УДК 511.35, 511.75, 511.48, 519.218.5

КОРРЕЛЯЦИЯ МЕЖДУ ДЕЙСТВИТЕЛЬНЫМИ СОПРЯЖЁННЫМИ АЛГЕБРАИЧЕСКИМИ ЧИСЛАМИ[1]

Ф. Гётце (г. Билефельд)

Д. В. Коледа (г. Минск)

Д. Н. Запорожец (г. Санкт-Петербург)

Аннотация

Пусть $B \subset \mathbb{R}^k$. Обозначим через $\Phi_k(Q, B)$ число лежащих в B упорядоченных наборов из k различных вещественных сопряжённых алгебраических чисел степени $\leq n$ и высоты $\leq Q$. Справедливо следующее соотношение:

$$\Phi_k(Q; B) = \frac{(2Q)^{n+1}}{2\zeta(n+1)} \int\limits_{B} \chi_k(\mathbf{x}) \prod_{1 \leqslant i < j \leqslant k} |x_i - x_j| \, d\mathbf{x} + O\left(Q^n\right), \quad Q \to \infty,$$

где функция χ_k непрерывна в $\mathbb{R}^k$ и будет явно выписана. Если $n = 2$, в остаточном члене появляется дополнительный множитель $\log Q$. Данное соотношение может быть истолковано как "отталкивание" вещественных сопряжённых алгебраических чисел друг от друга.

Функция

$$\rho_k(\mathbf{x}) := \chi_k(\mathbf{x}) \prod_{1 \leqslant i < j \leqslant k} |x_i - x_j|$$

совпадает с k-точечной корреляционной функцией случайного многочлена степени n с независимыми коэффициентами, равномерно распределёнными на отрезке $[-1, 1]$.

Ключевые слова: сопряжённые алгебраические числа, корреляции между алгебраическими числами, распределение алгебраических чисел, целочисленный многочлен, случайный многочлен.

Библиография: 18 названий.

CORRELATIONS BETWEEN
REAL CONJUGATE ALGEBRAIC NUMBERS

F. Götze (Bielefeld, Germany)

D. Kaliada (Minsk, Belarus)

D. Zaporozhets (Sankt-Peterburg, Russia)

Abstract

For $B \subset \mathbb{R}^k$ denote by $\Phi_k(Q, B)$ the number of ordered k-tuples in B of real conjugate algebraic numbers of degree $\leq n$ and naive height $\leq Q$. We show that

$$\Phi_k(Q; B) = \frac{(2Q)^{n+1}}{2\zeta(n+1)} \int_B \chi_k(\mathbf{x}) \prod_{1 \leqslant i < j \leqslant k} |x_i - x_j| \, d\mathbf{x} + O\left(Q^n\right), \quad Q \to \infty,$$

where the function χ_k is continuous in $\mathbb{R}^k$ and will be given explicitly. If $n = 2$, then an additional factor $\log Q$ appears in the reminder term. This relation may be regarded as a "repulsion" of real algebraic conjugates from each other.

The function

$$\rho_k(\mathbf{x}) := \chi_k(\mathbf{x}) \prod_{1 \leqslant i < j \leqslant k} |x_i - x_j|$$

coincides with a k-point correlation function of real zeros of a random polynomial of degree n with independent coefficients uniformly distributed on $[-1, 1]$.

Keywords: conjugate algebraic numbers, correlations between algebraic numbers, distribution of algebraic numbers, integral polynomial, random polynomial.

Bibliography: 18 titles.

1. Introdution

Baker and Schmidt [2] proved that the set of algebraic numbers of degree at most n forms a *regular system*: there exists a constant c_n depending on n only such that for any interval $I \subset \mathbb{R}^1$ and for all sufficiently large $Q \in \mathbb{N}$ there exist at least

$$c_n |I| \, Q^{n+1}/(\log Q)^{3n(n+1)}$$

algebraic numbers $\alpha_1, \ldots, \alpha_l$ of degree at most n and height at most Q satisfying

$$|\alpha_i - \alpha_j| \geq (\log Q)^{3n(n+1)}/Q^{n+1}, \quad 1 \leq i < j \leq l.$$

Later Beresnevich [4] showed that the logarithmic factors can be omitted.

Beresnevich, Bernik, and Götze [5] obtained the following result about the distribution of distances between conjugate algebraic numbers. Let $n \geqslant 2$ and $0 < w \leqslant \frac{n+1}{3}$. Then for all sufficiently large Q and any interval $I \subset \left[-\frac{1}{2}, \frac{1}{2}\right]$ there exist

at least $\frac{1}{2}Q^{n+1-2w}|I|$ real algebraic numbers α of degree n and height $H(\alpha) \asymp_n Q$ having a real conjugate α^* such that $|\alpha - \alpha^*| \asymp_n Q^{-w}$.

The simplest example of algebraic numbers are the rational numbers. Appropriately ordered, they form *the Farey sequences*. It is well-known that they are equidistributed in $[0,1]$, see [15] for an elementary proof and [8] for a deeper discussion of the subject. For the history of the problem we refer the reader to [7].

In 1971 Brown and Mahler [6] introduced a natural generalization of the Farey sequences: the Farey sequence of degree n and order Q is the set of all real roots of integral polynomials of degree n and height at most Q. The distribution of the generalized Farey sequences has been investigated in [12] (see also [11], [13] for the case $n = 2$).

Namely, fix $n \geq 2$ and consider an arbitrary interval $I \subset \mathbb{R}$. Denote by $\Phi(Q; I)$ a number of algebraic numbers $\alpha \in I$ of degree at most n and height at most Q. Then we have that

$$\Phi(Q; I) = \frac{(2Q)^{n+1}}{2\zeta(n+1)} \int_I \rho(x)\, dx + O\left(Q^n \log^{l(n)} Q\right), \quad Q \to \infty, \tag{1}$$

where $\zeta(\cdot)$ denotes the the Riemann zeta function and $l(n)$ is defined by

$$l(n) = \begin{cases} 1, & n = 2, \\ 0, & n \geq 3. \end{cases} \tag{2}$$

The limit density ρ is given by the formula

$$\rho(x) = 2^{-n-1} \int_{D_x} \left| \sum_{j=1}^n j t_j x^{j-1} \right| dt_1 \ldots dt_n, \tag{3}$$

where the domain of integration D_x is defined by

$$D_x = \left\{ (t_1, \ldots, t_n) \in \mathbb{R}^n : \max_{1 \leq k \leq n} |t_k| \leq 1, \ |t_n x^n + \cdots + tx| \leq 1 \right\}.$$

If $x \in [-1 + 1/\sqrt{2}, 1 - 1/\sqrt{2}]$, then (3) can be simplified as follows:

$$\rho(x) = \frac{1}{12} \left(3 + \sum_{k=1}^{n-1} (k+1)^2 x^{2k} \right).$$

The function ρ coincides with the density of the real zeros of the random polynomial

$$G(x) = \xi_n x^n + \xi_{n-1} x^{n-1} + \cdots + \xi_1 x + \xi_0, \tag{4}$$

where $\xi_0, \xi_1, \ldots, \xi_n$ are independent random variables uniformly distributed on $[-1, 1]$ (see, e.g., [18]). It means that for any Borel subset $B \subset \mathbb{R}^1$,

$$\mathbb{E}N(G, B) = \int_B \rho(x)\, dx,$$

where $N(G, B)$ denotes the number of zeros of G lying in B. The real zeros of G can be considered as a random point process. Its distribution can be described by its k-point correlation functions $\rho_k(x_1, \ldots, x_k)$, $k = 1, 2, \ldots, n$ (also known as joint intensities; see Section 2 for definition). The one-point correlation function ρ_1 coincides with the density ρ. The explicit formula for ρ_k has been obtained in [9] (see Section 2 for details).

The aim of this paper is to show that, like in the case $k = 1$, the correlation functions ρ_k are closely related with the joint distribution of real conjugate algebraic numbers.

Note that for $k = n$ we obtain the joint distribution of totally real algebraic numbers. These numbers (in particular, fields formed by them) are of great interest and possess some interesting properties. For example, lattices built by them are very well distributed in parallelepipeds, see [16].

We also mention that there are a number of papers where total number of k-vectors whose coordinates form a field extension of degree n over some base number field is considered. See e.g. [14] or [3] for some interesting results and references. In this area the multiplicative Weil height is usually used to measure such vectors.

2. Notations and main result

Let us start with some notation. Fix some positive integer $n \geq 2$ and $k \leq n$. Denote
$$\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{R}^k.$$

We use the following notation for the elementary symmetric polynomials:

$$\sigma_i(\mathbf{x}) := \begin{cases} 1, & \text{if} \quad i = 0, \\ \sum_{1 \leqslant j_1 < \cdots < j_i \leqslant k} x_{j_1} x_{j_2} \ldots x_{j_i}, & \text{if} \quad 1 \leq i \leqslant k, \\ 0, & \text{otherwise}. \end{cases}$$

Denote by $\mathcal{P}(Q)$ the class of all integral polynomials of degree at most n and height at most Q. The cardinality of this class is $(2Q + 1)^{n+1}$.

Recall that an integral polynomial is called *prime*, if it is irreducible over $\mathbb{Q}$, primitive (the greatest common divisor of its coefficients equals 1), and its leading coefficient is positive. Let $\mathcal{P}^*(Q)$ be the class of all prime polynomials from $\mathcal{P}(Q)$.

The *minimal polynomial* of an algebraic number α is a prime polynomial such that α is a root of this polynomial.

For a Borel subset $B \subset \mathbb{R}^k$ denote by $\Phi_k(Q; B)$ the number of ordered k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in B$ of *distinct* real numbers such that for some $p \in \mathcal{P}^*(Q)$ it holds

$$p(\alpha_1) = \cdots = p(\alpha_k) = 0.$$

Essentially $\Phi_k(Q; B)$ denotes the number of ordered k-tuples in B of conjugate algebraic numbers of degree at most n and height at most Q.

Given a function $g : \mathbb{R}^1 \to \mathbb{R}^1$ and a Borel subset $B \subset \mathbb{R}^k$ denote by $N_k(g, B)$ the number of ordered k-tuples $(x_1, x_2, \ldots, x_k) \in B$ of *distinct* real numbers such that

$$g(x_1) = \cdots = g(x_k) = 0.$$

For any algebraic number its minimal polynomial is prime, and any prime polynomial is a minimal polynomial for some algebraic number. Therefore we have that

$$\Phi_k(Q; B) = \sum_{p \in \mathcal{P}^*(Q)} N_k(p, B). \tag{5}$$

Applying Fubini's theorem to the right hand side we obtain

$$\Phi_k(Q; B) = \sum_{m=0}^{\infty} m \cdot \#\{p \in \mathcal{P}^*(Q) \,:\, N_k(p, B) = m\}. \tag{6}$$

Since $N_k(p, B) \leq n!/(n-k)!$, the sum in the right hand side is finite.

Now we are ready to state our main result.

THEOREM 1. *Let B be a region in $\mathbb{R}^k$ with boundary consisting of a finite number of algebraic surfaces. Then*

$$\Phi_k(Q; B) = \frac{(2Q)^{n+1}}{2\zeta(n+1)} \int_B \rho_k(\mathbf{x}) \, d\mathbf{x} + O\left(Q^n \log^{l(n)} Q\right), \quad Q \to \infty. \tag{7}$$

Here the function ρ_k is given by the formula

$$\rho_k(\mathbf{x}) = 2^{-n-1} \prod_{1 \leqslant i < j \leqslant k} |x_i - x_j| \int_{D_{\mathbf{x}}} \prod_{i=1}^{k} \left| \sum_{j=0}^{n-k} t_j x_i^j \right| dt_0 \ldots dt_{n-k}, \tag{8}$$

where the domain of integration $D_{\mathbf{x}}$ is defined by

$$D_{\mathbf{x}} = \left\{ (t_0, \ldots, t_{n-k}) \in \mathbb{R}^{n-k+1} \,:\, \max_{0 \leq i \leq n} \left| \sum_{j=0}^{n-k} (-1)^{i-j} \sigma_{i-j}(\mathbf{x}) t_j \right| \leq 1 \right\}.$$

The implicit big-O-constant in (7) depends on n, the number of the algebraic surfaces and their maximal degree only. The proof of Theorem 1 is given in Section 3.

COROLLARY 1. *The case $k = 1$ implies* (1).

COROLLARY 2. *If $k = n$, then* (8) *can be simplified as follows:*

$$\rho_n(\mathbf{x}) = \frac{2^{-n}}{(n+1)} \left(\frac{1}{\max_{0 \leqslant i \leqslant n} |\sigma_i(\mathbf{x})|} \right)^{n+1} \prod_{1 \leqslant i < j \leqslant n} |x_i - x_j|.$$

It has been shown in [9, Section 3] that the function ρ_k defined in (8) is a k-point correlation function of real zeros of the random polynomial G defined in (4). It means that for any Borel subset $B \subset \mathbb{R}^k$,

$$\mathbb{E} N_k(G, B) = \int_B \rho_k(\mathbf{x}) \, d\mathbf{x}. \tag{9}$$

Let us derive several properties of ρ_k.

PROPOSITION 5. *a) For any permutation s of length n,*

$$\rho_k\big(x_{s(1)}, x_{s(2)}, \ldots, x_{s(k)}\big) = \rho_k(\mathbf{x}).$$

b) For all $\mathbf{x} \in \mathbb{R}^k$,

$$\rho_k(-\mathbf{x}) = \rho_k(\mathbf{x}).$$

c) For all $\mathbf{x} \in \mathbb{R}^k$ with non-zero coordinates,

$$\rho_k(x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}) = \rho_k(\mathbf{x}) \prod_{i=1}^{k} x_i^2.$$

PROOF. The first and the second properties are trivial. To prove the last one, note that for any integral irreducible polynomial $g(z)$ of degree n, the polynomial $z^n g(z^{-1})$ is also irreducible and has the same degree and height. Therefore for any Borel set $B \subset \mathbb{R}^k$ which does not contain points with zero coordinates we have

$$\Phi_k(Q; B^{-1}) = \Phi_k(Q; B),$$

where B^{-1} is defined as

$$B^{-1} := \big\{ (x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}) : (x_1, x_2, \ldots, x_k) \in B \big\}.$$

Letting Q tend to infinity, we obtain from (7) that

$$\int_B \rho_k(\mathbf{x}) \, d\mathbf{x} = \int_{B^{-1}} \rho_k(\mathbf{x}) \, d\mathbf{x}.$$

Making the substitution $(x_1, \ldots, x_k) \to (x_1^{-1}, \ldots, x_k^{-1})$, we obtain

$$\int_B \rho_k(\mathbf{x}) \, d\mathbf{x} = \int_B \left(\prod_{i=1}^{k} x_i^{-2} \right) \rho_k(x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}) \, d\mathbf{x}.$$

Since the class of sets B is large enough, the third property follows. $\square$

3. Proof of Theorem 1

For a Borel set $A \subset \mathbb{R}^n$ denote by $\lambda^*(A)$ the number of points in A with coprime integer coordinates.

Consider a set $A_m \subset [-1, 1]^{n+1}$ consisting of all points $(t_0, \ldots, t_n) \in [-1, 1]^{n+1}$ such that

$$N_k(t_n x^n + \cdots + t_1 x + t_0, B) = m.$$

Then the number of primitive polynomials $p \in \mathcal{P}(Q)$ such that $N_k(p, B) = m$ is equal to $\lambda^*(QA_m)$. Hence it follows from the definition of a prime polynomial that

$$\left| \#\{p \in \mathcal{P}^*(Q) : N_k(p, B) = m\} - \frac{1}{2}\lambda^*(QA_m) \right| \le R_Q, \tag{10}$$

where R_Q denotes the number of reducible polynomials (over $\mathbb{Q}$) from $\mathcal{P}_Q$. Note that the factor $1/2$ arises because prime polynomials have positive leading coefficient. It is known (see [17]) that

$$R_Q = O\left(Q^n \log^{l(n)} Q\right), \quad Q \to \infty. \tag{11}$$

Combining (10) and (11) with (6), we obtain

$$\Phi_k(Q; B) = \frac{1}{2} \sum_{m=0}^{\infty} m\lambda^*(QA_m) + O\left(Q^n \log^{l(n)} Q\right), \quad Q \to \infty. \tag{12}$$

To estimate $\lambda^*(QA_m)$, we need the following lemma.

LEMMA 1. *Consider a region $A \subset \mathbb{R}^d$, $d \ge 2$, with boundary consisting of a finite number of algebraic surfaces. Then*

$$\lambda^*(QA) = \frac{\mathrm{Vol}(A)}{\zeta(n)}Q^d + O\left(Q^{d-1} \log^{l(d)} Q\right), \quad Q \to \infty, \tag{13}$$

where the implicit constant in the big-O-notation depends on d, the number of the algebraic surfaces and their maximal degree only.

PROOF. The results of this type are well-known, see, e.g., the classical monograph by Bachmann [1, pp. 436–444] (in particular, formulas (83a) and (83b) on pages 441–442). For the proof of Lemma 1, see [10]. □

Since the boundary of B consists of a finite number of algebraic surfaces, the same is true for A_m. Hence it follows from Lemma 1 that

$$\lambda^*(QA_m) = \frac{\mathrm{Vol}(A_m)}{\zeta(n+1)}Q^{n+1} + O\left(Q^n\right), \quad Q \to \infty,$$

which together with (12) implies

$$\Phi_k(Q; \Omega) = \frac{Q^{n+1}}{2\zeta(n+1)} \sum_{m=0}^{\infty} m \, \mathrm{Vol}(A_m) + O\left(Q^n \log^{l(n)} Q\right), \quad Q \to \infty. \tag{14}$$

To calculate $\sum_{m=0}^{\infty} m \operatorname{Vol}(A_m)$, note that

$$\operatorname{Vol}(A_m) = 2^{n+1}\, \mathbb{P}(N_k(G, B) = m),$$

where G is the random polynomial defined in (4). Hence

$$\sum_{m=0}^{\infty} m \operatorname{Vol}(A_m) = 2^{n+1}\, \mathbb{E}N_k(G, B). \tag{15}$$

Applying (9) finishes the proof.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Bachmann P. Die analytische Zahlentheorie, volume 2. BG Teubner, Leipzig, 1894.

2. Baker A., and Schmidt W. Diophantine approximation and Hausdorff dimension // Proc. London Math. Soc. 1970. Vol. 3, No. 1. P. 1–11.

3. Barroero F. Counting algebraic integers of fixed degree and bounded height // Monatshefte für Mathematik. 2014. Vol. 175, No. 1. P. 25–41.

4. Beresnevich V. On approximation of real numbers by real algebraic numbers // Acta Arith. 1999. Vol. 90, No. 2. P. 97–112.

5. Beresnevich V., Bernik V., and Götze F. The distribution of close conjugate algebraic numbers // Compos. Math. 2013. Vol. 146, No. 5. P. 1165–1179.

6. Brown H., and Mahler K. A generalization of Farey sequences: Some exploration via the computer // J. Number Theory. 1971. Vol. 3, No. 3. P. 364–370.

7. Cobeli C., and Zaharescu A. The Haros-Farey sequence at two hundred years // Acta Univ. Apulensis Math. Inform. 2003. No. 5. P. 1–38.

8. Dress F. Discrépance des suites de Farey // J. Théor. Nombres Bordeaux. 1999. Vol. 11, No. 2. P. 345–367.

9. Götze F., Kaliada D., and Zaporozhets D. Correlation functions of real zeros of random polynomials // arXiv preprint. 2015. arXiv:1510.00025.

10. Götze F., Kaliada D., and Zaporozhets D. Distribution of complex algebraic numbers // arXiv preprint. 2015. arXiv:1410.3623.

11. Коледа Д. В. О распределении действительных алгебраических чисел второй степени // Весці НАН Беларусі. Сер. фіз.-мат. навук. 2013. № 3. С. 54–63.

12. Kaliada D. On the density function of the distribution of real algebraic numbers // arXiv preprint. 2014. arXiv:1405.1627.

13. Коледа Д. В. Об асимптотике распределения алгебраических чисел при возрастании их высот // Чебышевский сб. 2015. Т. 16, № 1. С. 191–204.

14. Masser D., and Vaaler J. D. Counting algebraic numbers with large height II // Trans. Am. Math. Soc. 2007. Vol. 359, No. 1. P. 427–445.

15. Mikolás M. Farey series and their connection with the prime number problem. I // Acta Univ. Szeged. Sect. Sci. Math. 1949. Vol. 13. P. 93–117.

16. Скриганов М. М. Решётки в полях алгебраических чисел и равномерные распределения по mod 1 // Алгебра и анализ. 1989. Vol. 1. No. 2. P. 207–228.

17. van der Waerden B. L. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt // Monatsh. Math. Phys. 1936. Vol. 43, No. 1. P. 133–147.

18. Запорожец Д. Н. Случайные полиномы и геометрическая вероятность // Докл. Акад. наук. 2005. Т. 400, № 3. С. 299–303.

REFERENCES

1. P. Bachmann 1894, "Die analytische Zahlentheorie", volume 2. BG Teubner, Leipzig.

2. A. Baker & W. Schmidt 1970, "Diophantine approximation and Hausdorff dimension", *Proc. London Math. Soc.*, vol. 3, no. 1, pp 1–11.

3. F. Barroero 2014 "Counting algebraic integers of fixed degree and bounded height", *Monatshefte für Mathematik*, vol. 175, no. 1, pp 25–41.

4. V. Beresnevich 1999, "On approximation of real numbers by real algebraic numbers", *Acta Arith.*, vol. 90, no. 2, pp 97–112.

5. V. Beresnevich, V. Bernik, & F. Götze 2010, "The distribution of close conjugate algebraic numbers", *Compos. Math.*, vol. 146, no. 5, pp 1165–1179.

6. H. Brown & K. Mahler 1971, "A generalization of Farey sequences: Some exploration via the computer", *J. Number Theory*, vol. 3, no. 3, pp 364–370.

7. C. Cobeli & A. Zaharescu 2003, "The Haros-Farey sequence at two hundred years", *Acta Univ. Apulensis Math. Inform.*, vol. , no. 5, pp 1–38.

8. F. Dress 1999, "Discrépance des suites de Farey", *J. Théor. Nombres Bordeaux*, vol. 11, no. 2, pp 345–367.

9. F. Götze, D. Kaliada & D. Zaporozhets 2015, "Correlation functions of real zeros of random polynomials", *Preprint, arXiv:1510.00025*.

10. F. Götze, D. Kaliada & D. Zaporozhets 2015, "Distribution of complex algebraic numbers", *Preprint, arXiv:1410.3623*.

11. D. Kaliada 2013, "Distribution of real algebraic numbers of the second degree", *Vestsi NAN Belarusi. Ser. fiz.-mat. navuk*, vol. , no. 3, pp 54–63. (In Russian).

12. D. Kaliada 2014, "On the density function of the distribution of real algebraic numbers", *Preprint, arXiv:1405.1627*.

13. D. Koleda 2015, "On the asymptotic distribution of algebraic numbers with growing naive height", *Chebyshevskii Sb.*, vol. 16, no. 1, pp 191–204. (In Russian).

14. D. Masser & J. D. Vaaler 2007, "Counting algebraic numbers with large height II", *Trans. Am. Math. Soc.*, vol. 359, no. 1, pp 427–445.

15. M. Mikolás 1949, "Farey series and their connection with the prime number problem. I", *Acta Univ. Szeged. Sect. Sci. Math.*, vol. 13:93–117.

16. M. M. Skriganov 1989, "Lattices in algebraic number fields and uniform distribution mod 1", *Algebra i Analiz*, vol. 1, no. 2, pp 207–228. (In Russian).

17. B. L. van der Waerden 1936, "Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt", *Monatsh. Math. Phys.*, vol. 43, no. 1, pp 133–147.

18. D. Zaporozhets 2005, "Random polynomials and geometric probability", *Dokl. Akad. Nauk*, vol. 71, no. 1, pp 53–57.

Университет г. Билефельда (г. Билефельд, Германия).
Институт математики НАН Беларуси (г. Минск, Беларусь).
Петебургское отделение Математического института РАН (г. Санкт-Петербург, Россия).