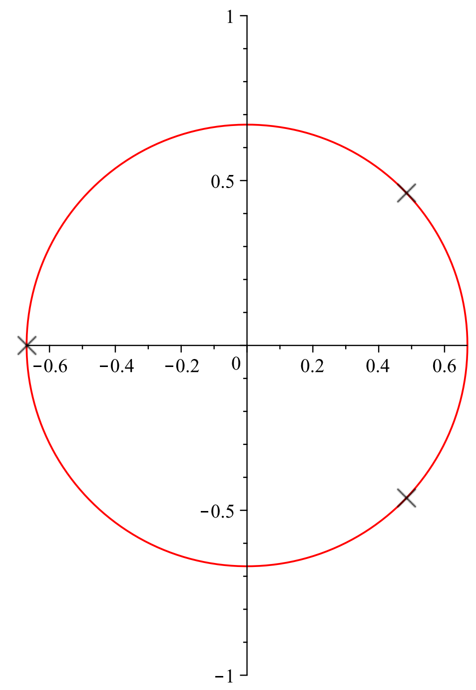
Absolute Root Separation

Bruno Salvy

AriC, Inria, ENS de Lyon



AMM, 2017

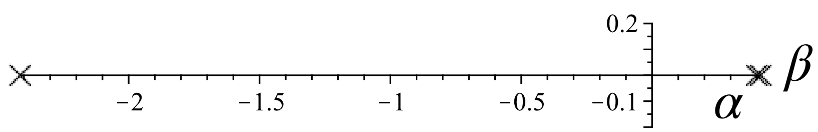
Exp. Maths., 2020

AriC seminar, March 2020

Joint work with Yann Bugeaud, Andrej Dujella, Wenjie Fang and Tomislav Pejković

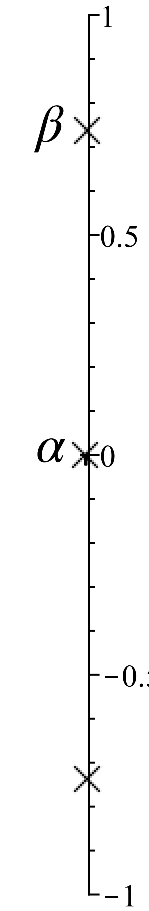
Close Roots of Polynomials

$$P \in \mathbb{Z}[X] \qquad P(\alpha) = P(\beta) = 0$$

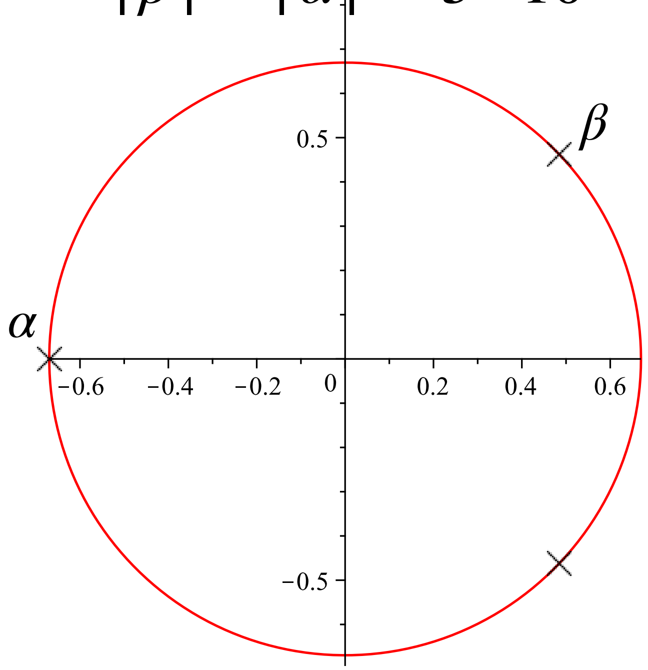


$$P = 5X^3 - 8X^2 - 9X + 2$$
$$\beta - \alpha \simeq 10^{-2}$$

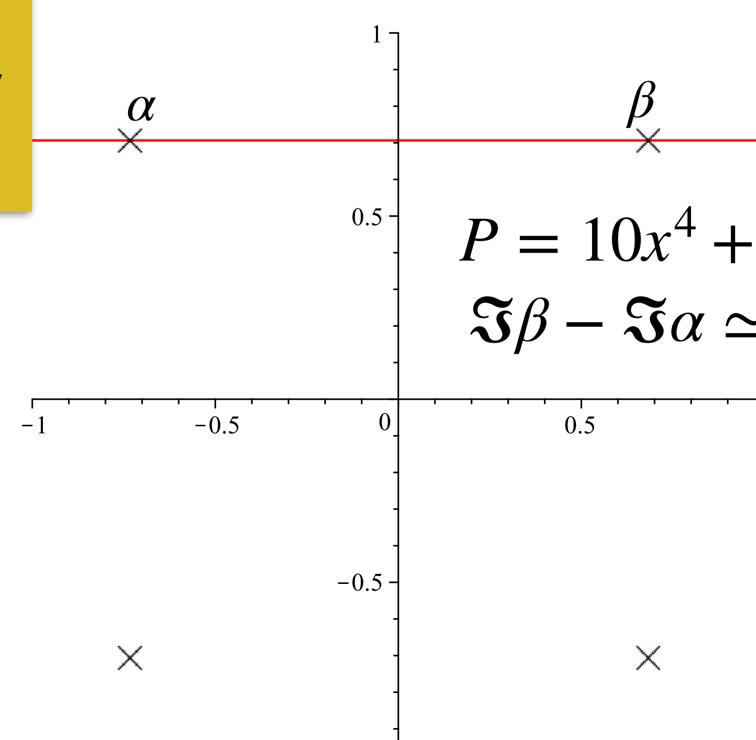
$$P = 7X^3 + 5X^2 + 5X + 1$$
$$\Re\beta - \Re\alpha \simeq 6 \cdot 10^{-4}$$



$$P = 10X^3 - 3X^2 - 2X + 3$$
$$|\beta| - |\alpha| \simeq 5 \cdot 10^{-4}$$



Aim: Bound precision needed to **decide** that two roots have identical value/real part/imaginary part/absolute value ?



$$P = 10x^4 + x^3 + 10$$
$$\Im\beta - \Im\alpha \simeq 6 \cdot 10^{-5}$$

Mahler's Bound

Def. Separation

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

Def. Height

$$H\left(\sum_{i=0}^{d} a_i X^i\right) := \max_i |a_i| \,.$$

Thm. If $P \in \mathbb{Z}[X]$ has degree d,

$$\operatorname{sep}(P) > \kappa(d)\, H(P)^{-d+1} \,.$$

explicit function of d

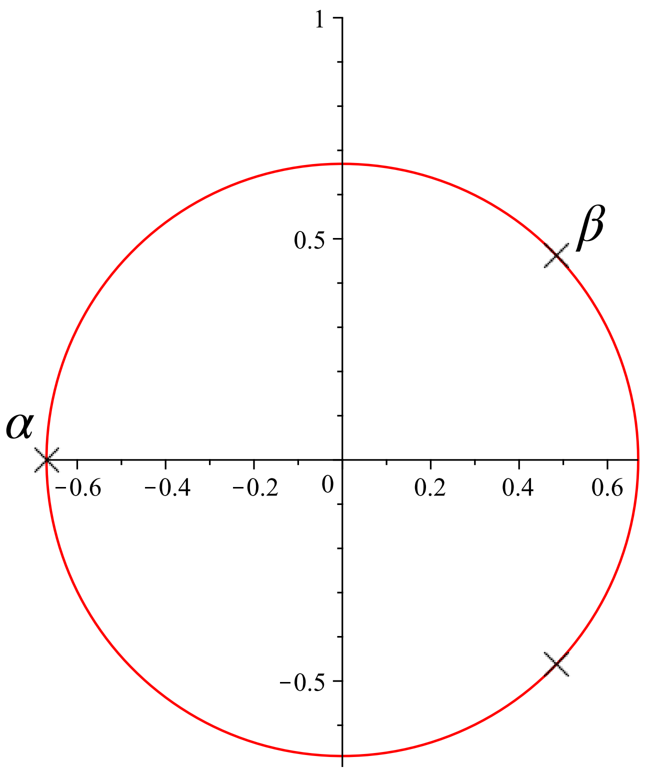
not known to be tight (except for d=3)

worst known family gives $-(2d-1)/3$.

Note: Computing isolating disks of radius $2^{-\kappa}$ for all roots can be done in time $\tilde{O}(d^3 + d^2 \log H(P) + d\kappa)$.

[Mahler 64; Evertse 04; Schönhage 06; BugeaudDujella 14; Mehlhorn, Sagraloff 15-16]

Absolute Separation



Motivation: asymptotics of linear recurrences & diagonals

Def. Absolute Separation

$$\operatorname{abssep}(P) := \min_{\substack{P(\alpha)=P(\beta)=0,\\ |\alpha|\neq|\beta|}} \Big|\,|\alpha|-|\beta|\,\Big| .$$

Aims:

not the same as before

1. $\operatorname{abssep}(P) > \kappa(d)\, H(P)^{-e(d)}$ with $e(d)$ small;

2. families for small d with

$$\operatorname{abssep}(P_H) \underset{H\to\infty}{\sim} \kappa' H^{-e'} \text{ and } e' \text{ large}.$$

Results

Previously $\quad e(d) \le d(d^2 + 2d - 1)/2 \quad$ 1996

$e(d) \le d^3/2 - d^2 - d/2 + 2 \quad$ 2015

$e(d) \le d^3/2 - d^2 - d/2 + 1 \quad (d \ge 4) \quad$ 2019

New: $e(3) = 4, \quad 5 \le e(4) \le 12, \quad 6 \le e(5) \le 24, \quad 7 \le e(6) \le 30,$

$$e(d) \le (d-1)(d-2)(d-3)/2 = d^3/2 - 3d^2 + \cdots \qquad (d \ge 4)\,.$$

+ more precise bounds when one or two of the roots are real
+ bounds on the separation between real/imaginary parts

[GourdonSalvy 96; DubickasSha 15; Sha 19]

II. Proof Technique for Upper Bounds

Auxiliary Polynomials

From $P(X) = \sum_{i=0}^{d} a_i X^i = a_d \prod_{i=1}^{d} (X - \alpha_i) \in \mathbb{Z}[X]$ of height $H(P)$

construct

$$M(X) = a_d^{2(d-1)} \prod_{i<j} (X - (\alpha_i - \alpha_j)^2) \in \mathbb{Z}[X]$$

and lower bound its nonzero roots.

Prop. 1 [Cauchy] If $\alpha \neq 0$,

$$P(\alpha) = 0 \Rightarrow |\alpha| \geq \frac{1}{1 + H(P)}.$$

Prop. 2 [Symmetric fcns]

$G \in \mathbb{Z}[X_1, \ldots, X_d]$ symmetric

with $\deg_{X_i} G \leq k$ for all i

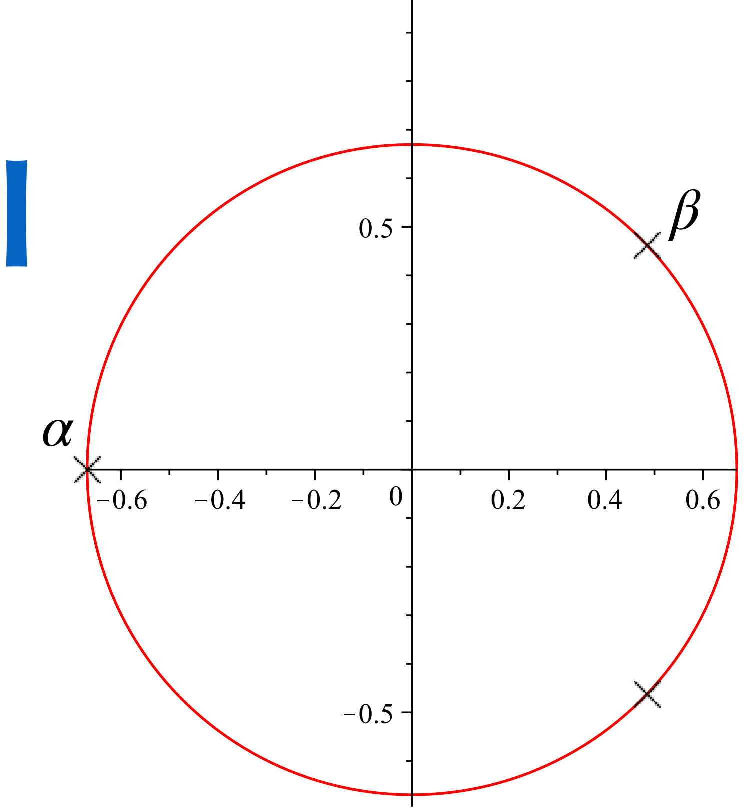
$\Rightarrow a_d^k G(\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}[a_0, \ldots, a_d]$

of total degree $\leq k$.

Application to $M \to |\alpha_i - \alpha_j|^2 > \kappa H^{-2(d-1)}$.

Recovers Mahler's exponent

A Bigger Polynomial



$$a_d^{(d-1)(d-2)(d-3)} \prod_{\substack{i<j,\\ k<\ell,\\ \{i,j\}\cap\{k,\ell\}=\varnothing}} \left(X^{1/2} - (\alpha_i\alpha_j - \alpha_k\alpha_\ell) \right)$$

gives exponent $(d-1)(d-2)(d-3)/2$ for the general case

More Auxiliary Polynomials

$$a_d^{2(d-1)} \prod_{i<j} (X - (\alpha_i + \alpha_j)^2)$$

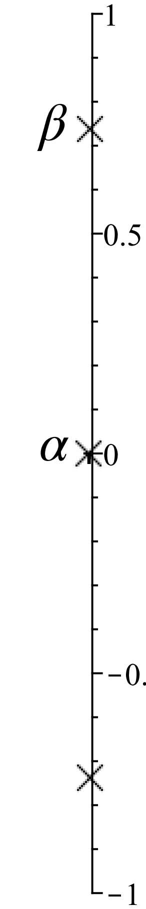
$$\alpha_j, \alpha_k \text{ real} \Rightarrow \Big| |\alpha_j| - |\alpha_k| \Big| > \kappa H^{-(d-1)}$$

optimal

$$a_d^{2(d-1)(d-2)} \prod_{i<j, k \notin \{i,j\}} (X - (\alpha_k^2 - \alpha_i \alpha_j))$$

$$\alpha_k \text{ real} \Rightarrow \Big| |\alpha_j| - |\alpha_k| \Big| > \kappa H^{-2(d-1)(d-2)}$$

Variants (×↦+)



$$a_d^{\frac{3}{2}(d-1)(d-2)} \prod_{i<j,k\notin\{i,j\}} \Big(X - (\alpha_i + \alpha_j - 2\alpha_k)\Big)$$

$$\alpha_k \text{ real} \Rightarrow \left|\alpha_k - \Re\alpha_i\right| > \kappa H^{-3(d-1)(d-2)/2}$$

$$a_d^{(d-1)(d-2)(d-3)} \prod_{\substack{i<j,\\ k<\ell,\\ \{i,j\}\cap\{k,\ell\}=\varnothing}} \Big(X^{1/2} - (\alpha_i + \alpha_j - \alpha_k - \alpha_\ell)\Big)$$

$$\left|\Re\alpha_k - \Re\alpha_i\right| > \kappa H^{-(d-1)(d-2)(d-3)/2}$$

and similarly for imaginary parts.

III. Experiments in Low Degree

Exhaustive Search

1. Solve the $(2H+1)^{d+1}$ pols in $\mathbb{Z}[X]_{\leq d}$ with height $\leq H$

and keep the records.

Ex.: $d=3,\ H=20 \rightarrow$ approx. 300,000 polynomials. (15 min.)
$d=4,\ H=20 \rightarrow$ approx. $115\ 10^6$ polynomials. (19 h)

2. Refine the search in the neighborhood of those; look for patterns

	abssep	real root
$17x^3+9x^2+7x+8$	$1.9\ 10^{-5}$	-0.7778352845
$102x^3+97x^2+71x+40$	$1.5\ 10^{-8}$	-0.7319587393
$153x^3-97x^2-71x+60$	$4.5\ 10^{-9}$	-0.7319587525
$181x^3+153x^2+112x+71$	$9.0\ 10^{-10}$	-0.7320261422

$\approx 1-\sqrt{3}$?

Degree 3: Optimal Exponent -4

Key polynomial:

$$P(X,Y) = X^3 - X^2 + 1 + \left(\frac{X^3}{2} - \frac{X^2}{3} + \frac{2}{3}X + 1\right)Y$$

$$P(X,\sqrt{3}) = \frac{\sqrt{3}+2}{6}\left(X - \sqrt{3} + 1\right)\left(X^2 + aX + (\sqrt{3}-1)^2\right), \quad a < 2(\sqrt{3}-1)\,.$$

discr<0 —> 3 roots with same modulus

Perturbation:

$P(X,\sqrt{3}+\epsilon)$ has a real root at $\sqrt{3} - 1 + (2-\sqrt{3})\epsilon + O(\epsilon^2)$

and a nonreal one with similar modulus, but a different O() term.

If p_n/q_n is the nth convergent of the continued fraction of $\sqrt{3}$,
$P_n(X) := 6q_nP(X, p_n/q_n) \in \mathbb{Z}[X], \quad \mathrm{abssep}(P_n) < \kappa\, H(P_n)^{-4}\,.$

Proof: $|p_n/q_n - \sqrt{3}| < 1/q_n^2\,.$

$$\sqrt{3} = 1 + \cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\ddots}}}$$

Perturbative Method (4≤deg≤6)

Principle

$$P(X,\epsilon) = R(X) + \epsilon\, Q(X)$$

with roots of identical |.|

with undeterminate coefficients

1. Pick two nonconjugate roots α, β of R

2. Compute expansions $\alpha(\epsilon), \beta(\epsilon)$ of roots of P with $\alpha(0) = \alpha, \beta(0) = \beta$ in $\mathbb{Q}(\alpha)[q_0, \ldots, q_d][[\epsilon]]$ (or β)

3. Form the expansion of $|\alpha(\epsilon)|^2 - |\beta(\epsilon)|^2$ in $\mathbb{Q}(\alpha,\beta)[q_0, \ldots, q_d][[\epsilon]]$

4. Look for a nondegenerate integer solution of the system formed by its first coefficients

Demo

Results

deg	R	Q	exponent
4	$x^4 - 1$	$x^3 - x^2 + x - 5$	-5
4	$(x^2 - 1)(x^2 + x + 1)$	$x^3 - 3x - 4$	-5
6	$x^6 - 1$	$9x^5 - 9x^4 - 26x^3 - 9x^2 + 9x - 28$	-7
5	$(x^2 + ax + r^2)(x^2 + bx + r^2)$ $\lvert a\rvert < 2r, \lvert b\rvert < 2r$	Too big for the Gröbner basis computation	

Loop over small values of a,b,r gives:

$$a = -9,\ b = -11,\ r = 6,\ Q = X^5 - 213X^3 + 2404X^2 - 11088X + 20736$$

exponent -6

Conclusion

New ideas needed

. to produce polynomials with small absolute separation in low degree;

. to generalize the key polynomial of degree 3;

. to produce (or disprove the existence of) subcubic exponents.

The End