)/(2d - 4)$
– 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 kth 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

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

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

$$1/n - 1/n^2 + 2/n^3 - 5/n^4 + 13/n^5 - \ldots + \\ +(-1)^d F_{2d-5}/n^{d-1} \pm i/n^{(2d-1)/2} + O(1/n^d).$$

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

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