Moscow Journal of Combinatorics and Number Theory

2020
vol. 9 no. 4

Algebraic integers close to the unit circle

Artūras Dubickas

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 9, No. 4, 2020
https://doi.org/10.2140/moscow.2020.9.361

Algebraic integers close to the unit circle

Artūras Dubickas

We show that for each $d \geq 3$ there is a monic integer polynomial P of degree d which is irreducible over $\mathbb{Q}$ and has two complex conjugate roots as close to the unit circle as is allowed by the Liouville-type inequality.

1. Introduction

For a polynomial

$$P(x) := a(x-\alpha_1)\cdots(x-\alpha_d) \in \mathbb{Z}[x], \quad a \neq 0, \tag{1}$$

of degree $d \geq 2$ let $H(P)$ be its *height*, i.e., the maximum modulus of its coefficients, and let

$$M(P) := |a| \prod_{k=1}^{d} \max\{1, |\alpha_k|\}$$

be its *Mahler measure*. A polynomial root separation problem is to find the smallest possible nonzero distance between the roots of $P \in \mathbb{Z}[x]$ of fixed degree d in terms of $H(P)$ (or $M(P)$), when $H(P)$ (resp. $M(P)$) tends to infinity. By a result of [Mahler 1964], the smallest possible such distance must be at least $\sqrt{3}d^{-d/2-1}M(P)^{1-d}$. The exponent $1-d$ for $M(P)$ is the best possible if $d = 2$ (trivially) and also if $d = 3$, as proved in [Evertse 2004; Schönhage 2006]. The question of whether the exponent $1-d$ is the best possible for $d \geq 4$ is still open; see [Bugeaud and Dujella 2011; 2014; Bugeaud and Mignotte 2004; 2010; Dujella and Pejković 2011; Herman et al. 2018].

Recently, in [Bugeaud et al. 2017] it was shown that the modulus of the sum $\alpha_i + \alpha_j$, where α_i, α_j are real roots of P, is either 0 or bounded below by $c_1(d)M(P)^{1-d}$, where $c_1(d)$ depends on d only, and, moreover, that the exponent $1-d$ is the best possible; that is, there exists a monic irreducible polynomial $P \in \mathbb{Z}[x]$ of degree d whose two real roots α_i, α_j satisfy $0 < |\alpha_i + \alpha_j| < c_2(d)M(P)^{1-d}$.

The above-mentioned root separation problem is essentially an estimation of $\min_{i\neq j} |\alpha_i/\alpha_j - 1|$. As observed in [Dubickas 2013], this quantity has an advantage over the standard root separation $\operatorname{sep}(P) := \min_{i\neq j} |\alpha_i - \alpha_j|$ because it remains the same if we replace P by its reciprocal polynomial $P^*(x) = x^d P(1/x)$. In this context, it seems natural to consider a kind of symmetric separation $\min_{1\leq i,j\leq d} |\alpha_i - 1/\alpha_j|$ or

$$\operatorname{symsep}(P) := \min_{\substack{1\leq i,j\leq d\\ \alpha_i\alpha_j\neq 1}} |\alpha_i\alpha_j - 1|.$$

We claim that

$$\operatorname{symsep}(P) \geq 2^{1-d(d-1)/2} M(P)^{1-d} \tag{2}$$

for $d \geq 3$.

MSC2010: primary 11C08; secondary 12D10.
Keywords: irreducible polynomial, roots close to 1, Mahler measure, resultant.

We will prove (2) by a Liouville-type argument essentially the same as that in [Feldman 1981, Theorem 5.3] and [Waldschmidt 2000, Lemma 3.14]. (It seems that those results do not imply (2) directly when α_i, α_j are both real.)

Fix a pair of indices (i, j), where $1 \le i, j \le d$ and $i \neq j$. Then, for the number $\gamma = \alpha_i\alpha_j \neq 1$ of degree, say n, we have $M(\gamma) \le M(P)^{d-1}$, where P is defined in (1), since the minimal polynomial of γ, say $Q(x) = c\prod_{\ell=1}^{n}(x-\gamma_\ell) \in \mathbb{Z}[x]$, divides the polynomial

$$a^{d-1} \prod_{1\le k<l\le d} (x-\alpha_k\alpha_l) \in \mathbb{Z}[x].$$

Next, in view of $\gamma \neq 1$ we have $1 \le |Q(1)| = |c|\prod_{\ell=1}^{n}|1-\gamma_\ell|$. Using the estimates $|1-\gamma_\ell| \le 2\max\{1, \gamma_\ell\}$ for every $\ell \ge 2$ we derive that

$$1 \le |\gamma-1|2^{n-1}M(\gamma) \le |\gamma-1|2^{n-1}M(P)^{d-1}. \tag{3}$$

Note that $n = \deg(\alpha_i\alpha_j) \le d(d-1)/2$, with equality if and only if either $d = 2$ or (when $d \ge 3$) P is irreducible over $\mathbb{Q}$ and the Galois group of its splitting field is 2-transitive. In particular, if P is reducible, $d \ge 3$, and α_i, α_j are the roots of its distinct irreducible factors then

$$\deg(\alpha_i\alpha_j) \le \deg\alpha_i \deg\alpha_j \le \deg\alpha_i(d-\deg\alpha_i) < d(d-1)/2.$$

Therefore, as $\gamma = \alpha_i\alpha_j$, for each $d \ge 2$ from (3) it follows that

$$|\alpha_i\alpha_j - 1| \ge 2^{1-d(d-1)/2}M(P)^{1-d} \tag{4}$$

for any pair of indices $i \neq j$ from the set $\{1, \dots, d\}$ such that $\alpha_i\alpha_j \neq 1$.

We next claim that for each $d \ge 2$ and each $i \in \{1, \dots, d\}$

$$|\alpha_i^2 - 1| \ge 2^{1-d}M(P)^{-1} \tag{5}$$

if $\alpha_i \neq \pm 1$. Indeed, if $|\alpha_i^2 - 1| \ge 1$ then (5) holds trivially. Otherwise, one has either $|\alpha_i - 1| < 1$ or $|\alpha_i + 1| < 1$. Without loss of generality we may assume that $|\alpha_i - 1| < 1$. Then, by $|\alpha_i - 1| \ge 2^{1-d}M(P)^{-1}$ and

$$|\alpha_i + 1| = |2 + \alpha_i - 1| \ge 2 - |\alpha_i - 1| \ge 2 - 1 = 1,$$

we find that $|\alpha_i^2 - 1| = |\alpha_i - 1||\alpha_i + 1| \ge 2^{1-d}M(P)^{-1}$, which is (5).

Since the right-hand side of (4) does not exceed that of (5) for $d \ge 3$, the combination of (4) and (5) yields (2) for each $d \ge 3$. For $d = 2$ the right-hand side of (5) is smaller than that of (4), so $\operatorname{symsep}(P) \ge 2^{-1}M(P)^{-1}$.

As in the above-mentioned problem [Bugeaud et al. 2017], we will show that the exponent $1-d$ in (2) is the best possible and give some other properties of the polynomial with two roots very close to the unit circle.

Theorem 1. *For each $d \ge 3$ and each sufficiently large positive integer H there is a monic, irreducible over $\mathbb{Q}$ polynomial $P(x) = \prod_{j=1}^{d}(x-\beta_{j,H}) \in \mathbb{Z}[x]$ with $M(P) = H(P) = H$ whose two roots $\beta_{d-1,H}, \beta_{d,H}$ with smallest moduli are complex conjugate and satisfy*

$$\operatorname{symsep}(P) = |\beta_{d-1,H}\beta_{d,H} - 1| = |\beta_{d,H}|^2 - 1 \sim H^{1-d} \quad \text{as } H \to \infty. \tag{6}$$

For the resultant of this polynomial P and its reciprocal $P^*(x) = x^d P(1/x)$ we have

$$|\mathrm{Res}(P, P^*)| = |P(1)P(-1)| = 3H^2 + u_d H + v_d, \tag{7}$$

where $u_d, v_d \in \mathbb{Z}$, and the roots of P satisfy

$$\prod_{1 \le k < l \le d} |\beta_{k,H}\beta_{l,H} - 1| = 1. \tag{8}$$

Note that for $d = 2$ we can take $P(x) = (H-1)x^2 - H$, where $H \ge 2$. Then, $M(P) = H(P) = H$ and $\mathrm{symsep}(P) = (H-1)^{-1}$, so (6) holds for $d = 2$ too, but in this example P is not monic.

In the next section we will present some lemmas. The proof of Theorem 1 is given in Section 3.

2. Lemmas for polynomials of the form $f(x) - H(x^2 + x + 1)$

Consider the sequence of monic integer polynomials $g_d(x)$, $d = 1, 2, 3, \ldots$, defined by $g_1(x) := x + 1$ and

$$g_d(x) := \frac{g_{d-1}(x) - g_{d-1}(0)}{x}(1 + x + x^2) + 1 \tag{9}$$

for $d = 2, 3, 4, \ldots$. Then, step by step, we find that

$$\begin{aligned}
g_2(x) &= x^2 + x + 2,\\
g_3(x) &= x^3 + 2x^2 + 2x + 2,\\
g_4(x) &= x^4 + 3x^3 + 5x^2 + 4x + 3,\\
g_5(x) &= x^5 + 4x^4 + 9x^3 + 12x^2 + 9x + 5,\\
g_6(x) &= x^6 + 5x^5 + 14x^4 + 25x^3 + 30x^2 + 21x + 10,\\
g_7(x) &= x^7 + 6x^6 + 20x^5 + 44x^4 + 69x^3 + 76x^2 + 51x + 22,
\end{aligned}$$

etc.

Although it is defined (and written) in a different way, one can verify that it is the same sequence of polynomials as that introduced in Sections 4.1 and 4.2 of [Uray 2019]. See the formulas (4.1), (4.2) (and a table below them) and the actual construction of polynomials in (4.8) of [Uray 2019]. One can formally check that the recurrence relations (4.1), (4.2) hold for the coefficients of the polynomials $xg_{d-1}(x)$, where g_d is introduced in (9). Our polynomials (9) are monic (not with leading coefficients -1), so in order to get the polynomials (4.8) as in Section 4.2 of [Uray 2019] with minus sign, we do not add but subtract from the polynomial $xg_{d-1}(x)$ of degree d the quadratic polynomial $Hx^2 + Hx + H$.

The next lemma is Theorem 2.4 of [Uray 2019].

Lemma 2. *For each $d \ge 3$ and each sufficiently large positive integer H the polynomial*

$$xg_{d-1}(x) - H(x^2 + x + 1)$$

has two complex conjugate roots, say $\beta_{d-1,H}$ and $\beta_{d,H} = \overline{\beta_{d-1,H}}$, whose moduli satisfy

$$(|\beta_{d-1,H}| - 1)H^{d-1} = (|\beta_{d,H}| - 1)H^{d-1} \sim \tfrac{1}{2} \quad \textit{as } H \to \infty. \tag{10}$$

Note that, by (9), $xg_{d-1}(x)$ is a monic integer polynomial of degree d with zero constant term whose other coefficients are positive. The proof of Theorem 2.4 in [Uray 2019] is based on some manipulation with a certain matrix obtained from the coefficients of the polynomial $xg_{d-1}(x) - H(x^2+x+1)$; see Lemma 4.2 in [Uray 2019]. In particular, one needs to show that this polynomial has all its roots outside the unit circle for H large enough. We will also prove such a statement but in a different way and in a more general setting. More precisely, in the next lemma we describe the location of the roots of polynomials of the form $f(x) - H(x^2+x+1)$, where $f \in \mathbb{Z}[x]$ is a fixed monic polynomial, and in addition show the irreducibility of such polynomials over $\mathbb{Q}$.

Lemma 3. *Let $d \geq 3$ and let*

$$f(x) := x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a monic polynomial, not divisible by x^2+x+1. Then, for each sufficiently large positive integer H the polynomial

$$P(x) := f(x) - H(x^2+x+1) \tag{11}$$

is irreducible over $\mathbb{Q}$ and its roots $\alpha_{1,H}, \dots, \alpha_{d,H}$ can be labeled so that

$$|\alpha_{j,H} - e^{2\pi i j/(d-2)} H^{1/(d-2)}| < \frac{d(1+|a_{d-1}-1|)}{d-2} \tag{12}$$

for $j = 1, \dots, d-2$ and

$$|\alpha_{d-1,H} - e^{2\pi i/3}| = |\alpha_{d,H} - e^{-2\pi i/3}| < \frac{dL(f)}{H}, \tag{13}$$

where $L(f) := 1 + \sum_{k=0}^{d-1} |a_k|$.

Proof. Let $\xi \in \mathbb{C}$ be any complex number satisfying $P'(\xi) \neq 0$. We will show that if α is the root of P nearest to ξ then

$$|\alpha - \xi| \leq \frac{d|P(\xi)|}{|P'(\xi)|}. \tag{14}$$

The result is trivial if ξ is a root of P. If not, we have $P'(\xi)P(\xi) \neq 0$, and so

$$\frac{P'(\xi)}{P(\xi)} = \sum_{j=1}^{d} \frac{1}{\xi - \alpha_{j,H}}.$$

This yields $|P'(\xi)/P(\xi)| \leq d/|\xi - \alpha|$, which implies (14).

We first will apply (14) to $\xi = e^{2\pi i/3}$. According to (11), we obtain

$$|P(e^{2\pi i/3})| = |f(e^{2\pi i/3})| \leq 1 + \sum_{k=0}^{d-1} |a_k| = L(f).$$

Also,

$$P'(e^{2\pi i/3}) = f'(e^{2\pi i/3}) - H(2e^{2\pi i/3}+1) = f'(e^{2\pi i/3}) - i\sqrt{3}H,$$

so $|P'(e^{2\pi i/3})| \sim H\sqrt{3}$ as $H \to \infty$. Consequently, for each sufficiently large H we have

$$\frac{d|P(e^{2\pi i/3})|}{|P'(e^{2\pi i/3})|} \leq \frac{0.9dL(f)}{H}.$$

Thus, by (14), for each sufficiently large H the circle with center at $e^{2\pi i/3}$ and radius $0.9dL(f)/H$ contains a root of P. This, combined with the same argument for $\xi = e^{-2\pi i/3}$, implies the existence of two roots of P satisfying (13). Equality in (13) holds, because the roots $\alpha_{d-1,H}$ and $\alpha_{d,H}$ must be complex conjugate by (12).

In order to prove (12) we fix $j \in \{1, \dots, d-2\}$ and apply (14) to the number $\xi_j := e^{2\pi ij/(d-2)} H^{1/(d-2)}$. From $\xi_j^{d-2} = H$ and

$$P(x) = x^2(x^{d-2} - H) + x(a_{d-1}x^{d-2} - H) + (a_{d-2}x^{d-2} - H) + \sum_{k=0}^{d-3} a_k x^k,$$

it follows that

$$P(\xi_j) = e^{2\pi ij/(d-2)}(a_{d-1} - 1)H^{1+/(d-2)} + (a_{d-2} - 1)H + \sum_{k=0}^{d-3} a_k \xi_j^k.$$

The modulus of the last sum $\sum_{k=0}^{d-3} a_k \xi_j^k$ is clearly less than H for H large enough. Hence,

$$|P(\xi_j)| < \left(\tfrac{1}{2} + |a_{d-1} - 1|\right) H^{1+1/(d-2)} \tag{15}$$

for each sufficiently large H. Similarly, from

$$P'(x) = x(dx^{d-2} - 2H) + (d-1)a_{d-1}x^{d-2} - H + \sum_{k=1}^{d-2} k a_k x^{k-1},$$

it follows that $|P'(\xi_j)| \sim (d-2)H^{1+1/(d-2)}$ as $H \to \infty$. Combining this with (15), we find that

$$\frac{d|P(\xi_j)|}{|P'(\xi_j)|} < \frac{d(1 + |a_{d-1} - 1|)}{d-2}$$

for H large enough. Hence, by (14), we derive the existence of the root of P, say $\alpha_{j,H}$, satisfying (12).

It remains to prove that P is irreducible. For a contradiction, suppose P is reducible, that is, $P(x) = P_1(x)P_2(x)$, where $P_1, P_2 \in \mathbb{Z}[x]$ are of degrees say $d_1 \geq 1$ and $d_2 \geq 1$, respectively. Since $\alpha_{d-1,H}$ and $\alpha_{d,H}$ are the roots of the same irreducible factor of P, without restriction of generality we may assume that they both are roots of P_1. Inserting $x = e^{2\pi i/3}$ and $x = e^{-2\pi i/3}$ into $P(x)$, by (11), we find that

$$\begin{aligned} f(e^{2\pi i/3})f(e^{-2\pi i/3}) &= P(e^{2\pi i/3})P(e^{-2\pi i/3}) \\ &= P_1(e^{2\pi i/3})P_1(e^{-2\pi i/3})P_2(e^{2\pi i/3})P_2(e^{-2\pi i/3}). \end{aligned}$$

Here, as $f(x)$ is not divisible by $x^2 + x + 1$, the modulus of the left-hand side is a nonzero integer, which is bounded above by $L(f)^2$. By (12), we get $|P_2(e^{\pm 2\pi i/3})| \sim H^{d_2/(d-2)}$ as $H \to \infty$. Hence,

$$0 < |P_1(e^{2\pi i/3})P_1(e^{-2\pi i/3})| = \frac{|f(e^{2\pi i/3})f(e^{-2\pi i/3})|}{|P_2(e^{2\pi i/3})P_2(e^{-2\pi i/3})|} < \frac{2L(f)^2}{H^{2d_2/(d-2)}}$$

for each sufficiently large H. However, $P_1(e^{2\pi i/3})P_1(e^{-2\pi i/3})$ is a nonzero integer due to the fact that $e^{2\pi i/3}$, $e^{-2\pi i/3}$ are quadratic conjugate algebraic integers. Selecting H so large that $2L(f)^2 < H^{2d_2/(d-2)}$ we conclude that there is a rational integer greater than 0 and smaller than 1, which is absurd. □

Now, we will express the moduli of two smallest roots of the polynomial P described in Lemma 3 in terms the resultant of P and its reciprocal P^*, and show that this resultant, as a polynomial in H, has degree at least 2.

Lemma 4. *For any monic polynomial $P \in \mathbb{Z}[x]$ of degree d satisfying $P(0) \neq 0$ and $P(\pm 1) \neq 0$ the resultant* $\mathrm{Res}(P, P^*)$ *of P and its reciprocal polynomial $P^*(x) = x^d P(1/x)$ is divisible by $P(1)P(-1)$.*

In particular, the resultant $\mathrm{Res}(P, P^*)$ *of any polynomial P defined in Lemma 3 and its reciprocal polynomial P^* is divisible by $(3H - f(1))(H - f(-1))$ if $H \in \mathbb{N} \setminus \{f(-1)\}$. Furthermore, the roots $\alpha_{d-1,H}$ and $\alpha_{d,H}$ of this P (as they are defined in Lemma 3) satisfy*

$$||\alpha_{d-1,H}| - 1| = ||\alpha_{d,H}| - 1| \sim \frac{\sqrt{|\mathrm{Res}(P, P^*)|}}{2\sqrt{3}H^d} \quad \text{as } H \to \infty. \tag{16}$$

Proof. If $P(x) = \prod_{i=1}^{d}(x - \beta_i)$ and $b = P(0)$ then

$$\begin{aligned}|\mathrm{Res}(P, P^*)| &= |b|^d \prod_{k,l=1}^{d} |\beta_k - \beta_l^{-1}| = \prod_{k,l=1}^{d} |\beta_k\beta_l - 1| \\ &= \prod_{k=1}^{d} |\beta_k^2 - 1| \prod_{1\le k<l\le d} |\beta_k\beta_l - 1|^2 = |P(1)P(-1)| \prod_{1\le k<l\le d} |\beta_k\beta_l - 1|^2.\end{aligned}$$

Since the product $\prod_{1\le k<l\le d}(\beta_k\beta_l - 1)$ is a symmetric function in $\beta_1, \dots, \beta_d$, it is a rational integer, which implies that $P(1)P(-1)$ divides $\mathrm{Res}(P, P^*)$.

The second claim for P defined in (11) follows by $P(1) = f(1) - 3H$ and $P(-1) = f(-1) - H$. Note that $f(1) \neq 3H$, since $f(x) = x g_{d-1}(x)$ and so, by (9), we deduce that

$$f(1) = g_{d-1}(1) = 3(g_{d-2}(1) - g_{d-2}(0)) + 1,$$

which implies that $f(1)$ is not divisible by 3 for each $d \geq 2$.

Finally, to prove (16) for P defined in Lemma 3 we first observe that

$$\begin{aligned}|\mathrm{Res}(P, P^*)| &= H^d \prod_{k,l=1}^{d} |\alpha_{k,H} - \alpha_{l,H}^{-1}| = H^d \prod_{k,l=1}^{d} |\alpha_{k,H} - \overline{\alpha_{l,H}}^{-1}| = \prod_{k,l=1}^{d} |\alpha_{k,H}\overline{\alpha_{l,H}} - 1| \\ &= \prod_{k=1}^{d} ||\alpha_{k,H}|^2 - 1| \prod_{k\neq l} |\alpha_{k,H}\overline{\alpha_{l,H}} - 1| = ||\alpha_{d-1,H}|^2 - 1|^2 \prod_{k=1}^{d-2} ||\alpha_{k,H}|^2 - 1| \prod_{1\le k<l\le d} |\alpha_{k,H}\overline{\alpha_{l,H}} - 1|^2.\end{aligned}$$

Hence,

$$||\alpha_{d-1,H}|^2 - 1| = \frac{\sqrt{|\mathrm{Res}(P, P^*)|}}{\prod_{k=1}^{d-2}(|\alpha_{k,H}|^2 - 1)^{1/2} \prod_{1\le k<l\le d} |\alpha_{k,H}\overline{\alpha_{l,H}} - 1|}. \tag{17}$$

By (12), we have

$$\prod_{k=1}^{d-2}(|\alpha_{k,H}|^2 - 1)^{1/2} \sim H \quad \text{as } H \to \infty. \tag{18}$$

Similarly, by (12), $|\alpha_{k,H}\overline{\alpha_{l,H}} - 1| \sim H^{2/(d-2)}$ as $H \to \infty$ when $l \le d-2$. Likewise, by (12) and (13), $|\alpha_{k,H}\overline{\alpha_{l,H}} - 1| \sim H^{1/(d-2)}$ as $H \to \infty$ when $k \le d-2$ and $l \in \{d-1, d\}$. It is also clear that

$$|\alpha_{d-1,H}\overline{\alpha_{d,H}} - 1| = |\alpha_{d-1,H}^2 - 1| \sim \sqrt{3}$$

as $H \to \infty$ by (13). Therefore, in view of

$$\binom{d-2}{2}\frac{2}{d-2} + \frac{2(d-2)}{d-2} = d-1$$

we obtain

$$\prod_{1 \le k < l \le d} |\alpha_{k,H}\overline{\alpha_{l,H}} - 1| \sim H^{d-1}\sqrt{3} \quad \text{as } H \to \infty. \tag{19}$$

On substituting (18) and (19) into (17) we obtain

$$||\alpha_{d-1,H}|^2 - 1| \sim \frac{\sqrt{|\mathrm{Res}(P, P^*)|}}{\sqrt{3}H^d} \quad \text{as } H \to \infty.$$

This yields (16), since $|\alpha_{d-1,H}| + 1 \sim 2$ as $H \to \infty$ by (13). □

3. Proof of Theorem 1

Let P be the polynomial $xg_{d-1}(x) - H(x^2 + x + 1)$ which is defined in the beginning of Section 2. By (9), the polynomial $f(x) = xg_{d-1}(x)$ modulo $x^2 + x + 1$ is x for each $d \ge 3$, so it is not divisible by $x^2 + x + 1$. Hence, P is a polynomial of the form as considered in Lemma 3. Thus, by Lemmas 2 and 3, we see that for H large enough $P \in \mathbb{Z}[x]$ is a monic irreducible polynomial satisfying

$$\mathrm{symsep}(P) = |\beta_{d-1,H}\beta_{d,H} - 1| = ||\beta_{d-1,H}|^2 - 1| \sim 2||\beta_{d-1,H}| - 1| \sim H^{1-d}$$

as $H \to \infty$. This proves (6). In particular, by Lemmas 2 and 3, all the roots of P lie outside the unit circle for each sufficiently large H, and hence $M(P) = H(P) = H$.

Next, by (10) and (16), we obtain $|\mathrm{Res}(P, P^*)| \sim 3H^2$ as $H \to \infty$. On the other hand, by Lemma 4, for any positive integer $H \ne f(-1)$ the resultant $\mathrm{Res}(P, P^*)$ is divisible by $(3H - f(1))(H - f(-1))$. Note that $\mathrm{Res}(P, P^*)$ is a polynomial in H with integer coefficients, since it can be written as a polynomial of the Sylvester matrix. This clearly forces

$$\mathrm{Res}(P, P^*) = \theta_d(3H - f(1))(H - f(-1)),$$

where $\theta_d \in \{-1, 1\}$ for each $d \ge 3$, which proves (7). In particular, a simple calculation shows that $\theta_2 = -1$, since the resultant of the polynomials

$$x^3 + (1-H)x^2 + (2-H)x - H \quad \text{and} \quad -Hx^3 + (2-H)x^2 + (1-H)x + 1$$

equals $-3H^2 - 2H + 8$, and similar calculations imply $\theta_3 = 1$.

Finally, since

$$\prod_{1 \le k < l \le d} |\beta_{k,H}\beta_{l,H} - 1|^2 = \frac{|\mathrm{Res}(P, P^*)|}{|P(1)P(-1)|}$$

(which was already proved in Lemma 4), (7) implies (8).

4. Some examples

By (10), the roots $\beta_{d-1,H}$ and $\beta_{d,H}$ of P are outside the unit circle. In fact, two smallest roots of P can also be inside the unit circle and close to the unit circle. For example, for $d=3$ take $f(x)=x^3+x^2+bx$. (Here, $b=2$ corresponds to the case considered in Lemma 2.) Then, the resultant of the polynomial $P(x)=x^3+(1-H)x^2+(b-H)x-H$ and its reciprocal P^* equals

$$-3(b-1)^2H^2-2(b-1)^3H+b^4-3b^2+2b.$$

Selecting $b=0$ we find that $\operatorname{Res}(P,P^*)=-3H^2+2H$ and $P(H)=-H<0$. So, the largest root of P, $\alpha_{1,H}$, is greater than H, and hence the two smallest roots $\alpha_{2,H}$, $\alpha_{3,H}$ that are complex conjugate by (13) and satisfy (16) must be inside the unit circle. Therefore, by Lemma 4,

$$1-|\alpha_{2,H}|=1-|\alpha_{3,H}|\sim\frac{1}{2H^2}\quad\text{as } H\to\infty.$$

In particular, as the reciprocal polynomial P^* has exactly two roots outside the unit circle, this shows that the results estimating how close the roots of an integer polynomial can be to the unit circle, e.g., [Dimitrov and Habegger 2019, Lemma 4.3] and [Dubickas 1997, Theorem 2], cannot be improved by much. For example, the upper bound $4d\log(2dM(P))$ on the quantity $\sum_j \log^+(1/||\alpha_j|-1|)$, where the sum taken is over the roots of a degree-d polynomial $P\in\mathbb{Z}[x]$ with $|\alpha_j|\neq 1$, (as obtained in [Dimitrov and Habegger 2019, Lemma 4.3]) cannot be made smaller than $(2d-2)\log M(P)+\log 4$ by (6).

For $d=4$ let us consider $f(x)=x^4+2x^3+2x^2+bx$. (Again, $b=2$ corresponds to the case considered in Lemma 2.) The resultant of the polynomial $P(x)=x^4+2x^3+(2-H)x^2+(b-H)x-H$ and its reciprocal P^* is equal to

$$3(b-1)^4H^2+2(b^5-8b^4+22b^3-28b^2+17b-4)H-b^6+15b^4-40b^3+45b^2-24b+5.$$

Selecting $b=0$ we find that $\operatorname{Res}(P,P^*)=3H^2-8H+5$. This time, one can verify that two smallest roots of $P(x)=x^4+2x^2+(2-H)x^2-Hx-H$ are outside the unit circle and we have

$$|\alpha_{3,H}|-1=|\alpha_{4,H}|-1\sim\frac{1}{2H^2}$$

as $H\to\infty$ by (16).

Finally, consider the polynomial $P(x)=x^3-Hx^2+2x-H$ (which is of a different type, since only the coefficients for x^2 and the constant term are "large"). Due to $P(H-1/H)=-1/H^3<0$ and $P(H)=H>0$, there is a root $\alpha_{1,H}$ of P in the interval $(H-1/H,H)$, so $\alpha_{1,H}\sim H$ as $H\to\infty$. Therefore,

$$H-\alpha_{1,H}=\frac{2\alpha_{1,H}-H}{\alpha_{1,H}^2}\sim\frac{1}{H}\quad\text{as } H\to\infty.$$

Two other roots are complex conjugate numbers $\alpha_{2,H}$ and $\alpha_{3,H}$, which tend to i and $-i$, respectively, as $H\to\infty$. From

$$|\alpha_{2,H}|^2-1=|\alpha_{3,H}|^2-1=\alpha_{2,H}\alpha_{3,H}-1=\frac{H-\alpha_{1,H}}{\alpha_{1,H}}\sim\frac{1}{H\alpha_{1,H}}\sim\frac{1}{H^2}$$

as $H \to \infty$ we obtain

$$|\alpha_{2,H}| - 1 = |\alpha_{3,H}| - 1 \sim \frac{1}{2H^2} \quad \text{as } H \to \infty.$$

So, although the polynomial $x^3 - Hx^2 + 2x - H$ is different from that considered in Lemma 2 (i.e., $xg_2(x) - H(x^2 + x + 1) = x^3 + (1 - H)x^2 + (2 - H)x - H$), for its roots (10) holds as well. (Its irreducibility over $\mathbb{Q}$ for each sufficiently large positive integer H can be shown by the same argument as that in Lemma 3.)

Acknowledgement

This research was funded by the European Social Fund according to the activity "Improvement of researchers' qualification by implementing world-class R&D projects" of Measure No. 09.3.3-LMT-K-712-01-0037.

References

[Bugeaud and Dujella 2011] Y. Bugeaud and A. Dujella, "Root separation for irreducible integer polynomials", *Bull. Lond. Math. Soc.* **43**:6 (2011), 1239–1244. MR Zbl

[Bugeaud and Dujella 2014] Y. Bugeaud and A. Dujella, "Root separation for reducible integer polynomials", *Acta Arith.* **162**:4 (2014), 393–403. MR Zbl

[Bugeaud and Mignotte 2004] Y. Bugeaud and M. Mignotte, "On the distance between roots of integer polynomials", *Proc. Edinb. Math. Soc.* (2) **47**:3 (2004), 553–556. MR Zbl

[Bugeaud and Mignotte 2010] Y. Bugeaud and M. Mignotte, "Polynomial root separation", *Int. J. Number Theory* **6**:3 (2010), 587–602. MR Zbl

[Bugeaud et al. 2017] Y. Bugeaud, A. Dujella, T. Pejković, and B. Salvy, "Absolute real root separation", *Amer. Math. Monthly* **124**:10 (2017), 930–936. MR Zbl

[Dimitrov and Habegger 2019] V. Dimitrov and P. Habegger, "Galois orbits of torsion points near atoral sets", preprint, 2019. arXiv

[Dubickas 1997] A. Dubickas, "Algebraic conjugates outside the unit circle", pp. 11–21 in *New trends in probability and statistics* (Palanga, 1996), vol. 4, edited by A. Laurinčikas et al., VSP, Utrecht, 1997. MR Zbl

[Dubickas 2013] A. Dubickas, "Polynomial root separation in terms of the Remak height", *Turkish J. Math.* **37**:5 (2013), 747–761. MR Zbl

[Dujella and Pejković 2011] A. Dujella and T. Pejković, "Root separation for reducible monic quartics", *Rend. Semin. Mat. Univ. Padova* **126** (2011), 63–72. MR Zbl

[Evertse 2004] J.-H. Evertse, "Distances between the conjugates of an algebraic number", *Publ. Math. Debrecen* **65**:3-4 (2004), 323–340. MR Zbl

[Feldman 1981] N. I. Feldman, Приближения алгебраических чисел, Moskov. Gos. Univ., Moscow, 1981. MR Zbl

[Herman et al. 2018] A. Herman, H. Hong, and E. Tsigaridas, "Improving root separation bounds", *J. Symbolic Comput.* **84** (2018), 25–56. MR Zbl

[Mahler 1964] K. Mahler, "An inequality for the discriminant of a polynomial", *Michigan Math. J.* **11** (1964), 257–262. MR Zbl

[Schönhage 2006] A. Schönhage, "Polynomial root separation examples", *J. Symbolic Comput.* **41**:10 (2006), 1080–1090. MR Zbl

[Uray 2019] M. J. Uray, "On the expansivity gap of integer polynomials", preprint, 2019. arXiv

[Waldschmidt 2000] M. Waldschmidt, *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables*, Grundlehren der Mathematischen Wissenschaften **326**, Springer, 2000. MR Zbl

Received 7 Oct 2019. Revised 13 Jan 2020.

ARTŪRAS DUBICKAS:
arturas.dubickas@mif.vu.lt
Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Vilnius, Lithuania

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2020 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Moscow Journal of Combinatorics and Number Theory

vol. 9 no. 4 2020

In memoriam
N. I. Feldman

Naum Ilyitch Feldman 351
NIKOLAY MOSHCHEVITIN

Effective simultaneous rational approximation to pairs of real quadratic numbers 353
YANN BUGEAUD

Algebraic integers close to the unit circle 361
ARTŪRAS DUBICKAS

On transcendental entire functions with infinitely many derivatives taking integer values at several points 371
MICHEL WALDSCHMIDT

Can polylogarithms at algebraic points be linearly independent? 389
SINNOU DAVID, NORIKO HIRATA-KOHNO and MAKOTO KAWASHIMA

The irrationality measure of π is at most $7.103205334137\ldots$ 407
DORON ZEILBERGER and WADIM ZUDILIN

Approximating π by numbers in the field $\mathbb{Q}(\sqrt{3})$ 421
MIKHAIL YU. LUCHIN and VLADISLAV KH. SALIKHOV

On approximations of solutions of the equation $P(z, \ln z) = 0$ by algebraic numbers 435
ALEXANDER GALOCHKIN and ANASTASIA GODUNOVA

Two integral transformations related to $\zeta(2)$ 441
RAFFAELE MARCOVECCHIO