DISCRIMINANT AND ROOT SEPARATION OF INTEGRAL POLYNOMIALS

FRIEDRICH GÖTZE AND DMITRY ZAPOROZHETS

Abstract. Consider a random polynomial

$$G_Q(x) = \xi_{Q,n}x^n + \xi_{Q,n-1}x^{n-1} + \cdots + \xi_{Q,0}$$

with independent coefficients uniformly distributed on $2Q + 1$ integer points \{-Q, \ldots, Q\}. Denote by $D(G_Q)$ the discriminant of $G_Q$. We show that there exists a constant $C_n$, depending on $n$ only such that for all $Q \geq 2$ the distribution of $D(G_Q)$ can be approximated as follows

$$\sup_{-\infty \leq a \leq b \leq \infty} \left| \mathbb{P} \left( a \leq \frac{D(G_Q)}{Q^{2n-2}} \leq b \right) - \int_a^b \varphi_n(x) \, dx \right| \leq C_n \log Q,$$

where $\varphi_n$ denotes the distribution function of the discriminant of a random polynomial of degree $n$ with independent coefficients which are uniformly distributed on \{-1,1\}.

Let $\Delta(G_Q)$ denote the minimal distance between the complex roots of $G_Q$. As an application we show that for any $\varepsilon > 0$ there exists a constant $\delta_n > 0$ such that $\Delta(G_Q)$ is stochastically bounded from below/above for all sufficiently large $Q$ in the following sense

$$\mathbb{P} \left( \delta_n < \Delta(G_Q) < \frac{1}{\delta_n} \right) > 1 - \varepsilon.$$

1. Introduction

Let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x - \alpha_1) \cdots (x - \alpha_n)$$

be a polynomial of degree $n$ with real or complex coefficients.

In this note we consider different asymptotic estimates when the degree $n$ is arbitrary but fixed. Thus for non-negative functions $f, g$ we write $f \ll g$ if there exists a non-negative constant $C_n$ (depending on $n$ only) such that $f \leq C_n g$. We also write $f \asymp g$ if $f \ll g$ and $f \gg g$.

Denote by

$$\Delta(p) = \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|$$

the shortest distance between any two zeros of $p$.

In his seminal paper Mahler proved that

$$\Delta(p) \geq \sqrt{3} n^{-1/2} \left( |a_n| + \cdots + |a_0| \right)^{1/2},$$

1. Introduction

Let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x - \alpha_1) \cdots (x - \alpha_n)$$

be a polynomial of degree $n$ with real or complex coefficients.

In this note we consider different asymptotic estimates when the degree $n$ is arbitrary but fixed. Thus for non-negative functions $f, g$ we write $f \ll g$ if there exists a non-negative constant $C_n$ (depending on $n$ only) such that $f \leq C_n g$. We also write $f \asymp g$ if $f \ll g$ and $f \gg g$.

Denote by

$$\Delta(p) = \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|$$

the shortest distance between any two zeros of $p$.

In his seminal paper Mahler proved that

$$\Delta(p) \geq \sqrt{3} n^{-1/2} \left( |a_n| + \cdots + |a_0| \right)^{1/2},$$

where $\varphi_n$ denotes the distribution function of the discriminant of a random polynomial of degree $n$ with independent coefficients which are uniformly distributed on \{-1,1\}.

Let $\Delta(G_Q)$ denote the minimal distance between the complex roots of $G_Q$. As an application we show that for any $\varepsilon > 0$ there exists a constant $\delta_n > 0$ such that $\Delta(G_Q)$ is stochastically bounded from below/above for all sufficiently large $Q$ in the following sense

$$\mathbb{P} \left( \delta_n < \Delta(G_Q) < \frac{1}{\delta_n} \right) > 1 - \varepsilon.$$

1. Introduction

Let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x - \alpha_1) \cdots (x - \alpha_n)$$

be a polynomial of degree $n$ with real or complex coefficients.

In this note we consider different asymptotic estimates when the degree $n$ is arbitrary but fixed. Thus for non-negative functions $f, g$ we write $f \ll g$ if there exists a non-negative constant $C_n$ (depending on $n$ only) such that $f \leq C_n g$. We also write $f \asymp g$ if $f \ll g$ and $f \gg g$.

Denote by

$$\Delta(p) = \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|$$

the shortest distance between any two zeros of $p$.

In his seminal paper Mahler proved that

$$\Delta(p) \geq \sqrt{3} n^{-1/2} \left( |a_n| + \cdots + |a_0| \right)^{1/2},$$

where $\varphi_n$ denotes the distribution function of the discriminant of a random polynomial of degree $n$ with independent coefficients which are uniformly distributed on \{-1,1\}.

Let $\Delta(G_Q)$ denote the minimal distance between the complex roots of $G_Q$. As an application we show that for any $\varepsilon > 0$ there exists a constant $\delta_n > 0$ such that $\Delta(G_Q)$ is stochastically bounded from below/above for all sufficiently large $Q$ in the following sense

$$\mathbb{P} \left( \delta_n < \Delta(G_Q) < \frac{1}{\delta_n} \right) > 1 - \varepsilon.$$
where
\begin{equation}
D(p) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (a_i - a_j)^2
\end{equation}
denotes the discriminant of \( p(x) \). Alternatively, \( D(p) \) is given by the \((2n-1)\)-dimensional determinant
\begin{equation}
D(p) = (-1)^{n(n-1)/2} \begin{vmatrix}
1 & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & \ldots \\
0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & \ldots \\
0 & \ldots & 0 & a_n & \ldots & a_1 & a_0 \\
0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
n & (n-1)a_{n-1} & (n-2)a_{n-2} & \ldots & 0 & 0 & \ldots \\
0 & \ldots & \ldots & 0 & na_n & \ldots & a_1
\end{vmatrix}
\end{equation}

Define the height of the polynomial by \( H(p) = \max_{0 \leq i \leq n} |a_i| \). It follows immediately from (3) that
\begin{equation}
|D(p)| \ll H(p)^{2n-2}.
\end{equation}

From now on we will always assume that the polynomial \( p \) is integral (that is has integer coefficients). Since the condition \( D(p) \neq 0 \) implies \( |D(p)| \geq 1 \) Mahler noted that (1) implies
\begin{equation}
\Delta(p) \gg H(p)^{-n+1},
\end{equation}
provided that \( p \) doesn’t have multiple zeros. The estimate (5) seems to be the best available lower bound up to now. However, for \( n \geq 3 \) it is still not known how far it differs from the optimal lower bound. Denote by \( \kappa_n \) the infimum of \( \kappa \) such that
\[ \Delta(p) > H(p)^{-\kappa} \]
holds for all integral polynomials of degree \( n \) without multiple zeros and large enough height \( H(p) \). It is easy to see that (5) is equivalent to \( \kappa_n \leq n - 1 \). Also it is a simple exercise to show that \( \kappa_2 = 1 \) (see, e.g., [3]). Evertse [4] showed that \( \kappa_3 = 2 \).

For \( n \geq 4 \) only estimates are known. At first, Mignotte [11] proved that \( \kappa_n \geq n/4 \) for \( n \geq 2 \). Recently Bugeaud and Mignotte [1, 2] have shown that \( \kappa_n \geq n/2 \) for even \( n \geq 4 \) and \( \kappa_n \geq (n + 2)/4 \) for odd \( n \geq 5 \). Shortly after that Beresnivich, Bernik, and Götze [1], using completely different approach, improved their result in the case of odd \( n \): they obtained (as a corollary of more general counting result) that \( \kappa_n \geq (n + 1)/3 \) for \( n \geq 2 \).

Formulated in other terms the above results give answers to the question "How close to each other can two conjugate algebraic numbers of degree \( n \) be?" Recall that two complex algebraic numbers called conjugate (over \( \mathbb{Q} \)) if they are roots of the same irreducible integral polynomial (over \( \mathbb{Q} \)). Roughly speaking, if we consider a polynomial \( p^* \) which minimizes \( \Delta(p) \) among all integral polynomials of degree \( n \) having the same height and without multiple zeros, then \( \Delta(p^*) \) satisfies the following lower/upper bounds with respect to \( H(p^*) \):
\[ H(p^*)^{-c_1n} \ll \Delta(p^*) \ll H(p^*)^{-c_2n}, \]
for some absolute constants \( 0 < c_2 \leq c_1 \). In this note, instead of considering the extreme polynomial \( p^* \), we consider the behaviour of \( \Delta(p) \) for a typical integral
polynomial $p$. We prove that for "most" integral polynomials (see Section 2 for a more precise formulation) we have

$$\Delta(p) \asymp 1.$$  

We also show that the same estimate holds for "most" irreducible integral polynomials (over $\mathbb{Q}$).

A related interesting problem is to study the distribution of discriminants of integral polynomials. To deal with it is convenient (albeit not necessary) to use probabilistic terminology. Consider some $Q \in \mathbb{N}$ and consider the class of all integral polynomials $p$ with $\deg(p) \leq n$ and $H(p) \leq Q$. The cardinality of this class is $(2Q + 1)^{n+1}$. Consider the uniform probability measure on this class so that the probability of each polynomial is given by $(2Q + 1)^{-n-1}$. In this sense, we may consider random polynomials

$$G_Q(x) = \xi_{Q,n}x^n + \xi_{Q,n-1}x^{n-1} + \cdots + \xi_{Q,0}$$

with independent coefficients which are uniformly distributed on $2Q + 1$ integer points $\{-Q, \ldots, Q\}$. We are interested in the asymptotic behavior of $D(G_Q)$ when $n$ is fixed and $Q \to \infty$.

Bernik, Götze and Kukso [3] showed that for $\nu \in [0, \frac{1}{2}]$

$$\mathbb{P}(\|D(G_Q)\| < Q^{2n-2-2\nu}) \gg Q^{-2\nu}.$$  

Note that the case $\nu = 0$ is consistent with (4). It has been conjectured in [3] that this estimate is optimal up to a constant:

$$(6) \quad \mathbb{P}(\|D(G_Q)\| < Q^{2n-2-2\nu}) \asymp Q^{-2\nu}.$$  

The conjecture turned out to be true for $n = 2$: Götze, Kaliada, and Korolev [8] showed that for $n = 2$ and $\nu \in (0, \frac{3}{4})$ it holds

$$\mathbb{P}(\|D(G_Q)\| < Q^{2-2\nu}) = 2(\log 2 + 1)Q^{-2\nu} \left(1 + O(Q^{-\nu} \log Q + Q^{2\nu-3/2} \log^{3/2} Q)\right).$$

However, for $n = 3$ and $\nu \in [0, \frac{3}{5})$ Kaliada, Götze, and Kukso [9] obtained the following asymptotic relation:

$$(7) \quad \mathbb{P}(\|D(G_Q)\| < Q^{4-2\nu}) = \kappa Q^{-5\nu/3} \left(1 + O(Q^{-\nu/3} \log Q + Q^{5\nu/3-1})\right),$$

where the absolute constant $\kappa$ had been explicitly determined.

In this note we prove a limit theorem for $D(G_Q)$. As a corollary, we obtain that "with high probability" (see Section 2 for details) the following asymptotic equivalence holds:

$$|D(P_Q)| \asymp Q^{2n-2}.$$  

The same estimate holds "with high probability" for irreducible polynomials.

For more comprehensive survey of the subject and a list of references, see [2].

2. Main results

Let $\xi_0, \xi_1, \ldots, \xi_n$ be independent random variables uniformly distributed on $[-1, 1]$. Consider the random polynomial

$$G(x) = \xi_n x^n + \xi_{n-1} x^{n-1} + \cdots + \xi_1 x + \xi_0$$

and denote by $\varphi$ the distribution function of $D(G)$. It is easy to see that $\varphi$ has compact support and $\sup_{x \in \mathbb{R}} \varphi(x) < \infty$. 

Theorem 2.1. Using the above notations we have

\[
\sup_{-\infty \leq a \leq b \leq \infty} \left| \mathbb{P} \left( a \leq \frac{D(G_Q)}{Q^{2n-2}} \leq b \right) - \int_a^b \varphi(x) \, dx \right| \ll \frac{1}{\log Q}.
\]

How far is this estimate from being optimal? Relation (7) shows that for \( n = 3 \) the estimate \( \log^{-1} Q \) cannot be replaced by \( Q^{-\varepsilon} \) for any \( \varepsilon > 0 \). Otherwise it would imply that \( \nu \leq \varepsilon/2 \).

The proof of Theorem 2.1 will be given in Section 2.1. Now let us derive some corollaries.

Relation (6) means that \( |D(G_Q)| \ll Q^{2n-2} \) holds a.s. It follows from Theorem 2.1 that with high probability the lower estimate holds as well.

Corollary 2.2. For any \( \varepsilon > 0 \) there exists \( \delta > 0 \) (depending on \( n \) only) such that for all sufficiently large \( Q \)

\[
P\left( |D(G_Q)| > \delta Q^{2n-2} \right) > 1 - \varepsilon.
\]

Proof. Since \( \sup_{x \in \mathbb{R}} \varphi(x) < \infty \), it follows from (5) that

\[
P\left( |D(G_Q)| < \delta Q^{2n-2} \right) \ll \delta + \frac{1}{\log Q},
\]

which completes the proof.

As another corollary we obtain an estimate for \( \Delta(G_Q) \).

Corollary 2.3. For any \( \varepsilon > 0 \) there exists \( \delta > 0 \) (depending on \( n \) only) such that for all sufficiently large \( Q \)

\[
P(\delta < \Delta(G_Q) < \delta^{-1}) > 1 - \varepsilon.
\]

Proof. For large enough \( Q \) we have

\[
P\left( |\xi_{Q,n}| > \frac{\varepsilon}{2} Q \right) > 1 - \varepsilon.
\]

Therefore it follows from (2) and (4) that with probability at least \( 1 - \varepsilon \)

\[
\Delta(G_Q) \leq \left( \frac{2}{\varepsilon} \right)^{2/n},
\]

which implies the upper estimate. The lower bound immediately follows from (9) and (1).

Remark on irreducibility. In order to consider \( \Delta(G_Q) \) as distance between the closest conjugate algebraic numbers of \( G_Q \) we have to restrict ourselves to irreducible polynomials only. In other words the distribution of the random polynomial \( G_Q \) has to be conditioned on \( G_Q \) being irreducible. It turns out that the relations (9) and (10) with conditional versions of the left-hand sides still hold. This fact easily follows from the estimate

\[
P(G_Q \text{ is irreducible}) \asymp 1,
\]

which was obtained by Dubickas [6].
3. Proof of Theorem 2.1

For \( k \in \mathbb{N} \) the moments of \( \xi_i \) and \( \xi_{i,Q} \) are given by

\[
\mathbb{E} \xi_i^{2k} = \frac{1}{2k + 1}, \quad \mathbb{E} \xi_{i,Q}^{2k} = \frac{2}{2Q + 1} \sum_{j=1}^{Q} j^{2k}.
\]

Since

\[
\frac{Q^{2k+1}}{2k+1} = \int_0^Q t^{2k} dt \leq \sum_{j=1}^{Q} j^{2k} \leq \int_0^Q (t+1)^{2k} dt \leq \frac{(Q+1)^{2k+1}}{2k+1},
\]

we get

\[
\frac{2}{2Q+1} \sum_{j=1}^{Q} j^{2k} - \frac{Q^{2k}}{2k+1} \leq \frac{2}{2Q+1} \sum_{j=1}^{Q} j^{2k} - \frac{2Q+1}{2} \frac{Q^{2k}}{2k+1}
\]

\[
\leq \frac{2}{2Q+1} \sum_{j=1}^{Q} j^{2k} - \frac{Q^{2k+1}}{2k+1} + \frac{Q^{2k}}{2Q+1} \leq \frac{2}{2Q+1} \frac{(Q+1)^{2k+1} - Q^{2k+1}}{2k+1} + \frac{Q^{2k}}{2Q+1} \leq 2^{2k} Q^{2k-1},
\]

which implies

\[
\left| \mathbb{E} \left( \frac{\xi_{i,Q}^{2k}}{Q} \right) - \mathbb{E} \xi_{i}^{2k} \right| \leq \frac{Q^{2k}}{Q}.
\]

It follows from (12) that for all \( k \in \mathbb{N} \)

\[
\left| \mathbb{E} D^k \left( \frac{G_{Q}}{Q} \right) - \mathbb{E} D^k(G) \right| \leq n^{2k} \sum_{k_0, \ldots, k_n} \prod_{i=0}^{n} \mathbb{E} \left( \frac{\xi_{i,Q}^{2k_i}}{Q} \right) - \prod_{i=0}^{n} \mathbb{E} \xi_{i}^{2k_i},
\]

where the summation is taken over at most \((2n-1)!)^k\) summands such that \( k_0 + \cdots + k_n = kn - 1\). Let us show that

\[
\prod_{i=0}^{n} \mathbb{E} \left( \frac{\xi_{i,Q}^{2k_i}}{Q} \right) - \prod_{i=0}^{n} \mathbb{E} \xi_{i}^{2k_i} \leq \frac{Q^{2k_0 + \cdots + 2k_n}}{Q}.
\]

We proceed by induction on \( n \). The case \( n = 0 \) follows from (12). It holds

\[
\prod_{i=0}^{n} \mathbb{E} \left( \frac{\xi_{i,Q}^{2k_i}}{Q} \right) - \prod_{i=0}^{n} \mathbb{E} \xi_{i}^{2k_i} \leq \left| \prod_{i=0}^{n-1} \mathbb{E} \left( \frac{\xi_{i,Q}^{2k_i}}{Q} \right) - \prod_{i=0}^{n-1} \mathbb{E} \xi_{i}^{2k_i} \right| \mathbb{E} \left( \frac{\xi_{n,Q}^{2k_n}}{Q} \right)^{2k_n} + \prod_{i=0}^{n-1} \mathbb{E} \xi_{i}^{2k_i} \left| \mathbb{E} \left( \frac{\xi_{n,Q}^{2k_n}}{Q} \right)^{2k_n} - \mathbb{E} \xi_{s_0}^{2k_0} \right|.
\]

Applying the induction assumption and (12), we obtain (13).

Thus, using (12), (13), and the relation \( k_0 + \cdots + k_n = kn - 1\) we get

\[
\left| \mathbb{E} D^k \left( \frac{G_{Q}}{Q} \right) - \mathbb{E} D^k(G) \right| \leq \frac{Q^{k}}{Q},
\]
where $\gamma$ depends on $n$ only.

Since $D(G)$ and $D(G_Q/Q)$ are bounded random variables, their characteristic functions

$$f(t) = \mathbb{E} e^{iD(G)}, \quad f_Q(t) = \mathbb{E} e^{iD(G_Q/Q)}$$

are entire functions. Therefore (14) implies that for all real $t$

$$|f_Q(t) - f(t)| = \left| \sum_{k=1}^{\infty} \frac{i^k}{k!} \mathbb{E} D_k(G_Q/Q) - \mathbb{E} D_k(G) \right| \leq \frac{1}{Q} \sum_{k=1}^{\infty} \frac{(\gamma|t|)^k}{k!} \leq \frac{\gamma|t| e^{\gamma|t|}}{Q}.$$

Now we are ready to estimate the uniform distance between the distributions of $D(G)$ and $D(G_Q/Q)$ using the closeness of $f(t)$ and $f_Q(t)$. Let $F$ and $F_Q$ be distribution functions of $D(G)$ and $D(G_Q/Q)$. By Esseen’s inequality, we get for any $T > 0$

$$\sup_x |F_Q(x) - F(x)| \leq \frac{2}{\pi} \int_{-T}^{T} \left| \frac{f_Q(t) - f(t)}{t} \right| dt + \frac{24}{\pi} \sup_{x \in \mathbb{R}} \varphi(x).$$

Applying (15), we obtain that there exists a constant $C$ depending on $n$ only such that for any $T > 0$

$$\sup_{-\infty \leq a \leq b \leq \infty} \left| \mathbb{P}(a \leq D \left( \frac{G_Q}{Q} \right) \leq b) - \mathbb{P}(a \leq D(G) \leq b) \right| \leq C \left( \frac{Te^{\gamma T}}{Q} + \frac{1}{T} \right).$$

Taking $T = \log Q/2\gamma$ completes the proof.

**Acknowledgments.** We are grateful to Victor Beresnevich, Vasili Bernik, and Zakhar Kabluchko for useful discussions. We also would like to thank Andrei Zaitsev for some remarks on notations.

**References**

[1] V. Beresnevich, V. Bernik, and F. Götze. The distribution of close conjugate algebraic numbers. *Compos. Math.*, 146:1165–1179, 2010.

[2] V. Beresnevich, V. Bernik, F. Götze, and O. Kukso. Distribution of algebraic numbers and metric theory of diophantine approximation. In *Limit Theorems in Probability, Statistics and Number Theory*, pages 23–48. Springer, 2013.

[3] V. Bernik, F. Götze, and O. Kukso. Lower bounds for the number of integral polynomials with given order of discriminants. *Acta Arith.*, 133:375–390, 2008.

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

[5] Y. Bugeaud and M. Mignotte. Polynomial root separation. *Int. J. Number Theor.*, 6(03):587–602, 2010.

[6] A. Dubickas. Polynomials irreducible by eisenstein’s criterion. *Appl. Algebra Engin. Comm. Comput.*, 14(2):127–132, 2003.

[7] J.-H. Evertse. Distances between the conjugates of an algebraic number. *Publ. Math. Debrecen*, 65:323–340, 2004.

[8] F. Götze, D. Kaliada, and M. Korolev. On the number of integral quadratic polynomials with bounded heights and discriminants. *Preprint*, arXiv:1308.2091, 2013.
[9] D. Kaliada, F. Götze, and O. Kukso. The asymptotic number of integral cubic polynomials with bounded heights and discriminants. Preprint, arXiv:1307.3983, 2013.

[10] K. Mahler. An inequality for the discriminant of a polynomial. Mich. Math. J., 11(3):257–262, 1964.

[11] M. Mignotte. Some useful bounds. In Computer Algebra, pages 259–263. Springer, 1983.

FRIEDRICH GÖTZE, FACULTY OF MATHEMATICS, BIELEFELD UNIVERSITY, P. O. BOX 10 01 31, 33501 BIELEFELD, GERMANY
E-mail address: goetze@math.uni-bielefeld.de

DMITRY ZAPOROZHETS, ST. PETERSBURG DEPARTMENT OF STEKLOV INSTITUTE OF MATHEMATICS, FONTANKA 27, 191011 ST. PETERSBURG, RUSSIA
E-mail address: zap1979@gmail.com