Записки научных
семинаров ПОМИ
Том 441, 2015 г.

F. Götze, D. Zaporozhets

DISCRIMINANT AND ROOT SEPARATION OF INTEGRAL POLYNOMIALS

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 $\{-Q, \dots, Q\}$. 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 $Q \geqslant 2$ the distribution of $D(G_Q)$ can be approximated as follows

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

where φ_n denotes the probability density 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

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

§1. Introduction

Let

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

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 $f \ll g$

Key words and phrases: distribution of discriminants, integral polynomials, polynomial discriminant, polynomial root separation.

The work was done with the financial support of the Bielefeld University (Germany) in terms of project SFB 701. The second author is supported by the RFBR grant 13-01-00256 and by the program of RAS "Modern problems of theoretical mathematics".

if there exists a non-negative constant C_n (depending on n only) such that $f \leqslant C_n g$. We also write $f \asymp g$ if $f \ll g$ and $f \gg g$.

Denote by

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

the shortest distance between any two zeros of p.

In his seminal paper Mahler [12] proved that

$$\Delta(p) \geqslant \sqrt{3}\, n^{-(n+2)/2} \frac{|D(p)|^{1/2}}{(|a_n| + \cdots + |a_0|)^{n-1}}, \tag{1}$$

where

$$D(p) = a_n^{2n-2} \prod_{1\leqslant i<j\leqslant n} (\alpha_i - \alpha_j)^2 \tag{2}$$

denotes the discriminant of $p(x)$. Alternatively, $D(p)$ is given by the $(2n-1)$-dimensional determinant

$$D(p) = (-1)^{n(n-1)/2}$$
$$\times \begin{vmatrix} 1 & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{n-2} & a_{n-3} & \dots & a_1 & a_0 \\ n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & 0 & 0 & \dots & 0 & 0 \\ 0 & na_n & (n-1)a_{n-1} & \dots & a_1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & 2a_2 & a_1 \end{vmatrix}. \tag{3}$$

Define the height of the polynomial by $H(p) = \max_{0\leqslant i\leqslant n} |a_i|$. It follows immediately from (3) that

$$|D(p)| \ll H(p)^{2n-2}. \tag{4}$$

From now on we will always assume that the polynomial p is integral (that is, it has integer coefficients). Since the condition $D(p) \neq 0$ implies $|D(p)| \geqslant 1$ Mahler noted that (1) implies

$$\Delta(p) \gg H(p)^{-n+1}, \tag{5}$$

provided that p doesn't have multiple zeros. The estimate (5) seems to be the best available lower bound up to now. However, for $n \geqslant 3$ it is still not known how far it differs from the optimal lower bound. Denote by κ_n the infimum of κ 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 $\kappa_n \leqslant n-1$. Also it is a simple exercise to show that $\kappa_2 = 1$ (see, e.g., [8]). Evertse [9] showed that $\kappa_3 = 2$.

For $n \geqslant 4$ only estimates are known. At first, Mignotte [13] proved that $\kappa_n \geqslant n/4$ for $n \geqslant 2$. Later Bugeaud and Mignotte [7, 8] have shown that $\kappa_n \geqslant n/2$ for even $n \geqslant 4$ and $\kappa_n \geqslant (n+2)/4$ for odd $n \geqslant 5$. 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 $\kappa_n \geqslant (n+1)/3$ for $n \geqslant 2$. Recently Bugeaud and Dujella [6] achieved significant progress showing that $\kappa_n \geqslant (2n-1)/3$ for $n \geqslant 4$ (see also [5] for irreducible polynomials).

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 $H(p^*)$:

$$H(p^*)^{-c_1 n} \ll \Delta(p^*) \ll H(p^*)^{-c_2 n},$$

for some absolute constants $0 < c_2 \leqslant c_1$. 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 $\deg(p) \leqslant n$ and $H(p) \leqslant Q$. 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 $\{-Q,\dots,Q\}$. We are interested in the asymptotic behavior of $D(G_Q)$ when n is fixed and $Q\to\infty$.

Bernik, Götze and Kukso [4] showed that for $\nu\in[0,1/2]$

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

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

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

The conjecture turned out to be true for $n=2$: Götze, Kaliada, and Korolev [10] showed that for $n=2$ and $\nu\in(0,3/4)$ it holds

$$\begin{aligned}&\mathbf{P}(|D(G_Q)| < Q^{2-2\nu})\\&\qquad = 2(\log 2+1)Q^{-2\nu}\left(1+O(Q^{-\nu}\log Q + Q^{2\nu-3/2}\log^{3/2} Q)\right).\end{aligned}$$

However, for $n=3$ and $\nu\in[0,3/5)$ Kaliada, Götze, and Kukso [11] obtained the following asymptotic relation:

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

where the absolute constant κ had been explicitly determined.

Recently Beresnevich, Bernik, and Götze [2] extended the lower bound given by (7) to the full range of ν and to the arbitrary degrees n. They showed that for $0\leqslant\nu<n-1$ one has that

$$\mathbf{P}(|D(G_Q| < Q^{2n-2-2\nu}) \gg Q^{-n+3-(n+2)\nu/n}.$$

They also obtained a similar result for resultants.

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 [3].

§2. Main results

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

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

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

Theorem 2.1. *Using the above notations we have*

$$\sup_{-\infty\leqslant a\leqslant b\leqslant\infty} \left| \mathbf{P}\left(a \leqslant \frac{D(G_Q)}{Q^{2n-2}} \leqslant b\right) - \int\limits_a^b \varphi(x)\,dx \right| \ll \frac{1}{\log Q}. \tag{8}$$

How far is this estimate from being optimal? Relation (7) shows that for $n = 3$ the estimate $\log^{-1} Q$ can not be replaced by $Q^{-\varepsilon}$ for any $\varepsilon > 0$. Otherwise it would imply that (6) holds for $\nu \leqslant \varepsilon/2$.

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

Relation (4) 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*

$$\mathbf{P}(|D(G_Q)| > \delta Q^{2n-2}) > 1 - \varepsilon. \tag{9}$$

Proof. Since $\sup\limits_{x\in\mathbb{R}} \varphi(x) < \infty$, it follows from (8) that

$$\mathbf{P}(|D(G_Q)| < \delta Q^{2n-2}) \ll \delta + \frac{1}{\log Q},$$

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*

$$\mathbf{P}(\delta < \Delta(G_Q) < \delta^{-1}) > 1 - \varepsilon. \tag{10}$$

Proof. For large enough Q we have

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

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

$$\Delta(G_Q) \leqslant \left(\frac{2}{\varepsilon}\right)^{2/n},$$

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

$$\mathbf{P}(G_Q \text{is irreducible}) \asymp 1,$$

which was obtained by van der Waerden [14].

§3. Proof of Theorem 2.1

For $k \in \mathbb{N}$ the moments of ξ_i and $\xi_{i,Q}$ are given by

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

Since

$$\frac{Q^{2k+1}}{2k+1} = \int_0^Q t^{2k}\,dt \leqslant \sum_{j=1}^{Q} j^{2k} \leqslant \int_0^Q (t+1)^{2k}\,dt \leqslant \frac{(Q+1)^{2k+1}}{2k+1},$$

we get

$$\begin{aligned}
\left|\frac{2}{2Q+1}\sum_{j=1}^{Q} j^{2k} - \frac{Q^{2k}}{2k+1}\right| &= \frac{2}{2Q+1}\Big|\sum_{j=1}^{Q} j^{2k} - \frac{2Q+1}{2}\frac{Q^{2k}}{2k+1}\Big| \\
&\leqslant \frac{2}{2Q+1}\Big|\sum_{j=1}^{Q} j^{2k} - \frac{Q^{2k+1}}{2k+1}\Big| + \frac{Q^{2k}}{2Q+1} \\
&\leqslant \frac{2}{2Q+1}\cdot\frac{(Q+1)^{2k+1} - Q^{2k+1}}{2k+1} + \frac{Q^{2k}}{2Q+1} \leqslant 2^{2k}Q^{2k-1},
\end{aligned}$$

which implies

$$\left| \mathbf{E} \left(\frac{\xi_{i,Q}}{Q} \right)^{2k} - \mathbf{E}\xi^{2k} \right| \leqslant \frac{2^{2k}}{Q}. \tag{11}$$

It follows from (3) that for all $k \in \mathbb{N}$

$$\left| \mathbf{E}\, D^k \left(\frac{G_Q}{Q} \right) - \mathbf{E}\, D^k(G) \right| \leqslant n^{nk} \sum_{k_0,\dots,k_n} \left| \prod_{i=0}^{n} \mathbf{E} \left(\frac{\xi_{i,Q}}{Q} \right)^{2k_i} - \prod_{i=0}^{n} \mathbf{E}\, \xi_i^{2k_i} \right|, \tag{12}$$

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

$$\left| \prod_{i=0}^{n} \mathbf{E} \left(\frac{\xi_{i,Q}}{Q} \right)^{2k_i} - \prod_{i=0}^{n} \mathbf{E}\, \xi_i^{2k_i} \right| \leqslant \frac{2^{2k_0+\cdots+2k_n}}{Q}. \tag{13}$$

We proceed by induction on n. The case $n = 0$ follows from (11). It holds

$$\begin{aligned} &\left| \prod_{i=0}^{n} \mathbf{E} \left(\frac{\xi_{i,Q}}{Q} \right)^{2k_i} - \prod_{i=0}^{n} \mathbf{E}\, \xi_i^{2k_i} \right| \\ &\qquad \leqslant \left| \prod_{i=0}^{n-1} \mathbf{E} \left(\frac{\xi_{i,Q}}{Q} \right)^{2k_i} - \prod_{i=0}^{n-1} \mathbf{E}\, \xi_i^{2k_i} \right| \mathbf{E} \left(\frac{\xi_{n,Q}}{Q} \right)^{2k_n} \\ &\qquad\qquad + \prod_{i=0}^{n-1} \mathbf{E}\, \xi_i^{2k_i} \left| \mathbf{E} \left(\frac{\xi_{n,Q}}{Q} \right)^{2k_n} - \mathbf{E}\, \xi_0^{2k_0} \right|. \end{aligned}$$

Applying the induction assumption and (11), we obtain (13).

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

$$\left| \mathbf{E}\, D^k \left(\frac{G_Q}{Q} \right) - \mathbf{E}\, D^k(G) \right| \leqslant \frac{\gamma^k}{Q}, \tag{14}$$

where γ depends on n only.

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

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

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

$$|f_Q(t) - f(t)| = \left| \sum_{k=1}^{\infty} i^k \frac{\mathbf{E}\, D^k(G_Q/Q) - \mathbf{E}\, D^k(G)}{k!} t^k \right|$$
$$\leqslant \frac{1}{Q} \sum_{k=1}^{\infty} \frac{(\gamma|t|)^k}{k!} \leqslant \frac{\gamma|t|e^{\gamma|t|}}{Q}. \quad (15)$$

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 $T > 0$

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

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

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

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

§4. Resultants

Given polynomials

$$p(x) = a_n(x - \alpha_1)\dots(x - \alpha_n), \quad q(x) = b_m(x - \beta_1)\dots(x - \beta_m),$$

denote by $R(p, q)$ the resultant defined by

$$R(p, q) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Obviously discriminants are essentially a specialization of resultants via:

$$D(p) = (-1)^{n(n-1)/2} a_n^{-1} R(p, p').$$

Repeating the arguments from Section 3 we obtain the following result. Consider the random polynomials

$$G_Q(x) = \xi_{Q,n} x^n + \xi_{Q,n-1} x^{n-1} + \dots + \xi_{Q,1} x + \xi_{Q,0},$$
$$F_Q(x) = \eta_{Q,m} x^m + \eta_{Q,m-1} x^{m-1} + \dots + \eta_{Q,1} x + \eta_{Q,0}$$

with independent coefficients uniformly distributed on $2Q + 1$ points $\{-Q, \ldots, Q\}$ and consider the random polynomials

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

$$F(x) = \eta_m x^m + \eta_{m-1} x^{m-1} + \cdots + \eta_1 x + \eta_0$$

with independent coefficients uniformly distributed on $[-1, 1]$. Denote by ψ the distribution function of $R(G, F)$. We have

$$\sup_{-\infty \leqslant a \leqslant b \leqslant \infty} \left| \mathbf{P}\left(a \leqslant \frac{R(G_Q, F_Q)}{Q^{m+n}} \leqslant b \right) - \int_a^b \psi(x)\, dx \right| \ll \frac{1}{\log Q}.$$

Acknowledgments. We are grateful to Victor Beresnevich, Vasili Bernik, and Zakhar Kabluchko for useful discussions.

References

1. V. Beresnevich, V. Bernik, F. Götze, *The distribution of close conjugate algebraic numbers.* — Compos. Math., **146** (2010), 1165–1179.
2. V. Beresnevich, V. Bernik, F. Götze, *Integral polynomials with small discriminants and resultants.* — Preprint, arXiv:1501.05767, 2015.
3. V. Beresnevich, V. Bernik, F. Götze, O. Kukso, *Distribution of algebraic numbers and metric theory of diophantine approximation.* — In: Limit Theorems in Probability, Statistics and Number Theory, Springer, 2013, 23–48.
4. V. Bernik, F. Götze, O. Kukso, *Lower bounds for the number of integral polynomials with given order of discriminants.* — Acta Arith. **133** (2008), 375–390.
5. Y. Bugeaud, A. Dujella, *Root separation for irreducible integer polynomials.* — Bull. London Math. Soc. **162** (2011), 1239–1244.
6. Y. Bugeaud, A. Dujella, *Root separation for reducible integer polynomials.* — Acta Arith. **162** (2014), 393–403.
7. Y. Bugeaud, M. Mignotte, *On the distance between roots of integer polynomials.* — Proc. Edinb. Math. Soc. **47**, No. 2 (2004), 553–556.
8. Y. Bugeaud, M. Mignotte, *Polynomial root separation.* — Int. J. Number Theor. **6**, No. 03 (2010), 587–602.
9. J.-H. Evertse, *Distances between the conjugates of an algebraic number.* — Publ. Math. Debrecen **65** (2004), 323–340.
10. F. Götze, D. Kaliada, M. Korolev, *On the number of integral quadratic polynomials with bounded heights and discriminants.* — Preprint, arXiv:1308.2091, 2013.
11. D. Kaliada, F. Götze, O. Kukso, *The asymptotic number of integral cubic polynomials with bounded heights and discriminants.* — Preprint, arXiv:1307.3983, 2013.
12. K. Mahler, *An inequality for the discriminant of a polynomial.* — Mich. Math. J. **11**, No. 3 (1964), 257–262.

13. M. Mignotte, *Some useful bounds. Computer Algebra*. Springer, 1983, 259–263.
14. B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*. — Monatshefte für Mathematik **43**, No. 1 (1936), 133–147.

Faculty of Mathematics,
Bielefeld University,
P.O.Box 10 01 31, 33501 Bielefeld, Germany
E-mail: goetze@math.uni-bielefeld.de

Поступило 10 октября 2015 г.

St. Petersburg Department of
Steklov Institute of Mathematics,
Fontanka 27, 191011 St. Petersburg, Russia
E-mail: zap1979@gmail.com