Root distance of polynomials

Jan-Hendrik Evertse
Universiteit Leiden

Kálmán Győry 75 symposium

July 10, 2015, Debrecen

Slides can be downloaded from
http://pub.math.leidenuniv.nl/∼evertsejh/lectures.shtml

Mahler's Lemma

Let $f = a_0 \prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ of degree $n \geq 2$ with $a_0 \in \mathbb{Z}$ and distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ and define

$$\begin{aligned}
\mathrm{sep}(f) &:= \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j| \ \text{(minimal root distance of } f\text{)},\\
M(f) &:= |a_0| \prod_{i=1}^{n} \max(1, |\alpha_i|) \ \text{(Mahler measure of } f\text{)},\\
D(f) &:= a_0^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \ \text{(discriminant of } f\text{)}.
\end{aligned}$$

Lemma 1 (Mahler, 1964)

$\mathrm{sep}(f) \geq c(n)|D(f)|^{1/2} M(f)^{1-n}$ *(with* $c(n) = \sqrt{3} \cdot n^{-(n+2)/2}$*).*

Mahler's Lemma

Let $f = a_0 \prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ of degree $n \geq 2$ with $a_0 \in \mathbb{Z}$ and distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ and define

$$\begin{aligned}
\mathrm{sep}(f) &:= \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j| \ \text{ (minimal root distance of } f\text{)}, \\
M(f) &:= |a_0| \prod_{i=1}^{n} \max(1, |\alpha_i|) \ \text{ (Mahler measure of } f\text{)}, \\
D(f) &:= a_0^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \ \text{ (discriminant of } f\text{)}.
\end{aligned}$$

Lemma 1 (Mahler, 1964)

$\mathrm{sep}(f) \geq c(n)|D(f)|^{1/2} M(f)^{1-n}$ *(with $c(n) = \sqrt{3} \cdot n^{-(n+2)/2}$).*

Proof (ignoring value of $c(n)$).

$$\mathrm{sep}(f) \gg_n \prod_{1 \leq i < j \leq n} \frac{|\alpha_i - \alpha_j|}{\max(1, |\alpha_i|) \max(1, |\alpha_j|)} \gg_n |D(f)|^{1/2} M(f)^{1-n}.$$

□

Mahler's Lemma (II)

Lemma 1 (Mahler, 1964)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 2$. Then

$$\mathrm{sep}(f) \geq c(n)|D(f)|^{1/2}M(f)^{1-n} \text{ with } c(n) > 0.$$

Since $D(f) \in \mathbb{Z} \setminus \{0\}$, this implies

Corollary

$\mathrm{sep}(f) \geq c(n)M(f)^{1-n}$.

Can this be improved to an inequality with something larger in terms of $M(f)$ on the right-hand side?

Mahler's Lemma (II)

Lemma 1 (Mahler, 1964)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 2$. Then

$$\mathrm{sep}(f) \geq c(n)|D(f)|^{1/2} M(f)^{1-n} \text{ with } c(n) > 0.$$

Since $D(f) \in \mathbb{Z} \setminus \{0\}$, this implies

Corollary

$\mathrm{sep}(f) \geq c(n) M(f)^{1-n}$.

Can this be improved to an inequality with something larger in terms of $M(f)$ on the right-hand side?

NO if $n = 2, 3$; **YES** if $n \geq 4$.

Polynomials of degree at most 3

For a polynomial $f(X)$ of degree $n \geq 2$ and $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ define $f_U(X) := (cX + d)^n f(\frac{aX+b}{cX+d})$.

Call two polynomials $f, g \in \mathbb{Z}[X]$ *equivalent* if $g = f_U$ for some $U \in \mathrm{GL}_2(\mathbb{Z})$.

Theorem 1

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \in \{2, 3\}$. In case that $n = 3$, assume that f has a real, irrational zero. Then there are infinitely many polynomials $g \in \mathbb{Z}[X]$ such that g is equivalent to f and

$$\mathrm{sep}(g) \ll_f M(g)^{1-n}.$$

For $n = 2$ the proof is straightforward, for $n = 3$ this is a result of Schönhage (2006). His proof uses the convergents of a real irrational zero of f.

Theorem 1 is false for cubic f with three rational roots or one rational and two non-real roots.

An alternative proof of Schönhage's Theorem

Lemma 2

Let $n \geq 3$ and let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be distinct, with $\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$. Then $\mathbb{Z}^2$ has infinitely many bases $\{\mathbf{z}_1 = (a, b), \mathbf{z}_2 = (c, d)\}$ such that

$$|a - \alpha_1 b|,\ |c - \alpha_1 d| \ll \max(|a|, |b|, |c|, |d|)^{-1},$$
$$|a - \alpha_i b| \ll |c - \alpha_i d| \quad \text{for } i = 2, \ldots, n.$$

Here the implied constants depend on $\alpha_1, \ldots, \alpha_n$.

Proof (idea).

Apply Minkowski's Theorem on successive minima to the convex bodies $C_Q := \{(x, y) \in \mathbb{R}^2 : |x - \alpha_1 y| \leq Q^{-1},\ |y| \leq Q\}$ $(Q \geq 1)$. □

An alternative proof of Schönhage's Theorem (ctd)

Let $f = a_0(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \in \mathbb{Z}[X]$ with $\alpha_1, \alpha_2, \alpha_3$ distinct and $\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$.

Choose a basis $\{\mathbf{z}_1 = (a, b),\ \mathbf{z}_2 = (c, d)\}$ of $\mathbb{Z}^2$ according to Lemma 2 and let

$$g(X) := a_0 \prod_{i=1}^{3} \big((c - \alpha_i d)X - (a - \alpha_i b)\big), \quad \beta_i := \frac{a - \alpha_i b}{c - \alpha_i d} \quad (i = 1, 2, 3).$$

Then g is equivalent to f.

An alternative proof of Schönhage's Theorem (ctd)

Let $f = a_0(X-\alpha_1)(X-\alpha_2)(X-\alpha_3) \in \mathbb{Z}[X]$ with $\alpha_1, \alpha_2, \alpha_3$ distinct and $\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$.

Choose a basis $\{\mathbf{z}_1 = (a,b),\ \mathbf{z}_2 = (c,d)\}$ of $\mathbb{Z}^2$ according to Lemma 2 and let

$$g(X) := a_0 \prod_{i=1}^{3} \big((c-\alpha_i d)X - (a-\alpha_i b)\big), \quad \beta_i := \frac{a-\alpha_i b}{c-\alpha_i d} \quad (i=1,2,3).$$

Then g is equivalent to f.

Put $A_i := \max(|a-\alpha_i b|, |c-\alpha_i d|)$ $(i=1,2,3)$. Then

$$\begin{aligned} A_1 &\ll_f \max(|a|,|b|,|c|,|d|)^{-1} \ll_f A_2^{-1}, A_3^{-1}, \\ A_i &\ll_f |c-\alpha_i d| \ \text{ for } i=2,3, \\ M(g) &= |a_0| \cdot A_1 A_2 A_3, \end{aligned}$$

An alternative proof of Schönhage's Theorem (ctd)

Let $f = a_0(X-\alpha_1)(X-\alpha_2)(X-\alpha_3) \in \mathbb{Z}[X]$ with $\alpha_1, \alpha_2, \alpha_3$ distinct and $\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$.

Choose a basis $\{\mathbf{z}_1 = (a,b),\ \mathbf{z}_2 = (c,d)\}$ of $\mathbb{Z}^2$ according to Lemma 2 and let

$$g(X) := a_0 \prod_{i=1}^{3} \big((c-\alpha_i d)X - (a-\alpha_i b)\big), \quad \beta_i := \frac{a-\alpha_i b}{c-\alpha_i d} \quad (i=1,2,3).$$

Then g is equivalent to f.

Put $A_i := \max(|a-\alpha_i b|, |c-\alpha_i d|)$ $(i=1,2,3)$. Then

$$\begin{aligned} A_1 &\ll_f \max(|a|,|b|,|c|,|d|)^{-1} \ll_f A_2^{-1}, A_3^{-1}, \\ A_i &\ll_f |c-\alpha_i d| \text{ for } i=2,3, \\ M(g) &= |a_0| \cdot A_1 A_2 A_3, \end{aligned}$$

hence
$$\operatorname{sep}(g) \le |\beta_2-\beta_3| = \frac{|ad-bc|}{|c-\alpha_2 d|\cdot|c-\alpha_3 d|} \ll_f (A_2A_3)^{-1} \ll_f (A_1A_2A_3)^{-2} \ll_f M(g)^{-2}. \qquad \square$$

Polynomials of degree at least 4

For polynomials $f \in \mathbb{Z}[X]$ of degree ≤ 3, Mahler's inequality is best possible in terms of $M(f)$.

For polynomials of degree ≥ 4 we can do slightly better.

Theorem 2 (Ev. and Győry)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then

$$\mathrm{sep}(f) \geq c(n)M(f)^{1-n}(\log 2M(f))^{1/(10n-6)},$$

where $c(n) > 0$ is effectively computable.

Polynomials of degree at least 4

For polynomials $f \in \mathbb{Z}[X]$ of degree ≤ 3, Mahler's inequality is best possible in terms of $M(f)$.

For polynomials of degree ≥ 4 we can do slightly better.

Theorem 2 (Ev. and Győry)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then

$$\mathrm{sep}(f) \geq c(n) M(f)^{1-n} (\log 2M(f))^{1/(10n-6)},$$

where $c(n) > 0$ is effectively computable.

Conjecture

For $f \in \mathbb{Z}[X]$ a separable polynomial of degree $n \geq 4$ we have

$$\mathrm{sep}(f) \geq c_1(n) M(f)^{1-n+c_2(n)}$$

with $c_1(n) > 0$, $c_2(n) > 0$.

Polynomials with small minimal root distance

Mignotte, Bugeaud and Mignotte, and Bugeaud and Dujella gave explicit examples of polynomials $f \in \mathbb{Z}[X]$ of arbitrary degree $n \geq 4$ such that $\mathrm{sep}(f)$ is small compared with $M(f)$. We recall the best results to date.

Theorem (Bugeaud and Dujella, 2011, 2014)

Let $n \geq 4$, $\epsilon > 0$. Then there are infinitely many irreducible $f \in \mathbb{Z}[X]$ of degree n such that

$$\mathrm{sep}(f) \leq M(f)^{-a(n)+\epsilon} \quad \textit{with } a(n) = \frac{n}{2} + \frac{n-2}{4(n-1)},$$

and also infinitely many reducible, separable $f \in \mathbb{Z}[X]$ of degree n such that

$$\mathrm{sep}(f) \leq M(f)^{-b(n)+\epsilon} \quad \textit{with } b(n) = \frac{2n-1}{3}.$$

On the proof of Theorem 2

- Recall Mahler's Lemma $\mathrm{sep}(f) \gg_n |D(f)|^{1/2} M(f)^{1-n}$, $n = \deg f$.

  To get a lower bound for $\mathrm{sep}(f)$ better than $M(f)^{1-n}$ in terms of $M(f)$, we need a non-trivial lower bound for $|D(f)|$.

- $|D(f)|$ can not be estimated from below in terms of $M(f)$:

  Recall that two polynomials $f, g \in \mathbb{Z}[X]$ of degree n are called equivalent if there is $U \in \mathrm{GL}(2, \mathbb{Z})$ such that $g = f_U$, i.e., if $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $g(X) = (cX + d)^n f(\frac{aX+b}{cX+d})$.

  Equivalent polynomials have the same discriminant.

  So by varying f in an equivalence class one can make $M(f)$ arbitrarily large while fixing $D(f)$.

- But by means of Baker theory we can show that there is $g \in \mathbb{Z}[X]$ equivalent to f with small Mahler measure in terms of $|D(f)|$.

  This provides a useful lower bound for $|D(f)|$.

Polynomials of small Mahler measure in an equivalence class

Theorem 3 (Ev. and Győry, recent improvement of result from 1991)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then there is $g \in \mathbb{Z}[X]$ such that g is equivalent to f and

$$M(g) \leq \exp\left((17n^3)^{25n^2}|D(f)|^{5n-3}\right).$$

Polynomials of small Mahler measure in an equivalence class

Theorem 3 (Ev. and Győry, recent improvement of result from 1991)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then there is $g \in \mathbb{Z}[X]$ such that g is equivalent to f and

$$M(g) \leq \exp\left((17n^3)^{25n^2} |D(f)|^{5n-3}\right).$$

For polynomials of degree ≤ 3 much sharper results follow from classical work of Lagrange, Gauss and Hermite.

The main tool

Let K be a number field. Denote by O_K its ring of integers, by D_K its discriminant and d its degree. For non-zero $a, b, c \in O_K$ define

$$H_K(a, b, c) := \prod_{\sigma : K \hookrightarrow \mathbb{C}} \max\left(|\sigma(a)|, |\sigma(b)|, |\sigma(c)|\right).$$

Proposition 4 (Győry, 1978)

There are effectively computable $c_1(d), c_2(d) > 0$ *such that for all* $a, b, c \in O_K$ *with* $a + b = c$, $abc \neq 0$ *we have*

$$H_K(a, b, c) \leq (2|N_{K/\mathbb{Q}}(abc)|)^{c_1(d)|D_K|^{c_2(d)}}.$$

Proof.

Baker type lower bounds for linear forms in logarithms. The sharpest, completely explicit version of Proposition 4 to date is due to Győry and Yu (2006). □

Idea of proof of Theorem 3

Theorem 3

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then there is $g \in \mathbb{Z}[X]$ such that g is equivalent to f and

$$M(g) \leq \exp\left((17n^3)^{25n^2} |D(f)|^{5n-3}\right).$$

Proof (idea).

Let K be the splitting field of f and write $f = \prod_{i=1}^{n} (\beta_i X - \gamma_i)$ with β_i, γ_i "almost" in O_K. Put $\Delta_{ij} := \beta_i \gamma_j - \beta_j \gamma_i$ and apply Győry's and Yu's explicit version of Proposition 4 to

$$\Delta_{ij}\Delta_{kl} + \Delta_{jk}\Delta_{il} = \Delta_{ik}\Delta_{jl} \quad \forall i, j, k, l.$$

Idea of proof of Theorem 3

Theorem 3

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then there is $g \in \mathbb{Z}[X]$ such that g is equivalent to f and

$$M(g) \leq \exp\left((17n^3)^{25n^2}|D(f)|^{5n-3}\right).$$

Proof (idea).

Let K be the splitting field of f and write $f = \prod_{i=1}^{n}(\beta_i X - \gamma_i)$ with β_i, γ_i "almost" in O_K. Put $\Delta_{ij} := \beta_i\gamma_j - \beta_j\gamma_i$ and apply Győry's and Yu's explicit version of Proposition 4 to

$$\Delta_{ij}\Delta_{kl} + \Delta_{jk}\Delta_{il} = \Delta_{ik}\Delta_{jl} \quad \forall i, j, k, l.$$

Together with geometry of numbers, this implies that there is g equivalent to f with an upper bound for $M(g)$ which is polynomial in $|D(f)|$ but with $|D_K|$ in the exponent.

Estimating $|D_K|$ in terms of $D(f)$, this leads to an upper bound for $M(g)$ which is exponential in $|D(f)|$. □

Proof of Theorem 2

Theorem 2

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then

$$\mathrm{sep}(f) \geq c(n)M(f)^{1-n}(\log 2M(f))^{1/(10n-6)},$$

where $c(n) > 0$ is effectively computable.

This is proved by combining Theorem 3 with the following improvement of Mahler's Lemma.

Lemma (Ev., 1993)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$ and let $g \in \mathbb{Z}[X]$ be equivalent to f. Then

$$\mathrm{sep}(f) \geq c(n)|D(f)|^{1/2}M(f)^{-1}M(g)^{2-n},$$

where $c(n) > 0$ is effectively computable.

Proof of Theorem 2

Theorem 2

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \geq 4$. Then

$$\mathrm{sep}(f) \geq c(n) M(f)^{1-n} (\log 2M(f))^{1/(10n-6)},$$

where $c(n) > 0$ is effectively computable.

Proof of Theorem 2.

Choose g equivalent to f of minimal Mahler measure. Then

$$\begin{aligned}
\mathrm{sep}(f) &\gg_n |D(f)|^{1/2} M(f)^{-1} M(g)^{2-n} \\
&\gg_n M(f)^{-1} M(g)^{2-n} \big(\log 2M(g)\big)^{1/(10n-6)} \\
&\gg_n M(f)^{1-n} \big(\log 2M(f)\big)^{1/(10n-6)}.
\end{aligned}$$

□

Clusters of p-adic roots

We generalize the previous results to other absolute values and also to estimates for clusters of roots.

Let $M_{\mathbb{Q}} := \{\infty\} \cup \{\text{primes}\}$, $|\cdot|_\infty$ ordinary absolute value, $|\cdot|_p$ p-adic absolute value with $|p|_p = p^{-1}$ for p a prime.
For $p \in M_{\mathbb{Q}}$ we extend $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$, where $\mathbb{Q}_\infty = \mathbb{R}$, $\overline{\mathbb{Q}_\infty} = \mathbb{C}$.

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree n and $p \in M_{\mathbb{Q}}$.
Write $f(X) = a_0 \prod_{i=1}^{n}(X - \alpha_{i,p})$ with $a_0 \in \mathbb{Z}$, $\alpha_{i,p} \in \overline{\mathbb{Q}_p}$ and define

$$\begin{aligned} \mathrm{sep}_p(f) = \mathrm{sep}_{2,p}(f) &:= \min_{1 \le i < j \le n} |\alpha_{i,p} - \alpha_{j,p}|_p \quad (n \ge 2), \\ \mathrm{sep}_{k,p}(f) &:= \min_{|I|=k} \prod_{\{i,j\} \subset I} |\alpha_{i,p} - \alpha_{j,p}|_p \quad (k \ge 2,\ n \ge k), \end{aligned}$$

where the minimum is taken over all k-element subsets I of $\{1, \dots, n\}$ and the product over all 2-element subsets of I.

A generalization of Mahler's Lemma

Recall $\mathrm{sep}_{k,p}(f) := \min_{|I|=k} \prod_{\{i,j\}\subset I} |\alpha_{i,p} - \alpha_{j,p}|_p$ for $f(X) = a_0 \prod_{i=1}^{n} (X - \alpha_{i,p})$.

Lemma 3

Let $S = \{\infty, p_1, \ldots, p_t\}$, $k \in \mathbb{Z}_{\geq 2}$, and $f \in \mathbb{Z}[X]$ a separable polynomial of degree $n \geq k$. Then

$$\prod_{p\in S} \min\left(1, \mathrm{sep}_{k,p}(f)\right) \geq c(n) \Big(\prod_{p\in S} |D(f)|_p \Big)^{1/2} \cdot M(f)^{1-n},$$

where $c(n) > 0$ is effectively computable.

A generalization of Mahler's Lemma

Recall $\mathrm{sep}_{k,p}(f) := \min_{|I|=k} \prod_{\{i,j\}\subset I} |\alpha_{i,p} - \alpha_{j,p}|_p$ for $f(X) = a_0 \prod_{i=1}^{n}(X - \alpha_{i,p})$.

Lemma 3

Let $S = \{\infty, p_1, \ldots, p_t\}$, $k \in \mathbb{Z}_{\geq 2}$, and $f \in \mathbb{Z}[X]$ a separable polynomial of degree $n \geq k$. Then

$$\prod_{p\in S} \min\left(1, \mathrm{sep}_{k,p}(f)\right) \geq c(n)\Big(\prod_{p\in S} |D(f)|_p\Big)^{1/2} \cdot M(f)^{1-n},$$

where $c(n) > 0$ is effectively computable.

Corollary

$$\prod_{p\in S} \min\left(1, \mathrm{sep}_{k,p}(f)\right) \geq c(n)M(f)^{1-n}.$$

Can this be improved in terms of $M(f)$?

A generalization of Mahler's Lemma

Recall $\mathrm{sep}_{k,p}(f) := \min_{|I|=k} \prod_{\{i,j\}\subset I} |\alpha_{i,p} - \alpha_{j,p}|_p$ for $f(X) = a_0 \prod_{i=1}^{n}(X - \alpha_{i,p})$.

Lemma 3

Let $S = \{\infty, p_1, \ldots, p_t\}$, $k \in \mathbb{Z}_{\geq 2}$, and $f \in \mathbb{Z}[X]$ a separable polynomial of degree $n \geq k$. Then

$$\prod_{p\in S} \min\left(1, \mathrm{sep}_{k,p}(f)\right) \geq c(n)\Big(\prod_{p\in S} |D(f)|_p\Big)^{1/2} \cdot M(f)^{1-n},$$

where $c(n) > 0$ is effectively computable.

Corollary

$$\prod_{p\in S} \min\left(1, \mathrm{sep}_{k,p}(f)\right) \geq c(n)M(f)^{1-n}.$$

Can this be improved in terms of $M(f)$?

NO if $n \in \{k, k+1\}$; **YES** if $n \geq k+2$.

A generalization of Schönhage's Theorem

A polynomial $f \in \mathbb{Z}[X]$ is called *primitive* if its coefficients have gcd 1.

We call two polynomials $f, g \in \mathbb{Z}[X]$ $\mathrm{GL}_2(\mathbb{Q})$-equivalent if $g = \lambda f_U$ for some $\lambda \in \mathbb{Q}^*$, $U \in \mathrm{GL}_2(\mathbb{Q})$.

Theorem 5

Let $p \in M_{\mathbb{Q}}$, $k \in \mathbb{Z}_{\geq 2}$ and $f \in \mathbb{Z}[X]$ a primitive, separable polynomial of degree $n \in \{k, k+1\}$. In case that $n = k+1$, assume that f has a zero in $\mathbb{Q}_p \setminus \mathbb{Q}$.

Then there are infinitely many $g \in \mathbb{Z}[X]$, such that g is primitive, $\mathrm{GL}(2, \mathbb{Q})$-equivalent to f, and

$$\mathrm{sep}_{k,p}(g) \ll_{p,f} M(g)^{1-n}.$$

Proof.

Adèlic geometry of numbers. □

A generalization of Schönhage's Theorem

A polynomial $f \in \mathbb{Z}[X]$ is called *primitive* if its coefficients have gcd 1.

We call two polynomials $f, g \in \mathbb{Z}[X]$ $\mathrm{GL}_2(\mathbb{Q})$-equivalent if $g = \lambda f_U$ for some $\lambda \in \mathbb{Q}^*$, $U \in \mathrm{GL}_2(\mathbb{Q})$.

Theorem 5

Let $p \in M_{\mathbb{Q}}$, $k \in \mathbb{Z}_{\geq 2}$ and $f \in \mathbb{Z}[X]$ a primitive, separable polynomial of degree $n \in \{k, k+1\}$. In case that $n = k+1$, assume that f has a zero in $\mathbb{Q}_p \setminus \mathbb{Q}$.

Then there are infinitely many $g \in \mathbb{Z}[X]$, such that g is primitive, $\mathrm{GL}(2, \mathbb{Q})$-equivalent to f, and

$$\mathrm{sep}_{k,p}(g) \ll_{p,f} M(g)^{1-n}.$$

Pejkovic (2012, PhD-thesis) constructed in another way, for every prime p, an infinite class of separable cubic $g \in \mathbb{Z}[X]$ with $\mathrm{sep}_p(g) \ll M(g)^{-2}$.

Polynomials of degree at least $k+2$

Theorem 6

Let $k \in \mathbb{Z}_{\geq 2}$, $n \geq k+2$, $S = \{\infty, p_1, \ldots, p_t\}$. There is an effectively computable number $c(n,S) > 0$ such that for every separable polynomial $f \in \mathbb{Z}[X]$ of degree n we have

$$\prod_{p \in S} \min\left(1, \mathrm{sep}_{k,p}(f)\right) \geq c(n,S) M(f)^{1-n} (\log 2M(f))^{1/(10n-6)}.$$

Proof.

p-adic generalization of arguments sketched above. □

A conditional result

Theorem 7

Assuming the abc-conjecture over number fields, the following holds:

Let $S = \{\infty, p_1, \dots, p_t\}$, $k \in \mathbb{Z}_{\geq 2}$, $f \in \mathbb{Z}[X]$ *a separable polynomial of degree* $n \geq k+2$. *Then*

$$\prod_{p \in S} \min(1, \mathrm{sep}_{k,p}(f)) \geq c(n,S) M(f)^{1-n+\gamma(1-k/n)^2},$$

where $c(n,S) > 0$ *depends only on* n, S, *and* $\gamma > 0$ *is an absolute constant.*

This lower bound is probably far from the truth.

Congratulations Kálmán!